ON THE CONSENT MECHANISM FOR PROCESSING PERSONAL DATA OF MINORS

Chang Yusha[*]

I. INTRODUCTION

There are increasing concerns over data privacy, with information and communication technology proceeding at a rapid pace and posing intrusive challenges. Recognition of minors' vulnerability and transformation in their rights' protection occurred not far from where we stand at present. Such a combination breeds a new subject of exploring minors' personal data protection, among which the consent mechanism is highlighted.

China has introduced a comprehensive regulatory framework, including article 1035 of the *Civil Code of China*, article 31 of the *Personal Information Protection Law*, article 72 of the *Law on Protection of Minors*, and article 9 of the *Provisions on the Cyber Protection of Children's Personal Information* issued by the Cyberspace Administration of China. Legislators intended to strengthen the personal information protection of minors by empowering guardians to remedy their insufficient legal capacity. In reality, guardians' consent is deemed the golden rule for processing personal information from or about minors, and accordingly imposing uniform obligations on processors to obtain consent unexpectedly leads to the collapse of safeguards of both processors and guardians. On the side of processors, the *Personal Information Protection Law* literally requires that guardians' consent must be collected before processing minors' personal information, but remains silent on a series of unsolved issues such as ways to verify users' real age, lists of competent evidence proving user-guardian relationships and reliable methods for guardians authorizing the processing of data. In practice, lacking clear and mandatory standards and criteria for self-regulation, as well as economic incentives, many processors make little distinction between an adult and a minor on the consent procedure. As observed, they would rather

* Ph.D. Candidate at Renmin University of China and Joint Ph.D. Candidate at University of Geneva. This paper is supported by the China Scholarship Council's High-Level University Scholarship Program for Sponsored Graduate Students.

assume that guardians' consent is granted either by claiming guardians' own responsibilities to assist and supervise or alert minors to seek adults' help in their standard clauses or by users' simple ticking of the box of age range and statement of having obtained guardians' consent.[1] Guardians seldom take a serious attitude towards participating in the management of minors' data privacy, educating minors, and safeguarding them from potential risks. In addition, their interests are not always in line with those of minors, and they are not always as rational as presupposed. For instance, posting minors' photos and videos excessively on a platform to drive more traffic is not uncommon. Guardians who shoulder the primary role and responsibility of protecting minors' privacy are invisible privacy invaders and leakers.[2]

Given this reality, this article, using article 31 of the *Personal Information Protection Law* as a starting point,[3] endeavors to form a legal interpretation scheme with Chinese characteristics that is aimed at achieving optimum protection for minors under constrained conditions, coordinated with the contents and values of the *Civil Code of China*, personal information protection rules and other regulations, and compatible with international legal practices and trends. The second section sorts out core interest conflicts when implementing the guardian's consent rule and introduces an analytical framework by summarizing proposals of existing research to balance those interests. The third and fourth sections follow the three-level framework and separately deal with the substantive division of processors' and guardians' responsibilities to reduce minors' residual risks with as few social costs as possible and to control adverse side effects resulting from guardians' uncertain and occasional self-serving participation, procedural enforcement of substantive requirements in the hope of maximizing minors' welfare and minimizing processors' economic burdens, and final supplementary and adaptive refinement in light of minors' fundamental rights (discussed in the conclusion). The fifth section is the conclusion.

1 Zhang Suhua & Yin Xiaokun, *Regulations on Improper Application of Guardian Consent Rules in the Protection of Minors' Personal Information*, 10(2) Shanghai Legal Studies 139 (2023).

2 LEAH A. PLUNKETT, SHARENTHOOD: WHY WE SHOULD THINK BEFORE WE TALK ABOUT OUR KIDS ONLINE, at 4 (The MIT Press, 2019).

3 Regarding article 31 of the *Personal Information Protection Law* as the primary ground of interpretation lies in two reasons: the first one is that compared with article 1035 of the *Civil Code*, it is the special law; the other one is that compared with article 72 of the *Law on Protection of Minors* and article 9 of the *Provisions on the Cyber Protection of Children's Personal Information*, it is more comprehensive for it covers not only online but also offline environment.

II. CORE INTEREST DEMANDS AND TRADE-OFFS IN APPLICATION

A. Core Interest Demands When Applying the Consent Rule

1. Minors' Physical and Mental Immaturity Call for Special Concerns. — Minors' vulnerability and the universal consensus represented by the *Convention on the Rights of the Child* (hereinafter referred to as the CRC), which enshrines the ideals of upholding children's inherent dignity and the equal and inalienable rights, serve as justifications for particular attention afforded to minors in the aspect of personal data.

The enactment of the *Personal Information Protection Law* represents a milestone in meeting the challenges of abusing and exploiting personal information and leveling the data-processing playing field. When focusing on minors, it remains to be enquired 'if existing rules and principles are sufficient to keep control of the risks exposed to minors at a reasonable safety threshold, and if not, why and to what extent their data privacy is in special danger in the digital environment as opposed to adults'. Recital 38 of the *General Data Protection Regulation* (hereinafter referred to as the GDPR) explains that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, safeguards concerned, and their rights in relation to the processing of personal data. Technically speaking, their inadequate cognitive competence is compelling support for the rationality of general protection of the family, state, or society.

From the perspective of data collection, minors tend to reveal more data because of their inferior capability to assess the benefits and risks of processing activities of certain data, as well as to take countermeasures to mitigate these risks. On the one hand, minors who have little experience and lack a basic perception of social boundaries[4] are inclined to trust strangers or even AI machines.[5] They are also emotional and vulnerable enough to be influenced and manipulated[6] in an anonymous online environment, which

4 INTERNET SAFETY FOR KIDS: HOW TO PROTECT YOUR CHILD FROM THE TOP 7 DANGERS THEY FACE ONLINE, at https://usa.kaspersky.com/resource-center/threats/ top-seven-dangers-children-face-online (Last visited on January 2, 2025).

5 UNICEF, CHILDREN IN A DIGITAL WORLD, at https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (Last visited on January 2, 2025).

6 B. J. FOGG, PERSUASIVE TECHNOLOGY: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO, at 230 (Morgan Kaufmann Publishers, 2003).

is flooded with youthful peer cultures[7] and can easily bypass the traditional parental gatekeeping role.[8] Minors are seduced or fueled to actively disclose personal data about themselves, their families, close relatives, and friends to scopes from private parties to semi-public platforms and public ones in written, oral, picture, video, or other forms. On the other hand, compared with interpersonal data sharing, the risks of passive data tracking by an invisible commercial party are much more difficult to detect because they are intertwined with complex technological practices and dispersed among data subjects, which takes years to turn into possible negative consequences or tangible harms.[9] Minors' privacy management awareness thus shows an imbalance in the above two situations as their age increases.[10]

Minors encounter special risks from the perspective of data use. First, as minors are likely to disclose more data, it will be harder to control data misuse. For example, cyberbullying, a major digital harm experienced by minors,[11] is the result of viral spread of personal information which is either exclusively distributed by a single actor or gradually combined with several fragments contributed by separate parties in the transmission chain. Second, minors, due to vulnerabilities such as inexperience, irrationality, and copy-cat habits, are easily exploited, thereby becoming perfect targets of profit-grabbers. Once data processors harvest massive amounts of information, continued profiling analysis and other technical practices can produce precise descriptions of individuals or groups, including personality, habits, preferences, and so on, on the basis of which companies employ targeted marketing strategies and recommend appropriate advertisements at the appropriate time to appropriate persons to encourage excessive consumption and purchase.[12] Other instances indicating the exploitation of

7 S. Livingstone, M. Stoilova & R. Nandagiri, *Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review*, LSE Research Online 11 (2019).

8 Charlene Simmons, *Protecting Children While Silencing Them: The Children's Online Privacy Protection Act and Children's Free Speech Rights*, 12(2) Communication Law and Policy 123 (2007).

9 S. Livingstone, M. Stoilova & R. Nandagiri, *supra* note 7, 15. *See* also GRY HASSELBALCH LAPENTA & RIKKE FRANK JØRGENSEN, YOUTH, PRIVACY AND ONLINE MEDIA: FRAMING THE RIGHT TO PRIVACY IN PUBLIC POLICY-MAKING, at https://doi.org/10.5210/fm.v20i3.5568 (Last visited on January 2, 2025).

10 S. Livingstone, M. Stoilova & R. Nandagiri, *supra* note 7, 18.

11 UNICEF, *supra* note 5.

12 Viktorija Morozovaite, *Two Sides of the Digital Advertising Coin: Putting Hypernudging into Perspective*, 5(2) Market and Competition Law Review 107 (2021); N. Helberger, M. Sax & J. Strycharz et al., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, 45(2) Journal of Consumer Policy 176 (2022).

minors to achieve the goals of designers are financial fraud, tailored content feedings to influence attitudes or behavior, and inducing them to be more engaged in apps or websites. Finally, even if certain legitimate data use methods are equally applied to minors and adults, different scales of risk are posed to them. Personalized recommendation systems or generative AI, on the one hand, facilitate and promote the convenience and efficiency of daily life, and liberate users from enormous information; on the other hand, they work as 'cognitive outsourcing' to substitute part of the competence of information integration, analysis, anticipation and preference reflection necessary in decision-making.[13] Such competences are crucial for minors who are still in the development phase; otherwise, algorithm reliance would potentially jeopardize their autonomy.[14] Another example is the recommendation system applied to user-generated contents.[15] It not only transforms the possible accessibility of contents exposed on open platforms without access restrictions into actual approaches, increasing the actual spheres of people who consume minors' personal data, but also renders minors' social media accounts into a situation where whoever is interested in the contents can contact the identified minor directly, which together with content risks and conduct risks constitutes three main categories of digital dangers.[16] Residual risks appear when minors become subjects of personal data, which subsequently evokes the critical issue of whether and how to reduce these risks.

The international regulatory framework, CRC, adopted in 1989, is one of the most widely ratified treaties in history, with 196 countries ratifying it and reflecting a universal consensus. It represents the globally shared and comprehensive commitment and prospects in terms of children. The children's data protection sector provides the pre-eminence principle of the best interest of the child and warrants the right to development, the right

13 John Danaher, *Toward an Ethics of AI Assistants: An Initial Framework*, 31(3) Philosophy & Technology 632 (2018).

14 M. S. Gal, *Algorithmic Challenges to Autonomous Choice*, 25(1) Michigan Technology Law Review 94 (2018).

15 For example, in one case, an app was brought into a file due to the technology's ability to create algorithms and display underage users' content to predators that are able to then message, follow, and interact with the underage user. From January 2018 to May 2019, *Xu* received short video containing children's personal information, and contacted multiple children through its private message function, three of whom were molested. *See* CIVIL PUBLIC INTEREST LITIGATION CASE FILED BY THE PEOPLE'S PROCURATORATE OF YUHANG DISTRICT, HANGZHOU CITY, ZHEJIANG PROVINCE AGAINST BEIJING XX COMPANY FOR INFRINGEMENT ON CHILDREN'S PERSONAL INFORMATION RIGHTS AND INTERESTS, at https://www.spp.gov.cn/spp/jczdal/202203/t20220307_547759.shtml (Last visited on January 2, 2025).

16 UNICEF, *supra* note 5.

to privacy, and the right to access information and mass media, respecting the autonomy of parents and guardians to take care of children under needs-based theories. On the other hand, it acknowledges children's evolving capacities and accordingly invests their views with due weight in light of the autonomy-based theory.[17] To meet the demands for addressing increasing opportunities and risks faced by children's rights due to constant technical evolution, the *United Nations' General Comment No.25 (2021) on Children's Rights in Relation to the Digital Environment* (hereinafter referred to as the Comment No.25) further enriches the above framework, and structures and proposes a more detailed, systematic and specialized guidance, from which a vision of governance of the consent mechanism for processing minors' data can be extracted.[18]

2. Processors Enjoy Legitimate Interests in Pursuing Economic Profits. — Although regulatory rules are generally configured to lower residual risks—for example, by requiring strengthened measures or obtaining guardians' consent—the promise of protection is assured at the expense of processors' economic sacrifices.

In the classical economic model, agents are assumed rational. This means that when facing the choice of 'two states of the world', agents act to maximize their utility. In practice, processors choose between compliance and noncompliance with the consent rule, with the latter gaining a triumph in most crossroads because the costs of compliance far outweigh the expected costs of noncompliance.[19] In some countries, however, by reason of high expected costs of noncompliance, processors may decide whether to offer services to minors based on calculation and comparison of profits and expected costs. In view of the burdensome consent mechanism and potential costs of noncompliance arising from obscure compliance requirements,[20] some processors prefer blocking minors under 13 out of the gate. It is evident that precise, certain, predictable and practical codes of conduct and effective enforcement no doubt

17 B. Shmueli & A. Blecher-Prigat, *Privacy for Children*, 42(3) Columbia Human Rights Law Review 759-796 (2011).

18 UNITED NATIONS, GENERAL COMMENT NO. 25 (2021) ON CHILDREN'S RIGHTS IN RELATION TO THE DIGITAL ENVIRONMENT, at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (Last visited on January 2, 2025).

19 Zhang Suhua & Yin Xiaokun, *supra* note 1, 143.

20 Lauren A. Matecki, *Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5(2) Northwestern Journal of Law & Social Policy 379 (2010).

matter. What equally significant is by reasonable allocation of responsibilities to promote processors' economic incentives and willingness to abide by the law and to create the utmost overlaps with minors' best welfare.

Preserving processors' rights to engage in business also underlies a national recommended standard, *Information Security Technology: Implementation Guidelines for Notices and Consent in Personal Information Processing* (hereinafter referred to as the Guidelines), which well notices the positive correlation of the level of duty, economic expenses and entrepreneurs' support of guidelines. It evades some complex conflicts of interest on purpose in order to build consensus and accommodate the wider participation of corporations. For example, it leaves a blank for self-regulation of general audience-oriented service provider. Even though Douyin Group designs its products consistent with the Guidelines, guardians' consent is presumed and the 'teenager model' is still self-activated.[21]

3. Guardians' Responsibilities, Rights and Duties to Provide Appropriate Directions and Guidance, and Their Own Freedom of Act Shall Be Respected. — Guardians are generally endowed with overall functions to care for, nourish and assist minors and protect them from intrusion. Nevertheless, a wider divide and disjunction between the traditional expectation of guardians' roles and their actual performance in relation to minors' data privacy emerges. On the one hand, the depth and breadth of guardians' engagement in personal data protection vary from person to person, ranging from the authoritarian style, which provides minors with strict rules to follow, to the helicopter style, which involves monitoring any tiny activities.[22] No matter how they choose to parent, in an indifferent, careless, moderate, or over-controlling manner, this does not mean they are legally chastised or morally arbitrated for performing worse in mitigating residual risks or for diverging from the best interests of the child.[23] On the other hand, practicing their own freedom of act might exert externalities on minors, such as the freedom to post facial images of minors. However, few countries take direct measures based on

21 Douyin Group, *Notices and Consent in Personal Information Processing in the Context of Internet Information Services*, S1 Information Technology and Standardization 172 (2024).

22 THE COUNCIL OF EUROPE, PARENTING IN THE DIGITAL AGE-POSITIVE PARENTING STRATEGIES FOR DIFFERENT SCENARIOS, at https://edoc.coe.int/en/children-and-the-internet/8316-parenting-in-digital-age-positive-parenting-strategies-for-different-scenarios.html (Last visited on January 2, 2025).

23 Jelena Gligorijević, *Children's Privacy: The Role of Parental Control and Consent*, 19(2) Human Rights Law Review 205 (2019).

abundant arguments to achieve the internalization of externalities flowing from guardians. As such, family, as the smallest unit of society, claims autonomy and independence to a certain degree, yet it becomes an uncertain factor in determining the level of minors' personal data protection.

B. Trade-Offs of Conflicting Interests

To address these conflicts of interest, several scholars have contributed their value judgments and solutions. Some advocate the legal responsibilities of processors, who are expected to strengthen data security, filter minors-improper contents and adopt technical methods to notice and obtain consent from guardians.[24] This approach reveals preliminary insights of processors' essential role in coping with minors' residual risks and the impact of processors' active interactions with guardians on the allocation of their responsibilities. However, it neglects the financial burdens placed on processors and the inefficiency of excessive reliance on guardians. Some further realize that the digital rights of minors are supposed to be guaranteed so as to enjoy the development and welfare of information technology, and in the meantime, the prevention of risks that minors might suffer from deserves attention.[25] Arguably, controlling the costs of risk-mitigating methods benefits both ends of personal data rights protection and continual service provision to minors because the economic incentives of processors are assured. Unfortunately, this approach underlines more precautionary measures, such as algorithm restriction and privacy by default, ignoring the reverse effect when requirements are too rigid and expensive to implement. Some acutely discover inadequate safeguards by guardians even if their consent is strictly obtained, let alone dissatisfactory execution. Consequently, limitation of the range of guardians' responsibilities is labeled as a cure either by shifting appropriate amounts of stresses to processors[26] or by acknowledging minors' capability to resist risks.[27] On this

24 Shan Yong, *Study on the Origin and Rights Protection of Data Rights*, 27(11) Henan Social Sciences 55 (2019).

25 Xiao Wan, *The Recognition of Infringement of Children's Personal Information Rights by Large Online Platform*, 6 Journal of Law Application 78 (2022).

26 Lin Huanmin, *The Normative Response to Algorithmic Guardianship*, 3 Contemporary Law Review 113 (2023); Wang Yuan, *The Legislative Approach to the Protection of Minors' Online Personal Information in China*, 6 Journal of Xi'an Jiaotong University (Social Science) 138 (2019).

27 Sun Yueyun, *Review and Improvement of Guardian Consent Rules in the Protection of Minors' Personal Information*, 1 Journal of South China Normal University 159 (2023).

basis, more recent studies having adopted a more systematic and comprehensive narrative endeavor to minimize the compliance costs of processors and effectively urge guardians to responsibly perform their obligations through normative designs on the premise of minors' personal data preservation, thereby taking into account all the interest demands and correcting the failure of the omnipotent guardians' consent rule.[28]

The accumulation of academic literature finds its path gradually to promote better application of the consent rule with the hope of harmonizing and striking the balance of all the interests concerned. The best interests of the minors, the least economic burdens of processors and the most necessary control by guardians are partly aligned, as lower costs of compliance encourage processors to embrace minors, which in turn boosts the welfare arising from utilizing online services, and restricting guardians' control to where it is necessary conduces to the certainty of minors' personal data protection and narrows the situations (and therefore reduces the expenditure) of collecting consent by processors. Such a value judgment lays the foundation for a detailed interpretation of legislation and duty divisions. However, previous studies have indicated some imperfections when construing and integrating the above inference. On the one hand, there is a lack of a holistic body for installing piecemeal plans. This is embodied in the problem-solving mindset without examination of systematic effects and the blurring of the borderline between substantive and procedural obligations. Measures deployed to mitigate risks and methods to obtain consent are inherently diverse in nature but interact with each other. The former determines the scope and level of the latter, while the consequence of the latter again affects the allocation of responsibility together with the former. In addition, there is inability to properly deal with children's rights prescribed in the CRC, such as the right to privacy and the right to be given due weight. On the other hand, there is a tendency to simply mirror international practices to support arguments without deeply reflecting on their advantages and disadvantages.

To implement the three desires to which the consent rule is committed, this paper, upon drawing experience from the research discussed before,

28 Zhang Suhua & Yin Xiaokun, *supra* note 1, 145.

proposes a three-level framework to encompass points worthy of taking notes as much as possible, and to solve different issues logically and step by step. First, the substantive part focuses on the theory and rationality of the primary allocation of responsibilities between processors and guardians to respond to the arbitrary and boundless obligations of processors or guardians. Second, the procedural part mainly considers the trade-offs between the costs of different kinds of age verification and consent collection mechanisms and the effectiveness of minors' personal data protection, which forges a secondary allocation of responsibilities between processors and guardians literally. Finally, the third level will receive the test of minors' fundamental rights and accordingly make adaptive modifications.

III. FORMULATION OF SUBSTANTIVE LAW: A PRIMARY ALLOCATION OF RESPONSIBILITIES BETWEEN PROCESSORS AND GUARDIANS

A. Different Approaches and Evaluation

The different plans for the substantive allocation of responsibilities between processors and guardians, based on which the consent rule could be construed, are classified into three main categories.

1. The Guardians-Reliant Approach. — It means that it is entirely up to guardians who communicate with and direct minors to enhance their ability to encounter risks, and even carry out intensive supervision and intervention of their online activities to prevent possible harm. This approach is literally derived from the context of article 31 of the *Personal Information Protection Law* which assigns guardians the responsibility to implement measures to reduce residual risks led by minors' data processing whose processors are in obedience to uniform substantive regulations applying to all data subjects except the extra safeguards stipulated in article 28 of the *Personal Information Protection Law*.

However, this approach faces several challenges. The primary one is the significant heavy burden placed on guardians. For example, qualified guardians have to spend large amounts of time and energy to persistently monitor, censor, and selectively clear the contents recommended by apps

when no appropriate content filtering system is in place. As mentioned before, guardians' irrationality due to varying levels of media literacy and parenting skills,[29] indifference towards minors' digital risks,[30] and radical reactions, such as strict prohibitions of device use to avoid all the consequences, leave minors with evidently inadequate protection and even create tensions in internal relationships. In addition, guardians sometimes abuse the status of legal agents rather than acting on behalf of the interests of minors, and substitute those with their own when making decisions. Typical examples are submitting, sharing or allowing to process minors' personal information without keeping potential harm caused to minors in mind if they benefit from it,[31] and vice versa, hindering minors from resorting to relief through disclosing personal information.

2. The Processors-Reliant Approach. — In view of the limitation of guardians' roles, along with the complicated and often indeterminate enforcement of guardians' consent, the *Age Appropriate Design: A Code of Practice for Online Services* (hereinafter referred to as the ICO Code) concretizing the GDPR mainly takes a processor-reliant path,[32] where substantive methods adopted by processors are regarded as decisive factors so as to remove the obstacles of uncertain elements in restraining minors' residual risks. It introduces innovative tools and recommends processors to accommodate appropriate risks-mitigating settings to minors' age ranges and respective competence to encounter and resist potential harms. For example, minors merit specific care when using their personal data for marketing purposes or creating personality or user profiles, and more stringent rules are incorporated to process sensitive information such as precise geolocation information. With respect to the allocation of responsibility between processors and guardians, the ICO Code claims that adherence to its standards already provides considerable protection for minors, reducing the risks of inability to screen them out and verify guardians' status. As a result,

29 Lin Huanmin, *supra* note 26, 209.

30 FOCUS ON NETWORK FAMILY LITERACY: FORTY PERCENT OF CHILDREN USE THEIR PARENTS' ACCOUNTS, AND THIRTY PERCENT OF PARENTS ARE UNAWARE OF IT!, at https://mp.weixin.qq.com/s/tT6p5o2g7CZeS0jwBckh2w (Last visited on January 2, 2025).

31 LEAH A. PLUNKETT, *supra* note 2.

32 *See* ICO, THE UK GDPR, at https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/ (Last visited on January 2, 2025).

'parental consent becomes only one of a number of measures in place'.

Nevertheless, such assertions are swayed by the following facts. First, the doctrine significantly narrows the functional role that guardians are expected to play. In light of the ICO Code, for core processing, which is integral and indispensable to deliver the core services, normally contracts, legitimate interests, and public tasks rather than consent are utilized to legitimize it to avoid diluting different senses of consent and consent fatigue.[33] As contract as lawful basis stresses legal capacity of concluding agreements and leverages proxies so as to remedy minors' lack of understanding and awareness of the consequence,[34] guardians' consent is not omitted, but is implied in the requirements of entering into contract itself.

Second, although processors can mitigate risks sometimes, what happens more regularly is that the risks are intrinsic in the services provided. However, the ICO Code indicates that it is not necessary for processors to provide a privacy setting for data practices if they are essential.[35] Cyberspace is dominated by its architecture, and thereafter blossoms particular corresponding codes of conduct.[36] Therefore, inherent risks can hardly be lowered if the provider does not redefine the nature of the service.

Finally, even if processors command the *de facto* ability to hold all the risks to the bottom line, the equal role of guardians cannot be neglected. To achieve this goal, processors tend to invest disproportional economic costs with measures short of flexibility and scalability, which is less instructive, suitable for individual characteristics, and less socially desirable. However, guardians are in the front line of speculating individual tolerance for risks and are able to make more flexible adjustments appropriate to their minors by exerting, if there any, rights of opt-in or opt-out.

In brief, design by privacy and by default, age-appropriate applications, and risk-based approaches are instructive and inspiring, whereas further striving is expected to cover the blank field beyond their reach.

---

33 ICO, AGE APPROPRIATE DESIGN: A CODE OF PRACTICE FOR ONLINE SERVICES, at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ (Last visited on January 2, 2025).

34 N. DETHLOFF, K. KAESLING & L. SPECHT-RIEMENSCHNEIDER, FAMILIES AND NEW MEDIA: COMPARATIVE PERSPECTIVES ON DIGITAL TRANSFORMATIONS IN LAW AND SOCIETY, at 100 (Springer, 2023).

35 ICO, *supra* note 33.

36 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, at 30 (Basic Books, 1999).

3. Restrictions on Guardians' Empowerment. — A third approach is also dedicated to correcting the failure of omnipotent guardians' involvement, but focuses mainly on the relief of interest contradictions, with a display of three typical modes.

Firstly, designing exceptions from the perspective of substantive law. In Switzerland, the *Federal Data Protection Act* and the associated ordinance, the *Data Protection Ordinance*, do not refer to minors in particular.[37] In academia, the majority hold the view that consent to data processing is qualified as a legal act, an expression of exemption from a third party's infringement of personality rights,[38] and hence relevant provisions in the *Swiss Civil Code* apply. According to article 17 of the *Swiss Civil Code*, age threshold and discernment are accumulated factors that forge valid consent.[39] The capacity of discernment is a relative and contextual concept generally judged case by case,[40] absent from uniform specification in the *Swiss Civil Code* above which minors are deemed to be reasonable enough and act with intellect and will.[41] As age and discernment are connected while possessing separate functions, minors without discernment and minors with discernment are governed by respective terms. For the former, minors, based on articles 17, 19c and 304 of the *Swiss Civil Code*, are deprived of exercising civil rights and shall be represented by parents or guardians to carry on activities other than those involved with rights closely connected to personality. Doctrine and jurisprudence developed sub-concepts, including strictly absolute personal rights and strictly relative personal rights,[42] among which only absolute ones can fall into the proviso and escape from legal representation,[43] such as the publication of minors' intimate or medical information on the Internet.[44] Therefore, to process the personal information of minors without discernment, the consent of parents or

37 LA PROTECTION DES DONNÉES PERSONNELLES DES ENFANTS, at https://adide.ch/la-protection-des-donnees-personnelles-des-enfants-2/ (Last visited on January 2, 2025).

38 PHILIPPE MEIER, PROTECTION DES DONNÉES: FONDEMENTS, PRINCIPES GÉNÉRAUX ET DROIT PRIVÉ, at 317 (Stämpfli Editions SA Berne, 2011).

39 PASCAL PICHONNAZ, BÉNÉDICT FOËX & CHRISTIANA FOUNTOULAKIS ET AL., CODE CIVIL I: ART. 1-456 CC, COMMENTAIRE ROMAND, at 213 (Helbing Lichtenhahn, 2023).

40 *Id.*, 189.

41 *Id.*, 195.

42 *Id.*, 242.

43 *Id.*, 245.

44 PHILIPPE MEIER, *supra* note 38, 319-320.

guardians is indispensable in relation to cases of relative personal rights. In light of articles 19, 19c and 407 of the *Swiss Civil Code*, the exercise of civil rights, despite being deprived of as a rule, is reserved for minors with discernment in the domain of strictly personal rights. This type of capacity is unconditional, requiring no guardians' consent in general, and includes both the categories of strictly absolute personal rights and strictly relative personal rights, encompassing the permission to access personal data.[45]

This mode explicates the theoretical yet abstract principle of highlighting the most intimate personal information, whose rights are exercised by minors themselves, demonstrating a fatal drawback of execution. A negative obligation, neither with precautionary measures to prevent infringement nor with accountability mechanisms afterwards to internalize the externalities, would be difficult to fulfill.

Secondly, some jurisdictions engage in removing minors' obstacles in a specific context when they are in desperate need to actively alienate personal data rights. According to recital 38 of the GDPR, the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child. It furnishes an exemption from guardians' consent if their omission constitutes the primary interference.

Lastly, China has issued intensive policies and administrative regulations to respond to particular sectors, such as live video streaming, where minors' rights are exposed to extreme dangers, and even deprived the participation of guardians in such a field by voiding their consent to alleviate the impact of irrationality, indifference or chasing interests by sacrificing minors' interests. In accordance with article 76 of the *Minors Protection Law of China of 2020*, the online broadcast service provider shall not provide the account registration service of the online broadcast publisher for minors under the age of 16. When providing the service for minors who have reached the age of 16, the provider will authenticate the minor's identity information and obtain consent from his parents or other guardians. Admittedly, this law, located in a relatively high position of hierarchy, governs the abuse of granting consent in the registration process rather than guardians' own publishing acts, which is nevertheless feasible to be circumvented by intermittent presentation of

45 PASCAL PICHONNAZ, BÉNÉDICT FOËX & CHRISTIANA FOUNTOULAKIS ET AL., *supra* note 39, 243.

minors before the adult camera, delivering minors' voices behind the scene, or posting edited videos containing minors' routines.

B. A Proposal of Sharing Responsibilities of Processors and Guardians

To ensure confidentiality, integrity and fair limitation of minors' data privacy, strategies taken by guardians are changed with the regulatory rules that bind processors. Traditional tasks of guardians to nurture, to protect, to provide for, to love, to connect with and to guide their children continue in the context of the digital environment, in the form of monitoring the digital footprint, establishing harmonious and trusted relationships with minors so that they would be willing to autonomously communicate their online participation, instructing the time spent online and managing privacy settings, fostering the ability to distinguish contents and persons interacting with, and so on.[46] The depth and breadth of guardian interference vary in line with the design, interpretation, and enforcement of substantive law in different jurisdictions.

The reason for the reasonable allocation of responsibilities between these two parties derives from the economic analysis. In the minors' data protection scenario, it is a typical bilateral model in which the efforts of processors and guardians jointly determine the risks of minors' data processing. Despite that the possibility and magnitude of material harm lower if levels of care increase,[47] for a given reduction in the risks of specific data processing, the expenditure put on by processors or guardians generates different efficiency. For instance, with regard to the potential erosion of minors' autonomy by using equipment inserted with automatic-decision algorithms,[48] it will sometimes be harder for processors to control the exact input content of minors, the depth of their communication and therefore the emotional reliance than guardians who are at a better place to supervise the daily and physical usage with necessary convenience provided by processors. In contrast, to prevent minors from over-disclosing personal information in

46 THE COUNCIL OF EUROPE, *supra* note 22.

47 STEVEN SHAVELL, FOUNDATION OF ECONOMIC ANALYSIS OF LAW, at 182 (The Belknap Press of Harvard University Press, 2004).

48 UNICEF, *supra* note 5.

the publicly available profiling of social media, it is the processor that can set up default settings when designing products to shield this information at moderate costs. However, it is not always easy for either the government concerned or processors to draw a concrete line of compliance to achieve social welfare optimum because of information asymmetry, especially with regard to individual tolerance and resilience, which directly affects the assessment of the level of risks.[49] Therefore, this leaves room for guardians to play a role. Generally, for a given data processing activity, guardians are better at making individual assessments of the risks imposed on their child and the benefits flowing from such a practice, or choosing precautionary approaches to lower the risks aimed at reaching the best interest of the child, even if processors have already deployed corresponding child-friendly designs on the scientific premise of division of minors by groups with small granularity. In other words, empowering guardians to consent makes possible more delicate adjustments based on the benchmark, and consent endorses either a minor's capability to cope with the service or a guardian's commitment to take over residual risks.

Such an allocation of responsibility is not unique to activating non-core services promoted by the ICO Code, but rather similarly applies to the gate that controls the passage of data processing, *inter alia*, the conclusion of the digital content contract. For example, unlike the ICO Code, where users request core services by act and implied consent to data processing is accompanied by and integrated into the tacit contract, Chinese Guidelines convert it into visible consent whenever users initiate or subsequently trigger a novel purpose or method of data usage.[50] It empowers data subjects with a real choice, putting the question of whether to continue the service by submitting their data right on the table, and avoids the possibility that a customer inadvertently clicks and opens a service without any chance to refuse the automatic processing of strictly necessary data premised on the presumed willingness to use this service. Offer/acceptance in a service contract takes the form of an agreement in privacy policy, broadening the scope of consent from a narrow one to that necessary for the performance or

49 STEVEN SHAVELL, *supra* note 47, 94-97.

50 *Information Security Technology: Implementation Guidelines for Notices and Consent in Personal Information Processing*.

entering into a contract. It follows that guardians' involvement exists not only in the narrow meaning of 'consent' as lawful grounds, but also in a broader manifestation of willingness to (or refuse to) assume the consequence of certain acts.

The above structure loads both processors and guardians with respective duty of care in each single data processing activity, meaning that processors' escape from the boundary renders themselves liable or guardians' consent invalid. It automatically responds to a long criticism towards the consent mechanism that guardians might lack the knowledge to understand complex privacy policy and be discouraged to read in detail before simply clicking 'I agree',[51] and thus, by exploiting the irrationality of decision-making, processors would carry out high-risk processing. Nevertheless, confining guardians to where they could play the utmost function is still inadequate for solving subtle relationships with their children. Internal conflicts of interest between guardians and minors are nothing new to legal representation. Traditional civil law stipulates that national protection takes precedence only under exceptional circumstances. In such cases, individual relatives or organizations are in the second line to take voluntary responsibility.[52] Similarly, in the context of the digital environment, processors act as a medium for national protection, which is compulsory in nature. In this way, the restriction of guardians' empowerment could be converted into prohibition rules or regulatory rules binding processors to exempt guardians' consent when minors enjoy legitimate independence or erase adverse impacts on minors as much as possible. It is evident that the externalities caused by the guardians' severe harm are internalized by processors. Substantial duties are redistributed in combination with the aforementioned three modes. On the one hand, with regard to situations where guardians unreasonably hinder minors' exercise of personal data rights for the purpose of resorting to relief or involving fundamental dignity, processors can exempt guardians'

51 Jeremy Greenberg, *Dangerous Games: Connected Toys, COPPA, and Bad Security*, 2(1) Georgetown Law Technology Review 177 (2017).

52 For example, in the *Civil Code of China*, article 36 stipulates that 'Where a guardian has performed any of the following acts, the people's court shall, upon request of a relevant individual or organization, disqualify the guardian, adopt necessary temporary measures, and appoint a new guardian in the best interest of the ward in accordance with law: (1) engaging in any act which severely harms the physical or mental health of the ward; (2) being indolent in performing the duties of guardian, or being unable to perform such duties but refusing to delegate all or part of the duties to others, thus placing the ward in a desperate situation; or (3) engaging in any other act which severely infringes upon the lawful rights and interests of the ward.'

consent if adequate protection is in place. On the other hand, with regard to situations where the risks of processing minors' personal data are distinctly disproportional to the benefits even with proper measures configured, namely, posting regular videos on live-broadcasting platforms, or disclosing sensitive health information, processors can prohibit guardians' consent, send pop-up notice before posting, or remove improper contents in accordance with the severity of processing, sector of service, nature of information, scale of platform, etc.

In conclusion, a tiered system for allocating substantive responsibilities has been discovered. Take the video-generating and watching platform for instance. First, it requires a service contract when entering the core service, that is, searching and watching (guardians' consent in a broader meaning). Second, activating the supplementary comment function requires consent (guardians' consent in a narrow meaning). Third, activating a personalized recommendation function requires consent (guardians' consent in a narrow meaning) and processors are supposed to filter harmful contents and take other necessary measures to lower risks. Fourth, activating live streaming online functions is forbidden, even with the guardians' consent.

IV. REALIZATION OF PROCEDURAL MEASURES: REVISIONS FOLLOWING A RISK-BASED APPROACH

Part of the so-called under-protection of minors claimed in academia is the consequence of procedural measures adopted to enforce substantive law in different jurisdictions. Procedural realization such as the scope of subjects shouldering the above substantive obligation and the level of certainty about users' age and guardians' status directly affects the secondary allocation of the responsibility of processors and guardians. The distinction between substantive and procedural sections is derived from established practices, and can avoid the argument in a 'cause-result' circle. From a systematic perspective, transacting partners shall take reasonable care to ensure the legal capacity of another and will not be liable as long as the level of duty and burden of proof are satisfied. In addition, with respect to the verification of guardians and their capabilities under law, the liability of a third party is never strict, as indicated in article 19 of the *1996 Hague Convention on the*

Protection of Children.[53]

Economic considerations also exist for the separation of the two phases. The substantive construction of the consent mechanism concentrates on isolated data processing and the standard of the best interest of the child, but ignores its impact on processors and procedural realization as well, including the recognition of minors, obtaining guardians' consent, and processors' own calculation of costs and benefits, which might lead to stopping minors from the gate. That is to say, only when the burden of processors is reduced can minors' participation in online activities be safeguarded.

In this section, the age verification which mainly guards the entrance of possible special concerns awarded to minors and connects to the range of duty subject, and consent authentication determining the efficacy of guardians' control will be discussed.

A. Age Verification

1. A Relatively Static Duty of Care with Individualized Judgement in Recognizing Minors. — In Switzerland, the capacity for discernment is a notion of fact and an object of proof. Normally, capacity is presumed, and it is the person who invokes incapacity that burdens the proof.[54] Nevertheless, the experience derived from daily life suggests fine-tuning of the principle when fitted into minors, and indicates that the younger the minor is, the weaker the presumptions are. It follows that for a child, incapacity can be presumed (thus, it is for the person who claims capacity to prove, and they will be processors if failing to screen out minors), and for a minor approaching maturity, capacity can be presumed (thus, it is for persons who propose incapacity to prove).[55] Although the processors' obligation and efforts to recognize minors without discernment are unclear, all of them, regardless of whether they are online or offline and child-directed or not, are potentially liable for minors' data processing.

53 According to article 19 of the *1996 Hague Convention on the Protection of Children*, the validity of a transaction entered into between a third party and another person who would be entitled to act as the child's legal representative under the law of the State where the transaction was concluded cannot be contested, and the third party cannot be held liable, on the sole ground that the other person was not entitled to act as the child's legal representative under the law designated by the provisions of this Chapter, unless the third party knew or should have known that the parental responsibility was governed by the latter law.

54 PASCAL PICHONNAZ, BÉNÉDICT FOËX & CHRISTIANA FOUNTOULAKIS ET AL., *supra* note 39, 206.

55 *Id.*, 107-206.

The Swiss approach represents the experience of traditional law, which is not applicable to the context of data processing. On the one hand, traditional methods are based on physical communication between parties and individualized negotiation, and personal traits and age indicators, such as appearance, action, and voice, make one-to-one estimation and case-by-case judgments convenient. It is not compatible with data processing relying heavily on the virtual environment and involving mass users. On the other hand, risks vary from one data processing practice to another, and it is questionable to employ a one-size-fits-all approach with the same level of care imposed on all activities. The risks of data processing itself and the reliance on guardians to reduce risks are different; if the same expenses are invested, it would be inefficient because, in some cases, resources are redundant, making little improvement to overall risks, while in other cases, more resources could have been spared, thus improving the status quo.

2. A Website-Centric Approach for Recognizing Minors. — The *Children's Online Privacy Protection Rule* (hereinafter referred to as the COPPA) and its rules stipulate the following. Subjects who bear the burden of strengthening the protection of minors comprise operators of websites or online services directed to children under 13 (including websites or service providers targeting children as the primary audience and directed to mixed-audiences) and operators of general-audience sites having actual knowledge that they are collecting personal information from a child.[56] Generally, websites directed to children must treat all visitors as children, but mixed-audience services that do not target children as primary audiences can implement an age screen and only apply extra safeguards to selected portions of users. An age screen can also be employed by general audience sites that seek to block children under 13. In designing an age screen, processors are required to ask for age information in a neutral manner, avoid encouraging children to falsify age information, and use technical means to prevent children from back-buttoning to enter a different age.[57]

The main intents of utilizing the concept of 'directed to children' are to substitute the costs of verifying users with simpler judgement of nature

56 FEDERAL TRADE COMMISSION, COMPLYING WITH COPPA: FREQUENTLY ASKED QUESTIONS, at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (Last visited on January 2, 2025).

57 *Id*.

of services, and to work as a transmission device to provide signals to other operators interacting in the digital ecosystem. In this way, the minors' data protection is extended along the digital networking based on this classification. However, the website-centric approach, namely, distinguishing child-directed sites from general audience sites, is insufficient in the following aspects.

First, based on statutory requirements, general audience websites are barely governed by the COPPA except for their actual acknowledgment of minors, which is weak enough to be circumvented by pretending to be blind.

Second, the COPPA does not specify who should be subject to its regulations or under what conditions. In light of equivocal rather than quantitative consideration factors,[58] operators themselves have to beforehand determine whether they are bound by the COPPA. However, it is up to FTC with hindsight to have the final say, for example, the bright line between sites targeted to both children and others (so-called mixed-audience sites), and those targeted to general audience are too blurry and confusing. As such, statutory languages that reserve much room for discretion would render compliance less predictable.[59] This is also the case for general audience sites.

Finally, it makes sense to adopt such an approach when the services or contents are offered by a sole operator. However, what if they are offered by segmented operators assembled in the same platform or the same third party? Owing to its content-based characteristic and transmission function, minors who visit general audience-oriented channels will hardly be detected, while adults who visit child-directed channels only once will be coupled with minors' tags and enjoy the walled-off version.

3. A Risk-Based Approach in Recognizing Minors. — According to article 8 of the GDPR, guardians' consent is required only in relation to the offer of information society services (ISS) directly to a child. The ICO Code equates the wording of 'offer' and 'directly to a child' with 'likely to be accessed by children', which receives a 'more probable than not' test, namely considering (i) the nature and content of the service and whether that

58 According to 16 C.F.R. §312.2, the commission will consider subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of website or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children.

59 Lauren A. Matecki, *supra* note 20.

has particular appeal for children; and (ii) the way in which the service is accessed and any measures put in place to prevent children gaining access. If these conditions are satisfied, processors can use a method that is appropriate for the risks arising from data processing to verify the user's age.

On the one hand, the ICO Code governs more services to overcome the gap left by the COPPA and the *Guidelines 05/2020 on Consent under Regulation 2016/679* (hereinafter referred to as the EDPB Guidelines); on the other hand, it sets up more dynamic and concrete variants to consider as many indicators as possible that might influence the overall risks posed to minors and implement the risk-based approach more thoroughly in order to reduce compliance costs. However, it also has the drawback of encouraging redundant resources invested in prevention settings, which could be attributed to mistaking 'any measures put in place to prevent children gaining access' as an independent variable. In the structure of argumentation of whether a service constitutes offering directly to a child, parameters such as nature, contents, and objective availability are used to justify, whereas measures taken to enforce the age threshold are used to defend, which depend not only on the extent calculated based on the above parameters, but also on the data processing risks imposed on minors. It means that for general audience services intended to exclude minors, different prevention measures such as technological obstacles and age verification shall be burdened according to the level of risks produced in data processing, degree of attraction and availability, but once they fail, the defend to escape to be defined as 'offering directly to a child' cannot be established.

4. A Proposed Combination of the Website-Centric Approach with Individualized Authentication Accompanied by a Risk-Based Approach in Recognizing Minors. — To save economic expenditure on individualized recognition, US law adopts a website-centric approach. It is of benefit in clear-cut cases where services are targeted at minors by their intents, visual contents, use of animated characters or child-oriented activities and incentives, age of model, language and so on, and hereby treats all the users as minors. This kind of authentication can also, by transferring personal data with minors' identifier, be extended into software development kit (SDK) providers who for instance, insert behavior-tracking cookies for advertising, or develop Mini Program within child-directed services, while does not work

well when a platform is cluttered with both child-oriented, general-oriented and adult-oriented services sharing the same account.

In other contexts, individualized authentication accompanied by a risk-based approach enjoys a broader stage. The advantage is that resources can be allocated according to the risk distribution. During the process of age verification, technical accessibility, degree of appeal, and the risks without any special protection in place jointly determine the methods and strength of age verification. Based on this evaluation, the model can be classified into several scenarios.

First, if the index is extremely low, the age verification is exempted. In the COPPA, this is realized by limiting the purpose and usage of specified data, including supporting the internal operation by using a persistent identifier, and protecting the security or integrity of sites or services. Compared with the COPPA, *Directive 2002/58/EC* and *Opinion 04/2012 on Cookie Consent Exemption* list much more rigorous conditions, that is, 'for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user'. The exemption of age verification of strictly necessary data processing is cost-saving and user-friendly when visiting low-risk websites or apps by coincidence or mistake. Second, if the index is relatively low, regardless of the category of lawfulness, a low standard of age verification is sufficient to either prevent minors' entry or provide special protection to them. Third, if the index is neutral or high, it is similar to scenario B. In practice, self-declaration, facial recognition, hard identifiers, third-party age verification services, and other methods are used at various evaluation levels.

B. Consent Collection

1. Significance of Distinguishing Age Verification and the Consent Collection Process. — The EDPB Guidelines and the ICO Code endorse a risk-based approach, but they take disparate attitudes towards age verification and guardians' consent. There are two points highlighted in the EDPB Guidelines. First, controllers are expected to verify the user's age when the

data processing is on the basis of consent. Second, both the methods used to verify the user's age and guardian's consent may depend upon the risks inherent in the processing as well as the available technology. Therefore, except for the methods adopted, the substantial considerations are virtually the same in these two processes.[60] It is inevitable to cast doubt on this. Is age verification bound to go hand-in-hand with the guardians' consent? Is there any independent value inherent to age verification or consent collection? Do they share the same factors worthy of consideration? In fact, a service offered directly to a child ought to abide by several obligations, including taking a minor's specialty into account when using legitimate interest as the lawful basis and tailoring transparent information correspondingly, all of which call for age classification. Another problem led by double-layer verification considering similar elements is the imbalance between the benefits and costs. On the occasion where minimal efforts of age verification and guardians' verification are accommodated to low-risk processing, only a handful of minors will ultimately benefit from guardians' control after two phases of rough filtering while consuming skewed input.

The ICO Code differentiates age verification from guardians' consent. Age certainty serves more than a prerequisite for obtaining guardians' consent in form to a certain degree; technically, it is rather a starting point for designing child-friendly privacy settings, namely prohibiting detrimental use of data, limiting nudging features, deploying default rules to deactivate non-core essential services, making users' personal information invisible to an indefinite number of persons, and so on. All of these controls are rooted in the idea that minors are more vulnerable to risks arising from data processing. To shield them, in some aspects mandatory rules are equipped to hold up the benchmark such as prohibition of profiling used to feed poisonous contents or promote harmful behavior. In other aspects, default rules are allowed to be unlocked by guardians who are willing to take over the steering wheel of safeguarding minors such as consenting to analytics cookies. The interplay between regulatory rules and guardians' roles can be clearly seen.

It is the same case within China. Personal information of minors under 14 is deemed as sensitive data and thereby, besides guardians' consent,

60 *Guidelines 05/2020 on Consent under Regulation 2016/679.*

several other strengthened guarantees are awarded to minors: specific purpose and adequate necessity of processing data, strict security measures, separate consent, and expanded content of notice (describing the necessity of processing data and impacts on personal rights).[61] All these obligations bring the node of verifying the age of minors from the moment when consent is required forward to that when service is initiated.

As discussed in the substantive law section, for a given data processing, the processor and the specific guardian undertake shared responsibilities. If the target of age verification is to screen out minors demanding protection based on the overall calculation of the possibility of a minor's approach to the data processing and potential harms flowing from such an activity, the subsequent goal of seeking a guardian's shelter lies on a statistic and factual ground with much greater probabilities and certainty, including a given minor-user, a given data processing, given safety measures accomplished by the processor, and the given expected involvement of the guardian. Thus, by connecting procedural settings with substantive allocation of obligations, guardians' functions could stand out and be maximized. It is possible for a high-risk processor to provide a service with little attraction to minors to implement moderate- or low-level devices to recognize minors, but high-level devices to obtain guardians' consent.

2. Considerations When Obtaining Guardians' Consent. — In the process of obtaining verifiable guardians' consent, the strength of methods shall be in line with the data processing risks with processors' protection in place. For instance, anticipated participation of guardians in initiating comment function and content recommendation functions differs. Additional factors, such as the flexibility of safeguarding approaches erected by processors and their possible residual individualized risks, could also be taken into account. Some measures, such as content protection attached to a recommendation system filtering physical, mental and moral harmful ads, are more universal to minors of all ages, whereas others are more sensitive to intellectual maturity and consequently more elastic to a certain degree, because in the design processors have to set an average child with corresponding cognitive and volitional capacity as a starting point while such a safety standard might

61 Articles 28, 29, and 30 of the *Personal Information Protection Law*.

be either excessive or inadequate for a specific minor. In this way, guardians are expected to respond to residual individualized risks left by the rigid technical arrangements of processors. For example, for the default setting of hiding minors' profiling, it is more important for guardians to decide whether to lock or unlock it considering the tolerance and resilience of a particular minor.

In practice, email or SIM messages with a link, a toll-free call, provision of hard identifiers with real-time facial recognition or photo comparison, official third-party platforms with previously registered child-parent relationships, and other manners are used at different parental-reliance levels.

It is noticeable that in both the processes of age verification and consent collection, there are situations where duties could be exempted if the risks are minimal, namely, to protect the security or integrity of sites or services (exempting age verification) or to respond directly on a one-time basis to a specific request from the child (exempting guardians' consent). From the perspective of processors, this is the result of the most efficient distribution of limited resources, whereas from the perspective of minors, it could equally be justified by their capacity to consent if the residual risks are constrained to a negligible quantity.

In addition, reinforcing guardians' roles by step-by-step systematic construction not only relieves the implication of guardians' unpredictable and irrational actions, but also itself builds a 'choice architecture' to nudge guardians to better perform their undertakings by signaling the level of risks using different methods of requesting consent which correspond to their prospective breadth and depth of involvements.

V. CONCLUSION

This paper focuses on the allocation of substantive responsibilities between processors and guardians, and concentrates on the protective effects of different procedural measures adopted by processors on minors' personal data rights. However, there is a blank within the complex interaction of guardians and minors. In addition, the analytical framework is based on a series of presuppositions. Therefore, it is necessary to continue to enrich and supplement the framework, and to examine the challenges and defects faced

by it.

When guardians provide consent on behalf of minors, it remains to be solved that minors' participation and expression are not paid adequate attention and there are possible threats of privacy infringement within the legal representation relationship.

All the age thresholds of the capacity to make autonomous consent are respected and thus will not be criticized and discussed in this paper in view of an interpretative position. However, bright-line limits would inevitably generate rigidity problems in applications. This problem is partly relieved by admitting minors' capacity to consent when risks created by processors are extremely low and age verification is exempted, which is compatible with the comprehensive consideration of nature and categories of personal data, and purposes and methods to process them. In other circumstances, to preserve minors' participation and expression, a more flexible standard could be employed case by case and it relies on the positive proof of minors who claim capacity. On the other hand, the roles guardians play in the decision-makings would be different in accordance with respective level of cognitive maturity of minors. For example, for minors of younger ages, guardians play a leading role in the process of fostering and cultivating them, and exercising exclusive rights to provide consent though internal communication between guardians and minors is necessary, as in other traditional affairs. With minors getting older, the consent of the guardian becomes solicited as a reinforcement.

For privacy infringement, consent does not equal interference in online and offline activities. Consent is similar to a gatekeeper permitting specific processing operations of specific categories of data for specific purposes within a specific duration, whereas detailed data and its processing results are unknown to the gatekeeper. In other words, the gatekeeper is a global rather than a local master. However, more investigations are required in the right to access where privacy contests are in greater tension.

The whole analysis strictly follows the presupposed correlations: easing the burden of processors would deliver them incentives to provide services or products to minors; as the lowest impact on minors' personal data rights constitutes a foundation, the best interests of the child could be guaranteed for minors' benefits obtained from the right to access information

and mass media, and the right to development outweighs potential harms. However, such an assumption does not always exist. From the perspective of processors, the compliance costs of providing services or products to minors might still be higher than the benefits they gain, and the difference is even higher than the compliance costs of age verification and blocking minors from the services. Whether processors offer services to minors is based on their individual rational calculations. From the perspective of minors, the infringement of personal information rights is not the only way to damage them. For example, on top of that, social media platforms might also employ psychological manipulation to encourage near endless engagement, and push persistent notifications and alerts to impact negatively on sleep and attention.[62] Such externalities that are not produced by personal information processing have not been internalized by processors in the framework. The realization of the best interests of the child depends on the effective administrative monitoring of processors to ensure that processors take reasonable measures to reduce risks, and guardians' competence to make judgments on whether to consent, and if so, how to manage residual risks. Insufficient internalization of duties by processors leads to a downward-shifting responsibility effect, overburdening guardians and derogating minors' welfare.

In this way, minors' enjoyment of services or products provided by processors does not always create positive benefits, while meaningful enjoyment might not always be provided. As the *Online Safety Amendment (Social Media Minimum Age) Bill 2024* according to which users of age-limited social media platforms are supposed to reach 16 years indicates,[63] the tolerance of a certain type of application, function, or data processing method is rather a choice of legal policy.

By clarifying interests demands concerned, an idea of implementing Chinese consent rule could be formulated: firstly, the primary allocation of responsibilities between processors and guardians shall be based on the balance of relative cost spent to reduce the overall risks of minors to a given

62 EXPLANATORY MEMORANDUM: ONLINE SAFETY AMENDMENT (SOCIAL MEDIA MINIMUM AGE) BILL 2024, at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284 (Last visited on January 20, 2025).

63 *Id*.

quantitative value, and the power of guardians shall be restricted so as to moderate the implication of irrationality and internal interest conflicts, and to respect and sustain minors' fundamental human dignity and integrity as much as possible. Secondly, a second allocation of responsibilities between processors and guardians is realized by procedural measures based mainly on a risk-based approach. In the process of age verification, for websites intended for minors, processors could deem all the users as minors, whereas for other websites, the strength of age authentication (for equipping appropriate safeguarding or for preventing minor-users) shall be in proportion to the technical accessibility, the degree of appeal, and the risks without any special protection in place. In the process of obtaining guardians' consent, risks with processors' protections in place and the flexibility of safeguarding approaches erected by processors and their possible residual individualized risks should be taken into account. Finally, the guardian-minor relationship could be rearranged to compensate for the deficiency of the bright-line fixed thresholds, and legal policy could be used to remedy the failure of minors' rights protection.

(Edited by Li Jiesi)