SAFEGUARDING CHILDREN'S PRIVACY: A STUDY OF REGULATION AND PRACTICE IN THE UNITED KINGDOM AND THE UNITED STATES

Juncheng Cao*

Abstract: In recent years, there has been a growing emphasis on protecting privacy in the global internet economy and innovation. Consequently, governments have implemented strict regulations on the issue. However, information society service providers (ISS providers) may approach this problem differently due to their unique service domains. Compliance with regulations such as the ICO code and COPPA may present challenges for operators due to technical difficulties and unclear guidelines. Unfortunately, these issues ultimately harm users, especially children. To address this problem, this note examines the key elements and regulations of the ICO code and analyzes the privacy policies for children issued by five major technology companies. The aim is to clarify existing protective measures and identify areas for improvement. Additionally, this note highlights the challenges ISS providers face when trying to identify children. The author's objective is to provide a clear understanding of the current system for protecting children's privacy, with the goal of improving the situation.

Keywords: Children's Privacy; ICO Code; Information Society Service Providers; Consent; Parental Control

* KoGuan School of Law, Shanghai Jiao Tong University, China.

Table of Contents

INTRODUCTION

Protecting personal information, especially children's data, has been emphasized recently. Due to the COVID-19 epidemic, children are now online more than ever, not just for school but also for socializing and gaming.[1] As a result, regulations related to this issue have been implemented by Russia, China, and OECD countries and regions. Examples include the Children's Online Privacy Protection Act (COPPA) in the United States and the Age Appropriate Design Code (children's code) issued by the UK Information Commissioner's Office. In addition to legal requirements, technology giants have also made efforts to update their privacy policies to meet the latest standards set by local authorities. Despite these efforts to comply, some tech companies are still facing legal consequences for failure to adhere to these regulations. ByteDance and its affiliates are among the companies that have faced such consequences.

On 23 March 2023, the testimony of Shou Chew, CEO of TikTok Inc., captured global attention for previously, the media giant was confronted with the pressure of forced sales in the United States.[2] This can be a piece of breaking news for TikTok has already gained a stable colossal market share worldwide, with at least 150 million users merely in America. The two domains of this testimony are American privacy and protecting children from online harm, respectively.[3] Although some have questioned whether this was an action taken by US authorities to combat Chinese development in this field, Chew's testimony exemplified how livestream media providers are responding to the challenges of protecting children from online harm. In the hearing, Chew stated:

Minor safety and wellness are priorities of TikTok; its age-appropriate settings and controls consider not only children (under 13, by US regulations) but also the 13-17 teenage group. For instance, children are not allowed to post videos on the platforms. Messaging with others and advertising to those under 13 have also been banned.[4] To identify potential unqualified users, TikTok has also introduced text-based models such as Natural Language Processing in pursuit of full compliance with its privacy policies. Additionally, TikTok limits screen time for teenage users and children. Only when they reach 18 shall they access unlimited screen time. Moreover, Family Paring, proposed by TikTok, allows parents or guardians to link their accounts to youngsters' ones, empowering them to customize their teens' privacy and safety settings.[5] So far, no further result concerning the hearing has been announced, but the testimony is sufficient for a general idea of the latest practice in children's privacy protection. Chew's hearing was only part of recent news concerning TikTok and ByteDance's future.

---

[1] Chrissie Scelsi, *Children's Online Privacy Protection*, 37 GPSOLO 42 (2020).
Thanks to the COVID-19 pandemic, most schools are closed, turning every home with children into a home school of some sort. This often involves having students use various online platforms for classes and assignments. Kids are now online more than ever, not just for school but also for socializing and gaming, and parents who can work from home are often juggling trying to help their kids with school while managing their own workload.

[2] See March 23, 2023 - TikTok CEO Shou Chew testifies before Congress, https://edition.cnn.com/business/live-news/tiktok-ceo-congressional-hearing-shou-chew-03-23-23/index.html (last visited Apr. 12 2023)

[3] See Full Committee Hearing: "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms", https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms (last visited Apr. 12 2023)

[4] Testimony Before the U.S. House Committee on Energy and Commerce, https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-Wstate-ChewS-20230323.pdf (last visited Apr. 12 2023)

[5] Id.

ByteDance, founded in March 2012, is a Chinese technology giant boasting several well-known products such as TikTok, Toutiao, and Lark. Taking TikTok as an example, it has offices across the globe, including New York, London, Paris, Dubai, etc.[6] On 26 December 2022, the UK Information Commissioner's Office (ICO) announced that it would impose a £27 million fine on TikTok for failing to protect children's privacy.[7] More specifically, the 'notice of intent' issued by the ICO indicated that TikTok may have breached UK data protection law between May 2018 and July 2020. Even though ICO's findings are provisional, and it may still take some time for ICO to make the final decision,[8] the author of the note is convinced that much effort should be devoted to discussing whether TikTok had full compliance with the obligation to protect the privacy of children.

This was not the first time that TikTok was involved in cases of this type. As early as Feb. 2, 2019, MUSICAL.LY, a well-known video-sharing app merged into TikTok in 2018, was charged with violating the COPPA rules and the False Claims Act (FCA) by failing to protect children's personal information and several other reasons.[9] The American version of the TikTok case ended with the settlement reached between Musical.ly and the US government on condition that the defendants (1) pay $5,700,000 as a civil penalty; (2) report on their deletion obligations under penalty of perjury; (3) strictly observe the compliance reporting obligations; (4) keep necessary records as required and (5) accept compliance monitoring according to the order.[10] Merely one year later approximately, TikTok was once more fined £123,000 in South Korea for collecting data of children under 14 years old without the consent of legal guardians.[11]

Thanks to the ample quantities of privacy policies available on the Internet, the author is blessed with the opportunity to look into how technology giants who provide services targeted at children comply with the latest versions of the ICO Children's Code. In the first part, I will focus on the primary issue: why should children be taken special care of in the field of privacy protection from the perspective of children's cognitive capabilities? In the second part of this note, it interprets several important sections included in the ICO Children's code (*If not especially noted, 'ICO ADC' & Age-Appropriate Design Code & ICO Children's Code share the same meaning in this note, these terms refer to the Age-Appropriate Design Code*

---

[6] Our Products, https://www.bytedance.com/en/products (last visited Jan. 24, 2023)
TikTok is the leading destination for short-form mobile video. Our mission is to inspire creativity and bring joy. TikTok has offices across the globe, including Los Angeles, New York, London, Paris, Berlin, Dubai, Mumbai, Singapore, Jakarta, Seoul, and Tokyo.

[7] ICO could impose multi-million pound fine on TikTok for failing to protect children's privacy, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/ (last visited Jan. 23, 2023)
TikTok could face a £27 million fine after an ICO investigation found that the company may have breached UK data protection law, failing to protect children's privacy when using the TikTok platform. The ICO has issued TikTok Inc and TikTok Information Technologies UK Limited ('TikTok') with a 'notice of intent' - a legal document that precedes a potential fine. The notice sets out the ICO's provisional view that TikTok breached UK data protection law between May 2018 and July 2020.

[8] Id.

[9] Musical.ly and Musical.ly, Inc.: [Proposed] Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief - February 27, 2019, https://www.ftc.gov/system/files/documents/cases/musical.ly_proposed_order_ecf_2-27-19.pdf (last visited Jan. 23, 2023)

[10] Id.

[11] TikTok fined for mishandling child data in South Korea, https://www.bbc.com/news/technology-53418077 (last visited Jan. 24, 2023)

issued by the UK Information Commissioner's Office[12]). This study covers a range of topics related to the ICO ADC, including its applicability, the effectiveness of GDPR in Britain post-Brexit, and the protective measures implemented by the ICO ADC, such as the legal definition of 'child'. It also explores the individual rights afforded to children, the roles of parental and children's consent with regard to the sharing of children's information, and the process for conducting a Data Protection Impact Assessment (DPIA). Additionally, this work offers insight into the privacy policies for children of five technology giants: Apple, Microsoft, Instagram, Twitter, and TikTok. The author compares their policies and assesses their compliance with the ICO ADC.

I. THE NECESSITY OF SPECIAL CARE FOR CHILDREN

Why should children be given special care? Although it is commonly believed that children have limited ability to understand events, it is important to consider how this applies to information and technology. In this article, the author refers to "special care" as additional protection and argues that it is essential to determine different levels of care for children of different ages. The problem at hand is rooted in children's ability to comprehend instructions or statements made by information society service (ISS) providers. The author has not had access to updated experiments or research on children's understanding of essential characteristics of internet services. However, surveys conducted by Rona Abramovitch and other researchers may provide valuable information.

Rona's empirical study measured children's capacity to consent to participation in psychological research.[13] The subjects were 163 children whose ages ranged from five to twelve. In the study, experimenters explained to the children that they might participate in the research voluntarily and that the survey result would be kept confidential. The survey may only be conducted after the children agree to participate. In the studies, children were presented with two sections of questions. One section is designed to measure children's comprehension of the survey explanation, including confidentiality, the character of voluntary, etc. Whereas the other section is a plain survey with little regard to this article, in which children were required to respond to questions concerning unrelated topics such as foods.[14]

The researchers found out that, generally, most subjects performed positively in retelling the contents of the experiment, with 100% of children aged 9 to 11 correctly answering the contents and approximately 85% of children aged 7 to 8 correctly responding. Nevertheless, children need to be more capable of accurately understanding why the research will be conducted. Concerning confidentiality, three-quarters of children fully understand that their answers will be kept secret, and 100% of 11-year-old children responded correctly to this task. In addition, more than 85% of children aged from 10 to 11 comprehended that they were entitled to withdraw from the experiment so long as they wanted because the survey is entirely voluntary. The figure for children aged from 8 to 9 is 75%.[15]

The statistics mentioned earlier show that children aged 7 to 12 generally understand the contents and core functions of a new item. They also comprehend the meaning of

[12] (Noted by the author) The pdf version of the code can be downloaded from the website: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

[13] See Rona Abramovitch et al., *Children's Capacity to Consent to Participation in Psychological Research: Empirical Findings*, 62 CHILD DEVELOPMENT 1100 (1991).

[14] *Id.*

[15] *Id.*

confidentiality, as long as the statement provided is accurate. In addition, they understand the definition of 'volunteer' with regard to consenting to participate in an experiment. This survey provides valuable insights, demonstrating that children are capable of comprehending the characteristics of a task, item, or service, which can aid in their growth. It also indicates that young children are partly mature enough to give consent, although parental control or influence is still necessary to ensure their understanding is correct. In addition, it's brilliant for the researchers to notice that external factors such as the emotion of experimenters may exert unexpected influence on children's decisions, contributing to the availability of adapting the research to this article concerning children's privacy protection.[16]

Returning to our topic, based on the research mentioned above, it seems that it's a good idea for parents to accompany children under 13. This is because children may not fully understand the instructions or explanations provided by service providers. While the survey used simple language that everyone could understand, things can be more complex in the real world. Some ISS providers use complicated expressions that make it hard for users to comprehend, which can discourage them from reading privacy policies. This is one reason why adults should be involved in giving their consent.

On the other hand, the survey found that children are vulnerable to external factors such as emotions, and their consent may not be taken seriously when presented with engaging visual content. From the perspective of children's understanding, they can grasp the general meanings of terms like 'confidential' and 'voluntary' to some extent, but it's important to provide unique explanations. For example, young children may understand 'not telling anyone else, including one's parents,' instead of 'keeping the information confidential.' To get individual consent from children, simplified versions of privacy policies should be available. However, the author couldn't find any mandate rules that requires ISS providers to publish policies designed for children to read. In this regard, parental involvement is still necessary.

Moreover, the research also found that when children and parents had differing opinions on the use of a specific service, a significant number of children chose to follow their parents' opinions. This demonstrates that for young children, they still believe parents' instructions should be followed and obeyed, even though they may prefer the opposite option.

Considering the apparent influence of external factors and children's reliance on parents, the author concludes that special care for children under thirteen is still necessary. For lack of proficiency in comprehensive understanding, children's information rights may be violated without notice. However, I still regard providing children with due respect in giving individual consent as appropriate since children in the research have displayed their understandings and have already generated ideas different from their parents'. As is deduced from the survey results, providing elder children with a higher level of freedom coincides with their capability for comprehensive understanding. In light of this trend, it is necessary to guide ISS providers to allow children's access to services or determine their affairs as they mature while providing extraordinary care and secure services.

II. REGULATORY BASIS FOR CHILDREN'S PRIVACY PROTECTION

A. A Brief Introduction to the ICO Code and ICO ADC

[16] *Id.*

First, it is necessary to clarify the legal status of the ICO code to be discussed in this note. The ICO Children's code is issued by the UK Information Commissioner's Office, which is not a legislative authority. ICO is the UK's independent body set up to uphold information rights.[17] Unlike laws issued by legislative authorities, violating the ICO codes may not lead to direct legal consequences. Still, the deed of violation can indicate a corporation's failure to protect the user's privacy in a required approach.

The legal basis of the ICO code derives from Section 121(1) of the UK Data Protection Act 2018:

The Commissioner must prepare a code of practice which contains—

(a)practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and

(b)such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.[18]

Analyzing the section quoted above, issuing ICO Code is the obligation of the Information Commissioner's Office, and the ICO code exists to ensure a better practice in personal data sharing. More specifically, according to Subsection (a), the ICO code is designed to guide Internet service providers to share personal data in ways that do not violate data protection legislation. Therefore, if a service provider's protection mechanism can not satisfy the requirement of the ICO code, it stands a higher chance of breaking the Data Protection Act. Furthermore, the legal status of ICO ADC is similar to the general ICO Code. Section 123 of the Data Protection Act 2018 required that the Information Commissioner's Office issue a code designed to guide the information society services likely to be accessed by children.[19]

On the whole, the ICO ADC is comprised of 15 standards that online services need to follow, with the code's aim targeted at ensuring Internet service providers comply with their obligations and children's privacy is protected in a proper and effective method.[20] Evidently, the ICO ADC does not apply to children and their parents. Instead, information society services shall bear the responsibility of protecting personal information. More specifically, the information society service mentioned above can, to a certain extent, be limited to those likely to be accessed by children, even though children are not aimed. Meanwhile, the formal definition of ISS is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'[21]

---

[17] About the ICO, https://ico.org.uk/about-the-ico/who-we-are/ (last visited Jan. 25, 2023)
[18] Data Protection Act, 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[19] Id. at Section 123.
The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children. Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.
[20] Introduction to the Age appropriate design code, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (last visited Jan. 24 2023)
[21] Id.
The code applies to "information society services likely to be accessed by children". The definition of an ISS is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." What this means in practice is that most for-profit online services are ISS, and therefore covered by the code. [...] If your online service is likely to be accessed by children under the age of 18, even if

To further clarify the concept of ISS, the ICO indicated that the following services shall be under supervision: 'apps; programs; search engines; social media platforms; online messaging or internet-based voice telephony services; online marketplaces; content streaming services (e.g., video, music or gaming services); online games; news or educational websites; and any websites offering other goods or services to users over the internet.'[22] The wide range of services listed above contributes to the fact that most profit-driven services must comply with the ICO ADC to provide sufficient protection for children and their data.

It should be noted that the ICO ADC does not apply to schools or educational institutions, for they do not meet the definition of ISS.[23] That is, even though a certain information Society Service is provided for kids to use, if the service is provided via a school or similar institution, the ICO ADC shall not apply. However, this exemption differs from removing the school's responsibility regarding children's privacy protection. Schools still have to comply with the UK GDPR and other regulations. Since this note focuses mainly on the services to which the ICO children's code applies, I will not lay much emphasis on the regulation of schools.

In addition, the ICO children's code does not simply apply to companies registered in the UK. This code also applies to those who process the data of UK children.[24] This enables the ICO to be effective for overseas corporations, giving rise to more complex issues such as cross-border transferring of data, as I will discuss later.

B. Adaption of GDPR in the United Kingdom

The General Data Protection Act (GDPA in abbreviation) is one of Europe's most important legal sources of data protection. Due to Britain's exit from the European Union in 2018, GDPR no longer directly applied to Britain. Nevertheless, the EU GDPR has been incorporated directly into UK law as the UK GDPR.[25] Even though British data processors no longer have to comply with the EU GDPR in Britain, shall they wish to operate in the European Economic Area (EEA), they are still confined to the act.

For those data processors who obtain data from the EU or EEA, they shall be familiar with the term 'adequacy'. The European Union coined this term to describe countries,

---

it's not aimed at them, then you are probably covered by the code. This means you may need to make some changes to how you design your service and how you process personal data to ensure you conform with the code.

[22] Id.

[23] FAQs for education technologies (edtech) and schools, https://ico.org.uk/for-organisations/childrens-code-hub/faqs-for-education-technologies-edtech-and-schools/ (last visited Jan. 25 2023)
To be defined as an Information Society Service (ISS), organizations must meet several qualifying conditions which are set out in services covered by the code. Schools do not meet the definition of an ISS. However, the code's vision – to ensure that the best interests of children are a primary concern when using their data – also closely aligns with schools' own educational mission. Schools are also required to comply with UK GDPR and the Data Protection Act 2018, and the code sets out what good practice compliance looks like in the areas it covers. We therefore encourage schools to aspire to meet the code's 15 standards as a matter of general good practice.

[24] Introduction to the Age appropriate design code, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (last visited Jan. 24 2023)

[25] See Overview – Data Protection and the EU, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/ (last visited Feb. 16 2023)
The EU GDPR is an EU Regulation that no longer applies to the UK. You must comply with the Data Protection Act 2018 (DPA 2018) if you operate inside the UK. The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. There is little change to the core data protection principles, rights, and obligations in practice. GDPR recitals add depth and help to explain the binding articles. Recitals continue to have the same status as before – they are not legally binding and help understand the articles' meaning.

territories, sectors, or organizations with essentially equivalent data protection levels to the EU. So far, the EU Commission has adopted adequacy decisions for the UK GDPR, enabling British data processors to obtain data from EU countries freely on most occasions. However, if offices or branches of a UK corporation are established within EEA, this corporation shall comply with the UK and EU regulations.[26]

Except for the special case of corporations with branches mentioned above, it is worth noting that 'adequacy' does not apply to immigration exemption. Time and space limiting, I will not explain this case in this note.

C. What's the definition of children, and why should they be taken special care of in data protection?

Before discussing and analyzing the ICO ADC, it is of primary importance to define 'children' under the ICO code. As is indicated in Section 1 of the UK Family Law Reform Act 1969, the age of majority is set at 18, which gives rise to these issues: whether or not individuals must exceed 18 years old to consent to the use of their data. If not, how old will a child be mature enough to decide on the usage of his data? The answer to the above question lies in the application guideline named 'Children and the GDPR' issued by ICO. According to the guideline, if a child is to consent, the child should be at least 13 years old unless the ISS is an online preventive or counseling service.[27]

Generally speaking, children lack the legal status to fully shoulder legal liabilities because they may need to be more competent to understand the consequences of their deeds. Such is the case with data protection. Considering children's inability to understand what they consent to and what outcome their consents are giving rise to, they are deprived of the right to approve independently. However, shouldering legal liabilities and facing the risk of data misusing are of different severity. The latter one may exert less impact on a child since whether substantial harm may emerge remains unknown. Moreover, in the latter situation, the children's guardians may withdraw the previous consent as they wish, providing a chance to minimize the unwanted result aroused by false permission.

In conclusion, from the differences in consequence and possibility to compensate, it is reasonable to set lower age standards for children when it comes to data protection, and they should be granted more freedom to make their own decisions on data use even though they may not reach the age of majority.

D. Parental control versus children's independent right

Even though ICO has already provided several methods to guide ISS to identify teens below or above 13, children may make false presentations about their age to access services only available to older people, reducing the effect of the data protective mechanism. Moreover, not every child aged 13 can understand their approval's consequences. Therefore, parental control may be in place to keep children away from risks triggered by data misuse.

ICO indicates that introducing parental control is essential for children's best interests. Parental controls refer to the condition in which parents are allowed by service providers to monitor their children's internet-based activities, track their locations, or limit children's online

[26] Id.
[27] See https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/ (last visited Feb. 17 2023)

activities. This seems unreasonable for service providers since they have fewer chances to get children to use their service, putting servers at risk of losing potential customers. However, from the perspective of cost and effect, service providers' willingness to accept parental control justifies that they operate the service on the condition that children's best interests are guaranteed, reducing their risks of violating the ICO ADC. Therefore, accepting parental control can be wise for ISS providers in the long run. As it turned out, hosts of Internet giants such as Apple Inc. have set up children's accounts, which can only be activated with the company of parent accounts. I will discuss the design of parent & child accounts in the latter parts of this note.

Nevertheless, it cannot be neglected that children should be freed from parents' supervision in certain respects. Children, who can be viewed individually as data subjects, also expect their data privacy and sense of their identities to be respected. Therefore, children should at least be notified if their parents monitor their online activities. In fact, the conclusion stated above derives from Article 5(1)(a) of the GDPR, which demands that personal data be processed lawfully, fairly, and transparently.

In response to the GDPR, the ICO set forth a matrix of recommendations to guide ISS providers to balance children's right to private space and the necessity of parental control. In the first place, the ICO divided children under 18 years old (the age of majority) into five groups based on their maturity: (1) Pre-literate & early literacy (aged 0 to 5); (2) Core primary school years (aged 6 to 9); (3) Transition years (aged 10 to 12); (4) Early teens (aged 13 to 15) and (5) Approaching adulthood (aged 16 to 17).[28] This classification approach matches perfectly with the application of GDPR issued by ICO, which stated that only children reaching 13 years old are qualified to consent. This is to say, only early teens and individuals who are approaching adulthood can give sole consent, but their parents may still monitor them. In line with the matrix, the protection of Class I children is of the highest level among the five classes, while children of Class IV and V are granted more freedom compared to individuals from the other three categories. Listed below are recommended methods designed by the ICO to help balance the protection of children and the call for privacy respect.

First, 'providing a clear and obvious sign that indicates when monitoring or tracking is active.' can be found in the recommended items for all age groups. It is easy to understand that this recommendation responds to the transparency requirement. Furthermore, as the author understands, indicating to children that their online activities are being tracked and monitored demonstrates respect for children's privacy since there's no chance of being supervised without notice. While on the other hand, in addition to knowing what their children are doing with the ISS, the tracking alert may also prevent children from misbehaving online since children are informed of their parents' accessibility to their activities.

Another recommended item of information to be provided is 'materials for parents explaining the children’s right to privacy under the UNCRC '. This recommendation can be found in all five categories. Still, for Class I, II, and III, parents may also be informed of children's possible increasing expectations about their privacy rights as they age. The author finds this designation meaningful since when children do not reach the stage of 'transition', they are less likely to make decisions on themselves since they won't be blessed with the right to

[28] For the sake of convenience, in this note, Class I represents 'Pre-literate & early literacy'; Class II represents 'Core primary school years'; Class III represents 'Transition years'; Class IV represents 'Early teens' and Class V represents 'Approaching adulthood'.

give independent consent. Parents' understanding of children's need to increase privacy space may enable children to transition smoothly from the core primary school years to the next stage.

The third universally applied recommendation for class I, II, and III is 'providing materials for the child to understand that their parent is being told where they are and/or what they do online to help keep them safe.' The only difference is whether the children's location should be provided to parents. Nevertheless, the author proposes that there's no need to make such a difference since parents cannot thoroughly screen out the possibility of pre/early literate children using ISS outside some safe regions. Moreover, these children from Class I are more vulnerable than those from Class II and III. Thus they deserve a higher standard of protection. Therefore, I understand that recommending ISS providers to adopt location supervision for children under 13 can be a better version. According to the recommendation matrix, when children reach the age of thirteen, the ICO suggests ISS providers supply children with materials explaining how the service works and the balance between parental monitor and child privacy rights, providing children with more respect for their own decision and privacy. What's unique about Class III is that the ICO recommends ISS providers to 'provide resources suitable for the child to use independently which explain the service and discusses privacy rights'. As I understand, the reason for which this item can only be found in Class III is that ICO was trying to prepare children from 10 to 12 for their future independent consent. Only after being exposed to real decision situations will they be capable of giving responsible and reasonable independent approvals when they reach the age of 13.

Summarizing the aforementioned analysis, ICO's efforts were mainly to balance protecting children's data privacy and respecting children's private space. The two parts contradict each other since protecting children's data is completed via parental control, which may deprive kids of their personal space. Nevertheless, even though these two benefits may be counter, they are designed for children's best interests. The detailed approaches may vary. However, the ultimate legal benefits protected by the ICO ADC stay fixed.

E. Data Protection Impact Assessment

Data protection impact assessment (DPIA in abbreviation) is a process targeted at reducing the data protection risk while providing information society services. The ICO requires that DPIAs be carried out if the service is likely to lead to high risks to individual interests. If the service provider cannot mitigate the risk, ICO must be consulted about the issue.[29] DPIAs are not designed only to block compliance risks for ISS providers. They aim at preventing the potential for social and economic disadvantages as well. [30] It should be noted that DPIAs are compulsory under certain circumstances and may also be regarded as the successors of PIAs (Privacy Impact Assessments). Therefore, ISS providers who had previously conducted PIAs may alter the past assessments to fit them into the present compliance framework.

ICO has listed 13 situations in which DPIAs should be conducted on its official website. These include 'using systematic and extensive profiling', 'monitoring publicly accessible places on a large scale', 'processing biometric or genetic data', etc. The 13 situations mentioned above may be roughly categorized into the following types: (1) providers are trying to process data

[29] Data Protection Impact Assessments (DPIAs), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/ (last visited Feb. 19 2023)
[30] Id.

on a large scale; (2) the data to be processed is sensitive or closely related to data subjects' health and safety; (3) the data processing will be carried out without notifying the subjects. Therefore, adopting DPIAs can be considered a precaution for possible future breaches, preventing substantial deprivation of subjects' data rights from emerging.

A complete set of DPIA is comprised of the nine steps listed in the table below[31]:

Steps	Brief Intro	Requirements
1	Identify the need for a DPIA	The processors should indicate the purpose of data processing and clarify the types of data to be involved in the procedure.
2	2-1 Describe the nature of processing	In sub-step 2-1, the processors must reveal the data processing details. These details usually include the source of data; data sharing; the collection, use, storage, and deletion of data.
	2-2 Describe the scope of the processing	In sub-step 2-2, the processors should reveal the nature of the data to be worked on, including whether it is special or criminal offense data. In addition, critical information, including the quantity, the frequency of data collection, the storage period, the number of affected subjects, and geological coverage, are emphasized.
	2-3 Describe the context of the processing	In sub step 2-3, the relationship between processors and data subjects is critical. The processors shall reveal individuals' control over their data, the possible existence of vulnerable group of individuals, the public concern on the technology involved throughout the process, etc.
	2-4 Describe the purposes of the processing	In sub step 2-4, ICO intends to guide ISS providers clarify the ultimate intention of data processing and the benefits.
3	Consultation process	This step is intended by the ICO to learn how the processor is going to communicate with stakeholders and about whether other parties will be involved in the process.
4	Assess necessity and proportionality	As is universally recognized that personal data can only be processed based on necessity, this step requires processors to set forth the legal basis for the use of data and explain whether there exist alternative methods. Meanwhile, the ICO questions data processors how they are going to respect individuals' concerning rights in pursuit of proportionality.
5	Identify and assess risks	In step 5 of DPIAs, data processors are required to reveal the source of risk and the potential impact on individuals. More

[31] This table is summarized according to the DPIA template issued by the ICO. This table is abstracted from the original template; to find the original version, please refer to the official website: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf (last visited Feb. 19 2023)

		specifically, the risk is assessed from three dimensions: likelihood of harm, severity of harm and overall risk.
6	Identify measures to reduce risk	Apart from reminding the ICO (if necessary) and data subjects about the possible risks, ISS providers should go to lengths to mitigate the risks mentioned in Step 5. Simultaneously, the effect and residual risks of options to reduce risks shall also be included in the DPIA report so as to evaluate whether processors have fulfilled their obligations to minimize risks.
7	Sign off and record outcomes	Step 7 is a procedural step which requires processors to record the DPO advice; whether the advice was accepted or overruled and the reason for it; and the consultation response.
8	Integrate outcomes into plan	The outcome of the DPIA should not be separated with the practice. Therefore, DPIA outcomes shall be integrated into the project plans. Furthermore, ISS providers shall identify any action points and make sure they are implemented.[32]
9	Keep under review	As requested by the ICO, the aforementioned DPIA steps shall be cycled through until the plans are finalized. [33]

As far as the aid of transparency and accountability is concerned, data processors are encouraged to publish the DPIA outcome. In this way, data subjects may learn when, where, why, what, and how their data will be used, transferred, or deleted, allowing users to make prudent decisions on whether to accept the service. Reasonable as the publication can be, the openness of DPIA outcome is not mandatory. ISS providers may refuse to publicize their report and analysis because they intend to keep possible residual risks confidential. However, as the author understands, the refusal to open up DPIA reports may bring other disadvantages for data processors. For example, compared with those who choose to publish DPIA reports, others may not be trusted alike. Therefore, users may choose more transparent services, contributing to their eventual benefits.

Another problem with DPIA is whether ISS providers are required to submit the outcome of the assessment to the ICO. As the ICO maintains, processors do not always oblige to submit. If data processors identify high risks they cannot mitigate, then ICO must be consulted before the process starts. After the request for consultation is submitted to the ICO, the office will issue written advice within 8 or 14 weeks to warn service providers not to process or even ban the processing.[34]

[32] See How do we do a DPIA? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how13 (last visited Feb.19 2023)
You must integrate the outcomes of your DPIA into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project-management process to ensure these are followed through. You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalized.
[33] Id.
[34] Id.

In addition, as required by Article 35(4) of GDPR, ICO shall publish a list of processing operations that require a DPIA. The aforementioned regulation includes ' the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.', which means that if the ISS is likely to be accessed by children, the operator should conduct a DPIA. In conclusion, information society services accessible by children, on most occasions, have to carry out DPIAs on the ground that children's best interests are of first priority.

III. PRACTICES OF TECHNOLOGY GIANTS IN CHILDREN'S PRIVACY PROTECTION

In response to the strict regulation of data compliance regarding children's privacy protection, several technology giants, Apple, and Google, to name just a few, have adopted measures to set forth privacy policies particular for children. However, tech corporations targeting different services are burdened with different responsibilities. Therefore, the author finds it necessary to look into the differences and similarities among different technology giants' children's privacy policies. In this part of the article, privacy policies for children issued by five corporations, Microsoft, Apple, Twitter, Instagram, and TikTok, will be analyzed and compared in depth. Afterward, a conclusion can be reached from the analysis and comparison results.

A. Microsoft and Apple

In Part A of this section, I would like to compare two corporations whose market domain consists of both hardware devices and software. Microsoft and Apple are two of the biggest companies dominating the world's technology market, and both have developed a relatively mature privacy protection system. Hence, their products can meet the requirements of data compliance in most jurisdiction regions worldwide.

Microsoft issued its latest version of the privacy policy for young people (the equivalent of children's privacy policy) in March 2023. As introduced by Microsoft, this policy targets helping young people understand how to use Microsoft products in a way that protects their privacy. In addition, the policy also stresses information that can be essential to parents and guardians of children.[35] Generally, this policy is comprised of eleven parts in all, which includes: (1) personal data to be collected; (2) the usage of personal data; (3) advertising; (4) parental consent and control; (5) resources for young people and families; (6) access and control of personal data; (7) using Microsoft products at school; (8) data safety; (9) personal data sharing; (10) the place where data is kept; (11) the period of data storage. Among which, several items can be applied not only to Microsoft services but also to other ISS providers.[36]

As for Apple, the Family Privacy Disclosure for Children provides its young users with a set of privacy protection mechanisms that differs from that of Microsoft on a large scale. As I will discuss, the children's data privacy policy centers on children's Apple IDs, enabling it to become one of the most distinctive characteristics. The Family Privacy Disclosure for Children is made up of ten parts, namely (1) Introduction to children's ID; (2) Controls for parents; (3) Screen time; (4) Restrictions; (5) Family Sharing and Ask to Buy; (6) Creating Your Child’s

[35] See Privacy for young people, last undated March 2023, https://privacy.microsoft.com/en-us/young-people (last visited March 7, 2023)
[36] Id.

Apple ID; (7) Collection of Information; (8) Use of Information; (9) Disclosure to Third Parties and (10) Consent to Apple's Collection, Use, and Disclosure of Your Child's Information.

Parental consent and control, data sharing or disclosure, collection, and use of data can be found in the privacy policies issued by both corporations. As far as the four aforementioned types of elements are concerned, the latter three can be found in privacy policies for adults as well, indicating that only parental consent and control are targeted at children exclusively. This is in line with the previous analysis on the ground that parental consent is the prerequisite for children's privacy protection.

As Microsoft states in 'parental consent and control', parents and guardians of children can create a Microsoft family account regardless of the place of residence. By way of the family account, what children are allowed to do via the account can then be determined by their parents or guardians. In general, the two main functions of this design are to help children get into good digital habits and enable children to explore the Internet world safely through content filters.[37] The former one sets limits on the devices adequate to use, the applications and games that children are accessible and the screen time. When a child's account runs out of time available, his or her parents shall be in place to decide whether additional time should be granted or else to cultivate children's manners. Furthermore, parents will be able to monitor the online activities through the family account as well, providing them with better insights into their children's usage of Microsoft applications. While the formerly designed aim is intended to restrict screen time on most occasions, the latter lays more emphasis on the contents accessible by children. In pursuit of safe online spaces, Microsoft advises supervisors to set content filters to eradicate improper content and games from children's reach. On condition that kids use Microsoft Edge on Xbox and Windows, inadequate websites shall also be banned.[38]

To exercise control over children's Internet access, Microsoft suggests that parents or guardians choose a parental control app to monitor their children when they are playing games or browsing websites. Effective control apps often serve the following five purposes: filtering inappropriate content, enforcing screen time limits, monitoring activities, blocking content, and creating activity reports.[39]

A similar mechanism exists in Apple. However, Apple itself boasts special features. Instead of setting up family accounts, children are eligible to set up their own Apple IDs. As demonstrated in the Family Privacy Disclosure for Children, children may keep a close connection with their families, such as data and document sharing, schedule sharing, etc. As far as the essential requirement of 'consent' is concerned, as I will discuss, Apple provides its users with a clearer insight by noting parents' consent of Family Privacy Disclosure for Children (referred to as 'Apple Disclosure' in this article) is the prerequisite for the successful creation of children's Apple IDs. Besides, the consent may be verified through additional steps in order that Apple would fully comply with COPPA or similar laws in other jurisdictions.[40]

---

[37] See Microsoft Family Safety, https://www.microsoft.com/zh-cn/microsoft-365/family-safety?ocid=family_signin&rtc=1 (last visited March 8, 2023)

[38] Id.

[39] See Choosing a parental control app that works for you, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/choosing-a-parental-control-app (last visited Mar 8, 2023)

[40] See Family Privacy Disclosure for Children, https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ (last visited Mar 8, 2023)

In order to create an Apple ID for your child, we must first obtain your consent to this Family Privacy Disclosure for Children ("Disclosure") and to Apple's Privacy Policy, which is incorporated herein by reference. If there is a conflict between Apple's Privacy Policy and this Disclosure, the terms of this Disclosure will take precedence.

Nevertheless, such expression is not that evident in the policy issued by Microsoft, contributing to the conclusion that Apple has paid more attention to the consent of parents and guardians.

But how do Apple IDs for children under 13 (in US.) associate with their families? Apple explains that the children's Apple IDs cannot be independent of family, and family members are also not in the position to remove children from their family accounts until they are deleted or moved to another family account. In this way, the Apple IDs for children resemble those of Microsoft to a certain extent.

More importantly, Apple stated that its 'Disclosure' does not apply to any data collection practices of any third parties. As I maintain, this term can be of pivotal importance to such giant corporations as Apple because it provides brilliant platforms allowing third-party developers to post its apps. However, on condition that the third-party apps shall breach the regulations concerning privacy protection, the platform itself can be burdened with liabilities for inadequate supervision. In this regard, declaring its independence from third-party apps may be a sensible approach to avoiding possible penalties. On these occasions, it is the third-party app developers themselves that should pay attention to privacy protection and data compliance.

Besides screen time control, adult users of Apple are entitled to exercise control over young people through 'family sharing'. The 'Ask to buy' feature allows adults to review and approve the request of purchase and download of apps and in-app purchases, allowing parents to decide what apps kids will access. However, Apple noticed that purchases completed through methods other than iTunes or App Store might not apply to this function.[41]

As for screen time limits and restrictions on accessible types of apps, it is mostly the same as those of Microsoft. Therefore, I will not stress them once more.

In addition to the consent and control of accessible Internet services, other sections included in the privacy policies issued by Microsoft and Apple may also be intriguing. Regarding advertising, Microsoft announced that it would not demonstrate personalized advertisements to those under 18. This is to say, those under 18 will not receive ads that are presented based on the analysis of their online activities. Nevertheless, it should be noted that the threshold for personalized advertisement is 18 instead of 13 or similar age standards in other jurisdiction areas.[42] Therefore, hereby, I conclude that Microsoft's protective measure against possible risk aroused by characterized advertisements outweighs its protection against immature consents made by children. Regretfully, in the Apple Disclosure, Apple Inc. didn't include content of this sort. However, its credibility may lie in the superiority of Apple's operation systems' encapsulation, minimizing the possibility of violations in this respect.

As a corporation boasting hardware devices, operation systems, and software (applications), Microsoft also provides unique resources for young people and their families. These resources cover a variety of fields, from OS (windows) to browsers, from software for office (like Word and PowerPoint) to entertainment apps (Xbox).[43] In this article, I will mainly focus on Windows and Microsoft Edge, the popular Internet browser. Admittedly, the privacy policy for Windows itself can be defined as refined. However, few contents concentrate on children's protection. Cortana, an AI productivity assistant embedded into Windows, may harm

[41] Id.
[42] Privacy for young people, Last updated March 2023, https://privacy.microsoft.com/en-us/young-people (last visited Mar 9, 2023)
[43] Id.

kids if the talks between kids and the AI are accessible by other parties. It is understandable that young people may be unaware of the characteristics of artificial intelligence and may neglect the possible negative consequences it can contribute to. Whereas Microsoft indicates that it doesn't allow kids who are too young to access Cortana and measures are taken, neither has it clarified the age appropriate to use nor has it set forth the mechanism adopted to recognize the age of users.[44]

Comparatively, more protective policies are targeted at children when it comes to Edge. According to the official website, this browser has a built-in Microsoft Defender SmartScreen, protecting users against phishing or malware websites. Indeed, this feature is essential to everyone, but it is of primary importance for children since they are more vulnerable to malicious websites for lack of discernment. The 'shield' Edge possesses for special care of children's privacy safety is 'Kids Mood'. Parents or guardians may switch on the Kid's Mood, and this procedure won't be necessary to repeat since this mood will be activated whenever the browser is opened. However, children will be unable to switch the mood off since this operation requires inserting passwords. As introduced by Microsoft, passwords to exit kid's mood are the same as those of unlocking the computer.[45] In this regard, I propose that this mood can be altered for the better by differentiating the passwords of existing kids' mood from those unlocking the computer accounts. Shall children be allowed to log in to accounts independently or use the offline functions of computers without the supervision of parents, it is necessary for them to remember the passwords, disabling the restricted access to exit kids' mood.

Although one of the snapshots of kids' mood demonstrates that this mood is aimed at children whose ages range from five to twelve, which is in line with the practice in hosts of regions, this browser still failed to indicate to whom this mood shall be applied. The age-appropriate design of Edge is special in that children aged from 5 to 8, and those from 9 to 12 are entitled to different Internet resources. More specifically, even though they are only authorized to access resources under 'Strict Microsoft Bing SafeSearch, ' the elder ones will be provided with more interesting but safe content. In contrast, the younger ones will be blessed with more simplified browsers.

As the author maintains, the practice of Edge fully demonstrates how parents or guardians should supervise children's online behavior and provide kids with an age-appropriate online atmosphere. With the help of kids' mood, both children's due freedom and parents' power to consent are respected. Whereas aforementioned defects may exist, their merits and progressiveness shall not be ignored.

When it comes to the disclosure of information to third parties, Apple has provided a detailed introduction by illustrating the following aspects: family sharing, strategic partners, service providers, and other types of parties.[46] According to the 'Apple Disclosure', the purchase information, calendars, reminders, and photos may be shared among family members subject to the restrictions set by guardians and parents. Meanwhile, Apple warns that information of this kind may be accessed by unwanted people when children's Apple IDs are

[44] See Cortana and privacy, https://support.microsoft.com/en-gb/windows/cortana-and-privacy-47e5856e-3680-d930-22e1-71ec6cdde231 (last visited Mar 9, 2023)
[45] Learn more about Kids Mode in Microsoft Edge, https://support.microsoft.com/en-us/microsoft-edge/learn-more-about-kids-mode-in-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd (last visited Mar 10, 2023)
[46] See Family Privacy Disclosure for Children, https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ (last visited Mar 8, 2023)

logged on to devices in possession of third parties.[47] Under this circumstance, it is parents that should be cautious of the possible leak of information and potential negative consequences.

In addition, Apple acknowledges that it may share children's information with service providers to serve the purposes of assessing young customers' interests, conducting customer satisfaction surveys, fulfilling customer orders, etc. Meanwhile, Apple has also promised that these providers are obliged to protect children's information. From the author's point of view, this data sharing can be doubtful on the ground that deeds such as conducting satisfactory surveys among children may breach the principle of minimum necessity. Additionally, the 'Apple Disclosure' hasn't indicated whether or how the children's supervisors may consent to the sharing of data. For lack of solid proof, I cannot conclude that disclosure between Apple and service providers may incur legal liabilities, but as I maintain, it is sensible if due attention can be paid to obtain parents' consent since children may not be aware of the consequences of allowing their information to be accessed by third parties.

Apart from sharing among family members and service providers, Apple has claimed that it may also transfer children users' information to strategic partners so as to improve its products and services or share kids' information when necessary. For the latter situation, Apple has mentioned that these circumstances include requests by law, legal litigation, public authorities or simply to complete a transaction.[48] Sharing information of this sort, whether the subjects are children or not, shall not lead to debates so long as the information subjects (children and their parents if necessary) are informed.

Above all, Microsoft and Apple serve the purpose of demonstrating how modern tech giants process children's data and what aspects they lay emphasis on. With the worldwide advent of strict regulation on children's privacy policies, corporations like Microsoft and Apple should be careful with every single product, from hardware to application. Through the analysis above, I admit that Microsoft has established a comparatively refined protective mechanism for children by providing 'kids mood', enabling parents to look over their kids' online behavior. However, as GDPR states, children should be granted due freedom to make decisions that they are able to fully understand. It is apparent that Microsoft has failed to follow this requirement as far as 'kids' mood' is concerned. Therefore, the extent of freedom to which children should be provided when they're discovering the Internet world is deemed as one of the critical problems that browser developers should think over. Problems of such kind may also appear in Apple's privacy-protective methods designed for children. As I understand, this can be a universal issue due to the technical difficulty in identifying children's ages, and the opaque and differed regulation among jurisdiction regions. To change the situation for the better, mutual efforts in technological advancement and clarity of legal regulation are necessary. Despite existing defects, including the aforementioned ones, the protective mechanism set up by Microsoft and Apple can still be regarded as progressive since they have set up examples for browser and application developers as well as hardware device manufacturers. Corporations possessing combined businesses can develop more comprehensive children's privacy protection systems since there will be comparatively fewer challenges in internal information transferring, and it's also likely to encounter conflicts between policies proposed by multiple operations.

B. Twitter and Instagram

[47] Id.
[48] Id.

Twitter and Instagram are two of the most renowned and widely used instant communication services worldwide. It is known to all that operators of these social network platforms may easily store or work on users' data, to analyze the active period of users, to look into the social circle of users with different characters, for instance. Whereas young children may be unable to identify the risk of their information's giving off to service providers, they can fall victim to target advertising and other potential hazards caused by privacy deprivation. Therefore, as I set forth, children should at least be capable of recognizing these risks until they are allowed to access these media. This article hereby will focus on how Twitter and Instagram design their privacy policies to meet the requirements of regulations in various jurisdiction regions.

Twitter did include content regarding children in the latest version of its privacy policy. However, by far can it be regarded as a detailed one. Article 5 of 'The Twitter Privacy Policy' contends that their services are not designed for those under the age of thirteen, and users must reach the ages allowed to consent to the processing of personal data.[49] It is apparent that the effort Twitter has devoted to protecting children's privacy mentioned above is not adequately in line with UK GDPR or similar regulatory requirements. Concluding Article 5 of the policy, Twitter, in essence, intends to ban children under 13 and those unable to give individual consent to enjoy their services. But it is worth noticing that no further details concerning how Twitter is going to prevent children under the age of 13 from accessing this platform, putting Twitter under related legal risks.

Despite there may exist apparent defects in Twitter's written form private policy for kids, its effort to obtain parental consent should be recognized. Twitter warns that accounts may be temporarily locked on the condition that the users may not meet the requirement of minimum ages. Under this circumstance, Twitter require that users' parents provide their identity information, their relationship with users, guardianship information, and more importantly, they have to agree on their children's access to Twitter.[50] Twitter also informs guardians that they are allowed to withdraw their confirmation on children's access on the same website page.

As for how Twitter may judge whether its users reach the minimum age of 13, it is essential to look into the registration process. Twitter provides its users with three approaches: register via Apple accounts, via Google accounts or create a new account with name, e-mail, and birth date.[51] The system will verify whether the user is appropriate to access Twitter services based on the date of birth filled in by the applicant. However, I doubt how Twitter is going to pick out those who have made false presentations at their ages.

Above all, the general method Twitter has adopted to comply with regulations concerning children's privacy protection is to prevent underage children from accessing their services. In this way, there's no further need for Twitter to refine its policies specially designed for children. Judging from the effect, Twitter's approach seems effective for in the past few years, it has been involved in a few lawsuits concerning violation of children's privacy.

---

[49] See Twitter Privacy Policy, https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-aug-19th-2021/Twitter_Privacy_Policy_EN.pdf (last visited Mar 11, 2023)

[50] See Request Review, https://help.twitter.com/en/forms/account-restoration/parental-consent (last visited Mar 11, 2023)

[51] The three methods mentioned in this passage is based on the author's experiment with iMac (M1, 2021) on March 11, 2023. There can be other approaches if similar experiments are conducted with Android devices.

Unlike Twitter, Instagram provides more detailed regulations on this issue. Basically, Instagram banned children below 13 from registering for an account and anyone who has reached 13 is considered an authorized account holder.[52] Therefore, parents and guardians are denied access to their kids' Instagram accounts, nor will they be allowed to take any action on authorized accounts. However, parents are still able to report to Instagram that children who are underage have successfully signed up for this service. Parents' denial to access their children's accounts may bring to our alert for, in many regions, children above 13 are still not capable of making consents individually, whereas Instagram generally neglects this situation.

It seems that Instagram has noticed the necessity of parental involvement in children's use of this service for Instagram has provided 'A parent's guide to Instagram' ('Instagram Parent's Guide' in brief) in various languages on its official website. As introduced by Instagram, this guide focuses on managing privacy, interactions, time, and security on Instagram. Additionally, open conversations between parents and teenagers on this topic are encouraged.[53] The following paragraphs will mainly emphasize how the 'Parent's Guide' instructs parents to supervise adequately.

This guide has been generally designed to help kids be smart and kind in their online digital habits.[54] In the first place, Instagram Parent's Guide introduces that Instagram's existence is to bring people together through passions and interests by way of sharing photos, videos and messages. Among all the instructions that Instagram wishes to bring parents to, this guide introduces the differences between the private and public mood of services in the first chapter. Instagram suggests that parents encourage their children to adopt a private mood so that only those following their children can view these young people's updates on their accounts, providing them with sufficient privacy protection. The preference for privacy mood recommendation is followed by the control of messages. As Instagram's parent's guide stresses, the ease of interaction among users is one of the social media's most outstanding points. However, interactions containing harmful content may also give rise to cyberbullying. Therefore, by reporting to the service providers, Instagram encourages parents to educate their kids in posting positive content while braving toxic content such as discrimination and hate speeches. Furthermore, comment columns are what Instagram considers to be pivotal in order to provide children with proper online spaces. In this regard, Instagram has provided parents with ample information concerning the management, filtering and warning of comments in the hope of parents' guidance of their kids. Not only do these guides include what to do with offensive comments and how to set restrictions on commenting, but also how young users are able to manage bulk comments at one time.[55]

Unlike the approach accepted by Microsoft and Apple, Instagram sets no compulsory limits on screen time. Instead, it encourages parents to reach agreements with their children on the appropriate amount of time to be spent on the platform. Specifically, Instagram set forth three aspects that could contribute to the cause: firstly, enable children to be aware of the time spent on the app by showing the average screen time; secondly, encourage children to participate in activities without digital devices; lastly, agree on a period of time regularly during

[52] See Tips for Parents, https://help.instagram.com/154475974694511/?helpref=hc_fnav (last visited Mar 11, 2023)
[53] Id.
[54] See A Parent's Guide to Instagram, https://scontent-hkt1-1.xx.fbcdn.net/v/t39.8562-6/10000000_383976253354575_5551535427345148474_n.pdf?_nc_cat=109&ccb=1-7&_nc_sid=ae5e01&_nc_ohc=1O_ByDjITbkAX_r7LwC&_nc_ht=scontent-hkt1-1.xx&oh=00_AfAAxUXEv8Lec_QDPx5fUOBF9K1FycyuI-qPR2rfGyQqWQ&oe=6410CBD8 (last visited on Mar 13, 2023)
[55] Id.

which family members switch off their digital devices to improve communication offline. It seems that these approaches can be practical, especially for those kids who are taking form of their digital habits. In contrast, I reserve my opinion on this part of the guide in that Instagram may have shifted the burden of responsibility to protect children users to their parents in seemingly lawful ways.

The reason why the aforementioned guide is looked into in detail in this note is that this can be regarded as an innovation put forward by Instagram. But I have to clarify that the innovative characters are not equivalent to the conclusion that Instagram outperforms other similar applications as far as children's privacy protection is concerned. In essence, the Instagram Parent's Guide is merely an advisory brochure, without producing any legal effects. This indicates that parents are still not in a position to supervise their children who are above 13 and children may be allowed to make consent on items that require permission from parents if they choose to use other media platforms. Therefore, the legal effects of 'Instagram mood' is questionable.

It was due to Instagram's ignorance of the regulation of children reaching 13 years old that led it to negative legal consequences. This can be exemplified by Irish Data Protection Commission's fining Instagram for violating the privacy of children and adolescents in late 2022. This penalty was decided according to GDPR (EU), and the fine reached 405 million Euros on the ground that Instagram had allowed users between the ages of 13 and 17 to operate business accounts on the platform that displayed users' phone numbers and email addresses.[56] Although this case is not that closely related to parents' consent on adolescents' online behaviors, it fully serves the purpose of demonstrating the existing method taken by Instagram is not refined and adolescents aged from 13 to 17 can still be regarded as 'children' under certain regulations.

C. TikTok

Going back to the Introduction part of this note, it is meaningful to look into TikTok's children's privacy policy in that it well reflects how live stream media service providers design policies in this respect. This part of the analysis is based on the version updated on January 1, 2023.TikTok Children's Privacy Policy is comprised of six sections: (1) What Information We Collect from Children; (2) How We Use Children’s Information; (3) How We Share Children’s Information; (4) Data Security and Retention; (5) Rights and Choices and (6) Privacy Policy Updates.[57]

As I maintain, there may be confusion about TikTok's attitude towards young users in that the two types of privacy policies, for children and parents, respectively, contradict each other to a certain extent. On the one hand, the general privacy policy states in 'Children and Teens' that TikTok is not directed at children, and shall the personal information be collected from a child be noticed by the platform, the information will be deleted, and the account will be suspended by TikTok.[58] However, TikTok hasn't explained the definition of children mentioned above yet. In addition, this platform has asked users to report via a link if children under the age of 13 are found to be TikTok users. If users click on the link, another page named

[56] See Ecuador: Instagram Fined 405 Million Euros For Violating The Privacy Of Children And Adolescents, https://www.mondaq.com/privacy-protection/1239506/instagram-fined-405-million-euros-for-violating-the-privacy-of-children-and-adolescents (last visited Mar 13, 2023)
[57] See Children's Privacy Policy, https://www.tiktok.com/legal/page/global/privacy-policy-for-younger-users/en (last visited Mar 13, 2023)
[58] See Privacy Policy, https://www.tiktok.com/legal/page/us/privacy-policy/en (last visited Mar 13, 2023)

'Submit a request' will appear. But as the author operates, this webpage includes only columns that collect the reporter's personal information and a column that allows the reporter to upload files, without mentioning the possible results of this report. But on the other hand, Children's Privacy Policy claims that the special version of the policy is committed to protecting the privacy of children.[59] Specifically, this policy clarifies how the platform collects, uses, shares, and otherwise processes the personal information of children under 13.[60] It seems that the TikTok Privacy policy has gone to great lengths to prevent children, even though the definition here is unclear, from accessing TikTok services; but the TikTok Children's Privacy Policy specifies TikTok's processing of youngsters' personal data. Since the two policies are valid simultaneously and can both be found on the official website of TikTok, I hereby reach the conclusion that there may exist a contradiction between TikTok's multiple privacy policies, and therefore, it remains unsettled whether children under 13 are allowed to access this platform and what special precautions or protective mechanism are set forth for the sake of children's privacy protection.

In pursuing the purpose of having insight into TikTok's children's privacy policy, the above-mentioned contradiction can be set aside temporarily. As far as the types of information collected from children's accounts are concerned, TikTok does not collect such information as detailed location as they do to normal users.[61] That is to say, TikTok mostly collects children's information out of necessity. Secondly, when it comes to how the platform uses and regulates children's private information, TikTok proposes that it will use it only for providing and supporting its own services and it will not allow children to publicize their personal information. However, TikTok stresses that it may use children's information to provide personalized contents, which indicates that there may exist automatic analysis directed to children. Thirdly, as TikTok introduces, the information collected may be shared with service providers so that internal operations of the TikTok service can be maintained. This method of sharing is common in recent tech corporations' practice and can be deemed as a rather safe approach on condition that local regulations or laws do not exert specialized requirements.[62] Moreover, TikTok has realized the risk of data leaking due to the unavoidable possibility of information transmission via the Internet. In response to the risk, TikTok proposes that it has appropriate measures to minimize the risk and the information will be stored only for the necessary period of time.[63] This part of policy, seemingly effective to children's privacy protection, cannot be regarded as indicating substantial advancement made by TikTok in this respect and it is, in essence, a repetition of concerning regulations (such as GDPR), as the author points out. Finally, what rights are parents granted are included in this policy? Despite the fact that what the term 'children' refers to is still not clear, parents are permitted to submit a request to know, access, delete, or correct the information collected from their children by TikTok.[64]

Summarizing the contents provided above, TikTok hasn't brought us much unique information regarding children's privacy protection except for the requesting mechanism that allows parents to supervise their kids' information collection and usage. In addition, the introduction of feedback on request can be adapted to many other applications as well. Admittedly, the present version of children's privacy protection policy remains to be specified

[59] Id. at 49.
[60] Id.
[61] Id.
[62] Id.
[63] Id.
[64] Id.

in that the subject to which the guidelines aim should be further clarified and the current contents are remotely connected with the characters of TikTok which features live stream media. Therefore, as the author considers, TikTok Children's Privacy Policy is more a combination of requirements set forth by legal authorities than a document being specified notice to users' attention.

D. Analysis

By examining the ISS services discussed above, the author hereby provides the following analysis:

I. Generally, the age of thirteen is a distinction standard for 'children', which means that a number of applications, such as Instagram, should not be accessed by young people who are less than 13 years old. However, this standard gives rise to different attitudes towards this group of children among service providers. Some providers grant parents and guardians of children to look over their kids' online space so that they may give consent when necessary or block offensive and negative behaviors and content for young users. This, in fact, is the requirement of regulations in certain jurisdiction regions, GDPR, for instance, when children are not mature enough to make individual consents. On the other hand, ISS providers may claim that so long as a child reaches thirteen, they should be deemed as an individual granted the full ability to access any services provided. In this regard, parents and guardians are in no authority to restrict children's access to full content or give comments. Such is the case with Instagram, but its defects can also be apparent: shall regional legislation require parental consent for children of 14 to 17 years old or protections different from that of adults' apply, negative legal consequences may arise.

II. The approach multiple ISS providers take to verify the users' ages varies as well. While several services looked into in this note haven't indicated how this verifying process is carried out in their children's privacy policies, several others inquire about users on their birth date so as to judge whether they are eligible to access the services. However, it is unneglectable that false information, whether deliberately provided or not, leads to the ineffectiveness of this mechanism. Therefore, in this regard, hosts of ISS providers have set up accesses to enable users to report clues when they discover unqualified users' attempts to enjoy the services. It is true that this method prevents young kids from taking advantage of applications that they shouldn't have accessed, but on no account can it be seemed as reliable for the report from adults can be random and incomplete. Referring to what Chinese game developers have done in the past few years on the same issue when it has been ordered that individuals under the age of 18 shall not spend over an hour on games on weekdays and three hours on weekends. To comply with the regulatory requirements, Chinese game developers request the users to provide their Identity Card numbers and adopt other technologies, such as biological verification, to guarantee that children's screen time is controlled. This can be a way out of the trouble, but it can also be a challenge for service providers because the introduction of ID verification requires refined data storage and protection systems, adding much to operating expenses.

III. For service providers boasting versatile areas of businesses like Apple and Microsoft, they tend to associate children's accounts with parents' accounts or family accounts so that parental control can be exercised. This can be essential for giant corporations whose businesses expand widely for excluding children from their customers may result in unwanted consequences. In fact, the combination of a hardware device, operation system and applications enables such providers to construct their privacy protection framework better. When young users try to sign up for services only available for adults, it is unnecessary for the apps

embedded into the OS to verify their identity since the information needed can be drawn from the family or parent account associated with these devices and OS. Moreover, parental supervision has been made more accessible since parents and guardians can access the browser history or online activities of children's accounts on their own devices since the information transformation should not be confronted with technological obstacles nowadays. Furthermore, the ample amount of funds possessed by service providers of this kind also entitles them to build up a more comprehensive and consistent system of children's data protection, eradicating the possibility of negative legal liabilities in the long run.

IV. Based on the aforementioned research into children's privacy policies, it is discovered that multiple corporations have included the following items in their policies: the users their services are directed to, parents' role in their children's accessing services, and how the children's information is collected, used, shared, as well as stored. However, a distinctive feature shared among these policies is that they seldom integrate the policy with their services. Taking TikTok as an example, although it has already notified its users of the sorts of information to be collected and used, little has it mentioned how the automatic suggestion works and what possible influence it will have on young users. In fact, the issue of automated algorithms and decisions is given priority nowadays for its involvement in artificial intelligence.

V. Based on the research mentioned above, the author predicts that public involvement may play a more frequent role in protecting children's privacy. Public adult users have now been encouraged to report clues indicating ineligible individuals are accessing certain services, and parents have been asked to report offensive or improper content when they discover it. These measures do help in mitigating the pressure exerted on ISS providers. However, as maintained before, public involvement cannot be regarded as the last resort since public users are not the subjects burdened with the liability to supervise the online environment. In essence, who should shoulder the responsibility remains unchanged, while corporations can still amend the present children's privacy policy for the better.

IV. CHANGING DPIA FOR THE BETTER

Now that we've learned how the aforementioned tech giants provide specialized care for children's privacy protection for the time being, we may conclude that at least presently, there has been no consensus on what ISS providers should do to avoid possible breaches of privacy protection regulations for kids. As is discussed previously, DPIA is not compulsory unless the service is hazardous, leading to the consequence that ICO may only be able to get a knowledge of a limited portion of service providers. This is equivalent to the fact that hosts of companies may be found to have breached the regulations only after the happening of hazardous consequences. Additionally, there can also be a number of service providers who have also breached the rules but are left undiscovered due to ICO's ignorant of their children's privacy policies. Provided that ICO has access to all providers that should submit DPIA reports, it can still be challenging for ICO to fully regulate on the ground that merely opaque guideline in filling the DPIA form has been provided for the ISS corporations. To change the situation for both regulators and ISS providers for the better, hereby, the author proposes the following guideline for reference.

A. About the Access of Children

Before clarifying whether children are the targeted customers of this information Society Service, service providers may first determine what 'children' refers to in line with local

regulations. British, for instance, mostly regard those under 13 as individuals who should be taken special care of since they are not allowed to make consents without parental control.[65] It should be noticed that what matters in the field of privacy protection is not whether an individual is able to bear legal liabilities fully but to what extent he is able to decide on his online activities. Going back to the current practice in the UK, whoever under 13 making a consent should be accompanied by parental consent, indicating that an adequate verification of age that fulfills this purpose is necessary. Nevertheless, ICO also requires that child should understand what they are consenting to. For example, where usually a teenager aged 16 can fully understand the item consenting to, the ISS provider should confirm that the user reaches the higher age level to be allowed to give individual consent. In this case, it is advisable to include the classification of age groups that may make a difference in Step 2 of DPIA tests.

Now comes the issue concerning target users. As surveyed by the author, most services have indicated the user groups entitled to access the service. But admittedly, few services have disclosed their verification method of age. Should the verification be ineffective, the service developer may be confronted with legal liabilities for violating concerning regulations or laws. Provided that the service is designed for users from all age groups, the author considers it necessary to address what approach has been adopted to identify the exact age, either by face recognition, Identity card verification, or any other approach. During this process, another problem should be handled with care. It is suggested that the service provider pay attention to the potential privacy protection problems associated with the verification process. How will the identity information be stored? How long will the data be stored? Are there any precautions that prevent the data from being illegally accessed? Is it necessary to collect the data? The answers to these questions can be pivotal since they determine whether the service providers have lawfully collected information. The reply to the safety problem may be included in Step 4 of DPIA, for it is highly linked to necessity and proportionality issues.[66]

The verification approach is also unneglectable for applications requiring children to reach a certain age threshold to access. The filling-in of the DPIA form can be similar to the situation mentioned above. The only difference is whether under-age children are restricted from consent or denied access to the service.

B. About Parental Control

It is often the case that parental control exists where children under the age of independent consent are granted access to the service. As for verifying parents' or guardians' identity, I will not explain it once more since it is highly similar to the mechanism introduced in Part A. What's new is how the relationship between parents and children can be established. So far, I have seen no specialized approach designed to recognize the adult user's rights to exercise control. As I propose, it can be impractical since requiring a 'birth certification' can be

---

[65] See https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/ (last visited Mar 20, 2023)
When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.

[66] See Data protection impact assessments, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/ (last visited Mar 20, 2023)
You need to explain why your processing is necessary and proportionate for your service. You must also include information about how you comply with the GDPR, including: your lawful basis for processing (see Annex C); your condition for processing any special category data; measures to ensure accuracy, avoid bias and explain use of AI; and specific details of your technological security measures (e.g., hashing or encryption standards).

weird and may lead to other privacy problems. This can be a theoretical problem to be discussed. Still, the author concludes that it's unlikely that legal liabilities will be contributed to since the ICO code merely rules that children are not in a position to give independent consent. When qualified adults approve their consent, the service provider still complies with the regulation.

In addition, a commonly neglected issue is whether children's access to services is over-restricted. That is to say, the author suggests that ISS providers examine whether they are depriving young users of their proper passage to the Internet world. Even though it is often neglected, the requirement for step 4 issued by ICO deems the loss of autonomy or rights as a specific type of risk.[67] Therefore, the author recommends that information Society Service providers include the justification for their restriction methods to avoid potential deprivation.

The contents and screen time have always been important for services closely related to instant messenger exchanges. Technically, screen time control is easier to achieve, for it can be attached to the identification verifying procedure. However, the control of contents can be more difficult. On the one hand, the difficulty is brought by the opaque standard of 'improper' since service providers may have trouble judging whether particular contents are harmful to children. Strict supervision of the contents may lead to poor user experience, whereas otherwise, ISS providers may violate the regulations. So far, parents and guardians have been involved in the process by encouraging them to report inappropriate content or behaviors. It has to be recognized that this approach may work for parents who tend to be more cautious on this issue, but the risk shouldn't be deemed as eradicated. Therefore, explaining the risks that may arise in this field in step 5 of DPIA tests shall be essential. Some developers have introduced artificial intelligence technology to screen our offensive content for children. In this case, the autonomous characters of AI should be taken special attention while corresponding risks should also be disclosed in DPIAs.

V. COPPA AND ICO ADC

ICO ADC and COPPA are two regulations that protect children's privacy in the UK and the US respectively. COPPA, also known as the Children's Online Privacy Protection Rule, has been in place for about 25 years. Although it has not been fully discussed in this note, it is still a regulation worth studying. While ICO ADC provides guidelines to service providers to help them set policies for children, COPPA is a US law enforced by the US Federal Trade Commission (FTC). In terms of legal status, COPPA outweighs ICO ADC. Despite differences in enforcement effectiveness, both regulations share similar goals.

COPPA is comprised of 13 sections in total (from Sec 312.1 to 312.13). In the first place, the definition of 'children' can be found in section 312.2: individuals under thirteen are regarded as children according to COPPA. This mitigates the space of argument since introducing the capability of making independent consent is no longer necessary. In addition, 'parent' in US law not only includes biological and adoptive parents but also refers to guardians. More importantly, COPPA has clarified that 'obtaining verifiable consent' is equivalent to service providers' making reasonable efforts to ensure that before personal information is collected from a child, a parent of the child receives notice of collection, use, disclosure and the parent notified has authorized the aforementioned actions.[68] As I maintain, this definition displays the advancement of legislation; because compared to the ICO ADC, COPPA

[67] Id.
[68] See 15 U.S.C. §§ 6501.

explained more clearly that due notice and authorization combined could compose effective parental consent. Section 312.2 is of great importance to this act in that it lays a solid foundation for the following sections by introducing the terms that show up frequently.

Section 312.3 reflects US regulations on unfair and deceptive acts concerning personal information from and about children on the Internet.[69] S312.3 is the leading part of the following sections, for it essentially only maintained that Sections 312.4 to 312.8 should be observed, or a service provider may violate the laws. The explanation of 'reasonable' can be tricky, for it comprises plenty of requirements. Firstly, the writing of the notice should be clear and understandable. Deliberate design to make the characters of notice difficult to recognize may lead to breaches. Secondly, the notice should be directly sent to parents as far as technology permits. The contents of the notice should contain the collection, use, and disclosure of children's information and material changes to the aforementioned items.[70]

Whereas S312.4 put forward detailed requirements for notice, S312.5 set forth what composes qualified parental consent. Parental consent is the prerequisite for children's access to the splendid Internet world; its superiority is self-evident. In response to the previously mentioned issue that it's hard to identify the relationship between young users and their parents, COPPA rules that any method to obtain consent should be reasonably calculated regarding available technology. Indeed, COPPA hasn't provided a fixed standard either, but so long as FTC can prove that service providers may do better in this respect, they may bear legal liabilities in practice. As a general requirement, the COPPA regulates that service providers shall require parents to consent to disclose information to third parties, bringing the principle of minimum necessity to practice. However, there is no law but has an exception. The parental consent may step backward on condition that (1) the collection of information is aimed at obtaining consent; (2) collecting parents' information for the sake of informing them of children's online participation; (3) collecting contact information for single-time uses; (4) children and parents' contact information are collected for multiple-time requests but won't be used for any other purposes; (5) the collection of information is for the safety of children; (6) the collection of information is allowed by judicial proceedings or else, legal basis can be found; (7) collecting information for internal and continual service providing; (8) operators only collect persistent identifier while no further information is collected.[71] Based on the eight situations in which parental consent is not compulsory, I hereinafter conclude that COPPA has tried to balance the safety of children's private information and service providers' operation efficiency. Compared with ICO ADC, it is undoubtedly that the US regulation provides operators with more explicit instructions as far as parental consent is concerned.

As is discussed, parents' right to get knowledge of their kids' participation in online activities shall be limited to grant adequate space for young users. COPPA S312.6 regulates that having certified the parent's identity, parents should have access to types of information collected from children, and they are in a position to refuse future information use and collection. Accordingly, the operators shall terminate the service provided on request.[72]

Under Section 312.11, COPPA has introduced the so-called 'safe harbor program' to the children's privacy protection field. This program, with no parallels in regulations such as ICO ADC, allows industry groups to apply for approvals of self-regulatory program guidelines

[69] Id.
[70] Id.
[71] Id.
[72] Id.

on condition that the protection standard promised by the proposed guidelines are substantially analogous to COPPA requirements, self-assessment shall be carried out, and mandatory disciplinary actions for non-compliance shall exist.[73]

Compared with the age-appropriate design set forth by ICO in the UK, COPPA can be regarded as more a regulatory framework than a guideline. On the one hand, instead of providing information to Internet Service providers with recommended approaches to comply with, COPPA mainly states standards and administrative procedures of privacy protection without telling operators how to reach these goals. While on the other hand, ICO ADC has gone to great lengths to give instructions on this issue. The effort devoted to DPIAs illustrates this difference, for ICO may even provide its official conclusion on the possible information risk. FTC will not supply these services in the United States. As I propose, however, COPPA provides more evident concepts and regulatory requirements when compared to the age-appropriate design in the UK. Section 312.2, which includes the definition of hosts of terms, such as 'children', 'parental consent,' etc. The illustration of these concepts eradicates the necessity to clarify legal procedures and practices further. In addition, it's impressive that COPPA has described that 'reasonable effort' refers to the most outstanding possible efforts made with presently accessible technologies. From the perspective of legal status and negative consequences, even though these two vary in compulsion, they point to similar legal responsibilities in that violation of each code results in insufficient protection of children's privacy.

VI. CONCLUSION AND DISCUSSION

With the rise of internet technology and the increasing need for young people to access the virtual world, potential dangers also arise. Digital natives may not be aware that their every move, such as registration, consent, and sharing, can lead to improper privacy disclosure, resulting in unexpected consequences. Even more concerning, information leaks in the online world can potentially spill over into children's real lives through the illegal collection of data. Therefore, it is clear that legislation on children's privacy is both necessary and urgent. In recent years, major nations have implemented regulations aimed at protecting children's privacy, whether in the form of laws, acts, or other measures. Additionally, internet service providers have developed their own privacy policies. After analyzing the efforts made by Internet service providers and regulatory practices in the US and UK, I have come to the following conclusions:

Operators of various scales tend to emphasize different aspects. For those who provide livestream or instant message services, their main business model is characterized by fast-spreading information. As a result, these corporations prioritize blocking inappropriate content to prevent it from reaching children. In addition, these types of services set strict age limits, often requiring individuals to be older than a certain age to use their platform. To prevent underage users from accessing their services, operators also introduce a reporting mechanism to detect them instantly.

Meanwhile, operators who offer a variety of services, such as Apple, may focus on data sharing among their services. Operating systems (OS) operators can provide one-stop identification for applications with users' permission for data sharing, which brings many advantages.

[73] Id.

Admittedly, mainstream ISS providers have made efforts to design the children's privacy policies that best suit their needs, the parental consent has always been an issue. In the first place, verifying parents' identities can be a dilemma. I've discovered no applications requiring users to upload or provide official relationship certification. Therefore, the 'parent' granting children's access to services may be elder siblings or even adult strangers who bear no responsibility to the children. While strict monitoring of the relationship provides children with a safer online atmosphere, operators are confronted with more significant challenges in that the consequence of unexpected and illegal data access is unaffordable and irreversible. Meanwhile, due to the complicated verification mechanism, the market occupation and economic effects are subject to suffering.

Operators have not yet developed a widely recognized standard for parental involvement when it comes to children's privacy. Some services exempt children from parental supervision once they reach a certain age (such as 13 in the UK and the US), while others believe that parents are still responsible for their children's participation as they may not fully understand the gravity of their decisions. Based on current legislation and regulations, I believe the latter approach is preferred as information security should be given priority. This brings up another issue that is often overlooked: to what extent should children be granted online freedom? While COPPA has yet to rule on this problem, ICO ADC requests that due space be provided. Therefore, there is no consensus on this issue at the legislative and practical level. Although there has been no evident sign indicating that the situation will change for the better shortly, I believe that advancements in regulation capability will help resolve this issue, as it primarily contributes to children's online experience.

Another problem worth discussing is that the latest versions of children's privacy policies are highly similar to the general ones applicable to adults. This means that the former ones also contain paragraphs introducing how information is collected, stored, shared, and disclosed. For example, storage is not a unique concern for children and there is no need to emphasize it in the privacy policies for children. It is feasible to separate the storage of children's and parents' information and keep them under different stages of security. Therefore, ISS providers need to work out a new version of a particular privacy policy that features children's unique needs to distinguish the protective measures between children and other groups of users.

Privacy protection is becoming a heated topic worldwide, but it is also becoming a double-edged sword that may be used for purposes other than protecting policy. For instance, the TikTok event has long been regarded as an approach adopted by the United States authority to restrain the development of Chinese technology, composing the puzzle of the Sino-American trade conflict. Regardless of any external factors, one idea is for sure: the protective umbrella for children's privacy should be held firmly with no exception. As kids' access to the Internet world is unavoidable and beneficial, regulators, operators, and guardians should work collaboratively to provide a safe environment for our future generations. Whatever unexpected and unwanted factors exists, we must amend the previous versions of policies and prepare them for future needs and challenges.