Student (K-12) Data Protection in the Digital Age: A Comparative Study

Kai Feng and Sylvia Papadopoulos†*

Abstract
Schools have traditionally aggregated student education records themselves, in written formats and with relatively unsophisticated systems. However, today the amount of record keeping has increased and schools are ever more reliant on third-party operators, who compile information and operate databases systematically and more efficiently. These and other factors have opened opportunities for private vendors to access student data and to share it with others. In addition, schools now routinely incorporate various forms of digital technology in the form of educational software, teaching aids, websites, and programmes that provide connected devices to each student, allowing and encouraging teachers to incorporate technology into their lessons. By its very nature, the internet is a marketing information-sharing environment and the potential for traceability exists whenever the students are engaged in online activities. With these advances and developments, data security and other concerns become of paramount importance. Among the issues that have been raised are issues such as how can the legal system engage in harm reduction? Which legal approach is appropriate? What is the scope of student data that the law should protect? To what extent should schools and operators be held accountable for compliance? How do regulators maintain the balance between the need for student data protection and other interests? To date, proponents of new technology have given insufficient answers to these questions. This comparative study aims to find common strengths in different approaches to these issues relating to student data protection, while at the same time considering cultural and legal differences that exist among the following jurisdictions: the United States (US), the European Union (EU), China, and South Africa.

INTRODUCTION

Privacy is becoming the most pervasive issue on the internet worldwide. Privacy and personal data protection are facing challenges in the digital era, due to the universal proliferation of internet-based communications, which are notoriously difficult to police; the rise of data-hungry applications

* PhD LLM Bachelor of Law; Deputy Director and Associate Professor of America-China Law Institute, China University of Political Science and Law.
† BLC LLB LLM (*cum laude*) (UP); Senior Lecturer University of Pretoria and Chair of the Law Schools Global League: New Technology and the Law Research Group.

like search engines, targeted advertising platforms, or social networks; and the use of various methods of online surveillance by both private and governmental entities. The seemingly borderless nature of digital technology leads to a complicated set of normative and policy questions. These questions relate to the adequate scope of substantive balancing between the individual interest in privacy and the potential interest of other private users, commercial entities and governments in data disclosure, but also to questions of jurisdiction and governance. The dilemma is thus not only one of *how* (or *how far*) should privacy and personal data be protected, but also one of who should oversee establishing and enforcing the legal norms.

The pace of rapid technological developments and globalisation are significant forces that have brought about challenges for the protection of student (K-12) data.[1] Schools have traditionally aggregated student education records themselves, in written formats and with relatively unsophisticated systems. However, today the amount of record keeping has increased and schools are increasingly reliant upon third-party operators, who compile and operate the databases systematically and more efficiently. These and other factors have opened up opportunities for private vendors to access student data and to share it with others. In addition, schools now routinely incorporate various forms of digital technology in the form of educational software, teaching aids, websites, and programmes that provide connected devices to each student, allowing and encouraging educators to incorporate technology into their lessons.[2] The students themselves also drive this development. For example, school teams or groups communicate via social media or messaging applications (apps). The internet is, by its very nature, a marketing and information sharing environment and the potential for traceability exists whenever the students are engaged in online activities.[3] With these advances and developments, data security and other concerns become of paramount importance. Among the issues that have

---

1 (K-12) is a term used in education and educational technology in the United States, Canada, and other countries, and is a shortened term for the school grades prior to college. These grades are kindergarten (K) and the first through to the twelfth grade (1–12) of school. See <http://whatis.techtarget.com/definition/K-12> accessed 12 January 2018.

2 A 2014 study released by the Sesame Workshop reported that seventy-four per cent of K-8 teachers use digital games for instructional purposes, with fifty-five per cent of teachers reporting that they assign digital game playing to their students at least weekly. Lori M Takeuchi and Sarah Vaala, 'Level Up Learning: A National Survey on Teaching with Digital Games' (October 2014) <http://www.joanganzcooneycenter.org/publication/level-up-learning-a-national-survey-on-teaching-withdigital-games/> accessed 12 November 2017.

3 A 2014 Politico article pointed out that students are tracked by education technology companies as they play online games, watch videos, read books, take quizzes, and work on assignments from home. The data recorded may include information about their locations, homework schedules, internet browsing habits, and academic progress. Cf Stephanie Simon, 'Data Mining Your Children' *Politico* (15 May 2014) <http://www.politico.com/story/2014/05/data-mining-your-children-106676.html.> accessed 12 January 2018.

been raised are issues such as how can the legal systems engage in harm reduction? Which legal approach is appropriate? What is the scope of student data that the law should protect? To what extent should schools and operators be held accountable for compliance? How do regulators maintain the balance between the need for student data protection and other interests? To date, proponents of new technology have given insufficient answers to these questions. This comparative study hopes to find the common points for better practice in relation to student data protection, while at the same time taking into account cultural and legal differences that exist among the following jurisdictions: the United States (US), the European Union (EU), China and South Africa. The countries chosen represent different approaches (Western, Eastern, and African approaches) to the question of student data protection, and in a discussion of China's position on the topic it is hoped that the reader will gain some insight into a jurisdiction that is largely inaccessible and unknown to many by virtue of language barriers.

LEGISLATIVE FRAMEWORKS AND NEW DEVELOPMENTS

Student Data Protection in the US

For the past forty years, two US Federal Acts have played a fundamental role in student data protection. The first is the 1974 Family Educational Rights and Privacy Act (FERPA), which is applied to all schools that receive funds under applicable educational programmes of the US Department of Education (DOE). By imposing specific duties, it relies on the schools themselves to reduce the potential data privacy risks and is recognised as efficient in the traditional framework of protecting rights.[4] However, with the developments in big-data technology, FERPA is no longer able to meet fully the requirements of protecting student data. The biggest challenge with this Act is that third-party operators are not subject to this law, and loopholes have been exploited, weakening the law's effectiveness by allowing schools to provide data to private companies without parental consent.[5] For example, the schools can disclose the student data to 'school officials with legitimate educational interests' without consent[6] and third-party operators such as contractors, consultants and volunteers are then given the status of so-called 'school-officials' and thus escape liability. Further, FERPA has been criticised for its lack of sufficient opt-out rights, and its particularly limited opportunities for parents to correct errors in the

---

4 FERPA 20 USC 1232 has played a key role in protecting educational records in the US for more than forty years. cf Alex Molnar and Faith Boninger, 'On the Block: Student Data and Privacy in the Digital Age' National Education Policy Centre, Annual Report on Schoolhouse Commercialism Trends (May 2016) 15.

5 See Marc Rotenberg and Khaliah Barnes, 'Amassing Student Data and Dissipating Privacy Rights' (28 January 2013) <http://www.educause.edu/ero/article/amassing-student-data-and-dissipating-privacy-rights> accessed 15 January 2018.

6 20 USC 1232(b)(1)(D).

data collected about their children, or to opt-out of data collection entirely.[7] Additionally, only the DOE owns the right to bring an action under this law and thus the students whose rights have been infringed cannot obtain relief through litigation under FERPA.[8]

Another significant piece of US legislation is the Children Online Privacy Protection Act (COPPA, 1998), which contributes further to protect student data. However, its binding force on operators is limited and some aspects of the Act are in need of clarity. Firstly, COPPA does not protect children over the age of thirteen, excluding those who are likely to be more active online and in their use of technology and consequently more likely to disclose their personal data. In practice, the age restrictions and the parental consent process are easy for children to circumvent and sometimes the parents themselves even help their children to lie about their age.[9] Secondly, COPPA only applies to the personal data collected *from* children, not *about* children from parents or school officials and thus limits the amount of data that is protected.[10] Thirdly, some legal experts and mass media have continuously criticised the legislation as potentially unconstitutional (for its limits on the right to freedom of speech under the First Amendment).[11]

Despite these efforts, the protection against the disclosure or misuse of the student data remains inadequate in the US and as a result, legislative reform is moving to strengthen it. At the state level, at least twenty US states have enacted student-data-privacy laws during recent legislative sessions to correct loopholes, despite the fact that the bulk of the new statutes focus on either prohibiting the collection of certain types of data or requiring states and school districts to improve their governance infrastructure and processes for safeguarding student data.[12] The state of California has taken the biggest steps to tackle these issues head-on with the passing of the Student Online

---

7 Molnar and Boninger (n 4).

8 The Secretary of Education designated the Family Policy Compliance Office (FPCO) of US Department of Education to 'investigate, process, and review complaints and violations under [FERPA]': 34 CFR s 99.60(b)(1).

9 Brandon Griggs, 'Parents Help Kids Lie to Get on Facebook, Study Finds' *CNN.com*. (1 November 2011) <https://edition.cnn.com/2011/11/01/tech/social-media/underage-facebook-parents-study/index.html?no-st=9999999999> accessed 12 January 2018.

10 COPPA s 312.2 defines *collects* or *collection* as the gathering of any personal information from a child by any means, including but not limited to: (1) Requesting, prompting, or encouraging a child to submit personal information online; (2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or (3) Passive tracking of a child online.

11 See the related opinions in Katherine McGrath, 'Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act' (2016) 49 University of California Davis LR 1160.

12 Molnar and Boninger (n 4).

Personal Information Protection Act (SOPIPA, Senate Bill 1177),[13] a milestone in education-data-privacy law reform. To fill in FERPA's gaps, the Bill places restrictions on those companies that operate online sites and applications or that provide web-based services to K-12 students.[14] At the federal level, law reform has also continued albeit more quietly. During the 114th US Congress in 2015, a variety of House and Senate Bills were introduced that propose different approaches to addressing the growing concern about protecting the privacy of student data, and addressing student PII (Personal Identifiable Information) maintained by educational institutions and agencies. Based on the alert given by Duane Morris, a leading US law firm, the congressional proposals take different approaches such as (1) establishment of a study commission; (2) targeting operators providing certain technology services to K-12 educational institutions; and (3) proposing amendments to FERPA to strengthen student data protection and enhance FERPA enforcement mechanisms.[15]

Student Data Protection in the EU

The EU does not have an independent law that relates to the protection of children's data that is comparable to the US's COPPA or FERPA. Rather, it addresses the protection of children's data throughout its General Data Protection Regulation (GDPR)[16] by indicating which provisions within the GDPR warrant a higher standard to protect children's data. The GDPR has a wide focus on data protection for all natural persons. Further, the GDPR relates to all collection, use and disclosure of data and provides for instances where the standards enacted must be higher when the data comes from children.[17] In contrast to the GDPR discussed below, the US's COPPA is narrower in its focus, prohibiting unfair or deceptive practices related to children's data online. In addition, COPPA only applies to web operators or

---

13 SOPIPA (the Senate Bill 1177) was approved on 29 September 2014 and is operative from 1 January 2016.

14 See USC 22584(d).

15 Duane Morris, 'Student Data Protection in an Era of Education Technology Innovation' (7 August 2015) <http://www.duanemorris.com/alerts/student_data_protection_education_technology_innovation_0815.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original> accessed 10 October 2018.

16 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016. The GDPR or Regulation 2016/679 heralds some of the most stringent data protection laws in the world and applies in the EU from 25 May 2018.

17 See GDPR 2016/679 art 8(1) and the related Recital 38 relating to the special protection of children's personal information.

online services directed at children or at those who have actual knowledge that they are collecting personal information from children.[18]

Under the repealed Data Protection Directive 95/46/EC[19] there were criticisms relating to the aggravated burden of data processing on institutions because of its complex rules, with a lack of coordination among member countries in relation to the flow of international data.[20]

Other legal efforts in the EU include a number of opinions on the protection of personal data of children issued by the Data Protection Working Party, including an opinion addressed to school authorities.[21] Also significant are the responses to the public consultation initiated by the Commission following the publication of its 2010 Communication, 'A Comprehensive Approach on Personal Data Protection in the European Union'[22] that aimed to improve the current EU data protection legal framework and includes specialised focus on data protection for children. Furthermore, during a conference in Luxembourg in May 2012, the EU Data Protection Commissioners adopted a Resolution on the pending EU and Council of Europe reforms, and one of the proposals endorsed related to a specific provision on children, the right to be forgotten, and the right of portability.[23]

With regard to children, the GDPR adopts the 'consent' doctrine requiring that consent 'given or authorised by the holder of parental responsibility over the child' is necessary to process children's data.[24] Such a specific protection, in particular, should apply to the use of personal data for the purposes of marketing or creating personality or user profiles and the

---

18 Tay Nguyen, 'GDPR Matchup: The Children's Online Privacy Protection Act' (CIPP/US 5 April 2017) <https://iapp.org/news/a/gdpr-matchup-the-childrens-online-privacy-protection-act/> accessed 5 January 2018.

19 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ L 281, 23.11.1995.

20 Guo Yu, *Study on the Personal Data Protection* (CUPL Press 2012) 48–49.

21 Data Protection Working Party, Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) 398/09/EN, WP 160, (adopted 11 February 2009) < http://www.redipd.org/actividades/seminario_2009/common/opinion_2-2009_menores_colegios_en.pdf > accessed 16 January 2018.

22 A comprehensive approach on personal data protection in the European Union – EU Communication COM (2010)609/3 <https://ec.europa.eu/info/policies/justice-and-fundamental-rights_en> accessed 10 October 2018.

23 Ethan Williams, *Online Privacy Laws, European Union & Select Foreign Countries* (Nova Science Publishers 2013) 15.

24 According to the GDPR Regulation 2016/679, art 8(1), where art 6(1)(a) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least sixteen years old; where the child is below the age of sixteen years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states may provide by law for a lower age for those purposes provided that such lower age is not below thirteen years.

collection of personal data with regard to students when using services offered directly to a minor student.[25]

Student Data Protection in China

Deviating from its civil law tradition and tendency to emulate the European legislative developments, China neither has any general personal data protection law nor does it have any law focused specifically on the special need to protect student data. The immaturity of legal theory has partly accounted for the lack of legislation. As far back as 2006, several experts submitted advisory drafts of personal data protection laws for consideration[26] and some NPC[27] deputies have subsequently submitted related proposals.[28] However, in the authors' opinion it may be unfair to attribute China's lack of legislation merely to the shortage of experts or deficiency in law-making skills. This issue has to be viewed against the background of a very complicated Chinese jurisprudential context. For example, until recently the authorities have been in a state of constant flux, [29] therefore hindering the enactment of personal data protection to a certain extent. China must also maintain a balance between personal data protection and other interests. Therefore, it must be weighed within a certain framework and social or political context.

Despite the lack of direct regulation of personal data, China has positively responded to the protection of student data. In response to concerns raised, China has taken some legislative measures and plans to promulgate more laws and regulations to meet the challenge and reality posed by online activities. One such significant law is the 2013 Provisions for the Protection of Personal Information of Telecommunications and Internet Users (hereinafter the Provisions),[30] which adopts the legislative system of summarising and enumeration to define the scope of personal

---

25 Recital 38 of the GDPR Regulation 2016/679.

26 The State Council entrusted some experts to study the legislative issues on the personal data protection in 2003, and the expert's advisory draft by the Chinese Academy of Social Sciences was completed in 2006 and submitted to the State Council for consideration. And more scholars, for example Qi Aimin, also made related drafts.

27 The National People's Congress (NPC) is the national legislature of the People's Republic of China.

28 At least ten proposals are provided each year, involving hundreds of NPC deputies or commissioners. See Ou Yangwu, *To Strengthen the Legal Protection of Personal Data and Improve its Legislation*, *Research on Front Issues of Personal Information Protection* (Law Press China 2006).

29 For example, as the result of the reform of the Chinese Ministry System in 2008, the former information management authority was merged into the newly established Ministry of Industry and Information Technology (MIIT). Just a couple of years later, the Cyberspace Administration of China (CAC) was founded and is to some extent sharing part of the power with MIIT.

30 The Provisions were issued by Ministry of Industry and Information Technology of the People's Republic of China on 28 June 2013 (effective on 1 September 2013).

data,[31] regulating the principles and rules of data collection or use, agent management, and the reasonable measures to maintain data security. However, the Provisions only emphasise student data protection through the traditional consent doctrine[32] and it is the authors' opinion that the sanctions are too lenient.[33]

Two additional important laws in China are the Cyber Security Law (CSL)[34] and the General Provisions of the Civil Law (GPCL),[35] which are effective as from 2017. The CSL requires internet operators to follow the principles of legality, justice, necessity, and openness when collecting and using the personal data, clarifying the purpose, manner and scope, and obtaining the consent of the owner of the data.[36] This law imposes certain duties upon operators, for example, forbidding them to disclose, alter, or destroy the collected data of minor students.[37] Given its notable legislative importance in China,[38] the CSL is widely praised for taking the first step in building a line of legal protection.[39] The GPCL does not provide for separate protection for children[40] but, for the first time, China has personal data protection laws that will have an enormous impact in the future.

Furthermore, China also has a 2016 Draft of Minors' Online Protection Regulations (hereinafter the Draft). Due to the limited privacy-protection approach and the advances of big data in China, the Draft was opened for public comments in October 2016. The Draft is currently seen as the most specialised law relating to a minor's online protection, with its Articles 11,

---

31 Article 4 of the Provisions defines personal data through its core legal characteristics such as 'personally identifiable' and listing its varieties like the user's name, date of birth, address and identity number.

32 Article 9 of the Provisions.

33 It only sets a warning and imposes a fine of no more than thirty thousand yuan for the offenses. cf '2013 Provisions for the Protection of Personal Information of Telecommunications and Internet Users' Articles 14 and 20.

34 The Cyber Security Law became effective on 1 June 2017.

35 The General Provisions of the Civil Law were issued on 5 March 2017 and became effective on 1 October 2017.

36 Article 41 of CSL.

37 Article 42 of CSL.

38 As a law issued by the Standing Committee of NPC, the Cyber Security Law has raised a professional requirement on the personal data protection and will be an important guide in making further regulations and implementation rules.

39 Sai Di and Li Jianwu, 'CSC has Built a Legal Defense for Personal Information Protection' <http://www.cac.gov.cn/2016-11/10/c_1119889943.htm> accessed 15 January 2018.

40 Under Article 111: 'The personal information of a natural person shall be protected by the law. Any organization or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process or transmit the personal information of others, nor illegally market, provide or disclose the personal information of other persons.'

15, and 16 relating to student data protection.[41] There is much excitement and hope that this will result in comprehensive regulation. However, without good democratic support and wide participation from the public, the quality of this Draft may decrease significantly.

Student Data Protection in South Africa

Privacy is recognised and protected as a personality interest in terms of the South African common law as well as section 14 of the Constitution the Republic of South Africa, 1996. If the right to privacy has been infringed, generally it is both the common law right to privacy and the constitutional right to privacy that have been infringed where a person could rely on various legal actions to remedy the breach by preventing further harm or claiming compensation.[42] Advances in technology and inadequacies in the common law protection of data privacy necessitated the promulgation of the Protection of Personal Information Act 4 of 2013 (hereinafter the POPI Act) on 26 November 2013.[43]

This piece of legislation follows EU data protection trends and aims to protect personal information that is processed by public and private bodies and ensures that the processing of personal information takes place according to internationally accepted data protection principles reinforced by adequate enforcement mechanisms to ensure compliance.[44] In April 2014, the provisions of the POPI Act relating to the office of the Information Regulator and the issuing of the Act's regulations came into effect.[45] Once the remainder of the provisions of the POPI Act become enforceable, parties that process personal information will be required to conform to the provisions of the Act within one year from the commencement of the

---

41 Under the Draft of 'Minors' Online Protection Regulations' art 11, the schools (together with other public places as cultural centres or adolescent places) are required to install minor online protection software; under art 15, the schools (from primary to high schools) shall give a course for safe and reasonable use of the internet for educational purpose and art 16 imposes liabilities.

42 Dana van der Merwe and others, *Information and Communications Technology Law* (2 edn, LexisNexis 2016) 189–191; Sylvia Papadopoulos and Sizwe Snail (eds), *Cyberlaw at SA III: The Law of the Internet in South Africa* (Van Schaik 2012) 276; cf Johann Neethling and others, *Neethling's Law of Personality* (LexisNexis 2005) 221–252, 253, 267–280; Johann Neethling and others, *Neethling's Law of Delict* (LexisNexis 2015) 370–373.

43 Papadopoulos and Snail (eds) (n 42) 291.

44 Preamble to POPI Act.

45 Section 1 Part A of Ch 5, ss 112–113 of the POPI Act came into operation in accordance with the provisions of Proclamation No R25 in GG 37544 (11 April 2014).

remainder of the provisions.[46] To date, the president has not yet announced the commencement of the remainder of the provisions of the POPI Act.[47]

The purpose of the POPI Act is to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information. It also has the purpose of establishing conditions that prescribe the minimum threshold requirements for the lawful processing of personal information, providing persons with rights and remedies to protect their personal information from processing that is not in accordance with the POPI Act. The Act establishes voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by the POPI Act.[48]

Prior to the enactment of the POPI Act, children's information or data was not a specifically designated category of information to be protected. The only direct mandate relating to children was found in section 28(2) of the Constitution stipulating that a child's best interests are of paramount importance in every matter concerning the child. However, with the POPI Act, children's personal information is designated as a separate category of personal information where the conditions related to processing of this type of information are more stringent than the processing of other personal information.[49] As with the EU, the POPI Act also follows a competent person, consent-based doctrine.[50]

REGULATORY APPROACHES

The US Regulatory Approach

The US prefers what it calls a 'patchwork' approach, or a sectoral approach to data protection (as opposed to a unified overarching system of protection), which relies on a combination of legislation and self-regulation for different sectors of American society such as children and finance.[51] Scholars describe this kind of regulatory system as supplementing the existing law (mainly privacy law) and combining it with self-regulation.[52] That is, new

---

46 Section 43(1)*(l)* of POPI Act.

47 At the time of publication of this text, the Information Regulator's office was in the process of being set up and the indication is that the POPI Act is set to commence by the end of 2018. See also Pansy Tlakula, 'Briefing on The Work of The Information Regulator' (13 February 2017) <http://www.justice.gov.za/inforeg/docs/sp-20170213-InfoRegBriefing.pdf> accessed 28 February 2017; and the website of the Information Regulator (South Africa) <http://www.justice.gov.za/inforeg/index.html> accessed 28 January 2017.

48 Section 2 POPI Act.

49 Sections 26, 27, 34 and 35 POPI Act.

50 ibid.

51 See Robert Schriver, 'You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission' (2002) 70 Fordham LR 2779.

52 See Zhang Xinbao, 'From Privacy to Personal Information: Theory of Re-evaluation of Interests and System Arrangement' (2015) 3 China Legal Science 38, 39.

legislation would be created to meet the special situations, while enterprises are expected to take reasonable measures spontaneously to comply and protect personal data. This means that there is no single privacy law that dictates a complete set of rights or duties for those who process personal information. In some senses, this approach means that legislation is flexible and can meet different needs, but it is also criticised, as it may leave some legal *lacunae*. For children, however, lawmakers hold a more protective attitude and consent is strictly required for the collection or use of related data.[53] Thus, K-12 student data has received substantive attention.

Planted in a practical legal culture, the US's legislation tends to be adopted on an ad hoc basis and arises when there are certain sectors and circumstances requiring attention, which partly explains why the specialised regulations, including the special regulation on the student data protection, are popular in this society. Influenced by this secular view, the US has chosen a dualistic approach to protect student data: imposing the duties on the third-party operators, as part of the Business and Professions Code supervised by the Federal Trade Commission (FTC); and imposing the duties on the schools, as part of the Education Code supervised by the educational authorities. Such an approach places compliance liability on those who are in charge, and thus aims to improve law enforcement.[54]

The EU Regulatory Approach

The EU has followed a harmonising approach composed of Directives and Regulations that inform or harmonise domestic legislation,[55] which provides a uniform framework of personal data protection, while also permitting EU member states to preserve their national identities in their respective judicial practices. That is, the general principles on data processing contained in the Data Protection Directive and taken up and strengthened in the soon to be implemented General Data Protection Regulation (GDPR)—such as fairness; proportionality; relevance, and that only adequate, relevant and non-excessive data can be collected and processed—govern the processing of data subject information. Many respondents urged the adoption of a cut-off age and specific requirements for the processing of children's data, though others called for no specific and detailed provisions on children based on differing rules for the definition of a child among EU members and the divergence in maturity levels in children.[56] Williams suggested an

---

53 For example, COPPA s 1302(9) requires that, before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent.

54 The FTC has many dealings with the operators while the Department of Education is authorised to be in charge of the student businesses, so they are more likely to take the efficient and timely measures.

55 Xinbao (n 52) 39.

56 Williams (n 23).

exception to the general rule that the circumstances of minor students and their best interests should be taken into account. For example, the inaccurate or incomplete student data must be erased or corrected and that the right of access can be exercised either by the student based on his maturity level or by the student's representative.[57]

The GDPR eventually settled that should the processing of a child's personal data be based on consent, children under the age of sixteen could not give that consent themselves. Instead, consent is required from a person holding 'parental responsibility'. However the GDPR does permit member states to lower the age in law, so long as it is not below the age of thirteen.[58]

The member states of the EU have followed the legal principles of Directives, while taking various measures to meet the new challenges brought about by technology. In France, except for one clause specifically mentioning minors, the 1978 law does not explicitly mention the privacy rights of minors.[59] However, it favours informing children about the responsible use of the internet. It also provides a range of alternative methods to achieve the goal of student data protection. These include organising major communication campaigns for minors; investing in funding privacy awareness programme; creating special websites for minors; requiring schools to teach students how to develop a critical and reflective approach to the use of online communications during civic education classes; and informing the students of all their rights under the 1978 law.[60] Similarly, Germany has no age-specific privacy provisions either. However, many states provide educational programmes to make young people aware of the online attacks on privacy, including online privacy education in the school curricula.[61]

---

57 Id 9.

58 Article 8(1) GDPR.

59 France's data protection law dates back to 1978 with the enactment of Law 78-17 on Information Technologies, Data Files and Civil Liberties. This law is said to have inspired the drafting of European Union Directive 95/46/EC on personal data protection. The 1978 law has been amended on several occasions to comply with more recent European Union Directives. Personal data must be collected and processed fairly and lawfully for specified, explicit, and legitimate purposes, and with the consent of the data subject. In addition to the right to consent, data subjects have been given the following rights: right to be informed, right to object, right of access, right to correct and delete information, and right to be forgotten. 'Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés' (version consolidée au 27 août 2011) [Law 78-17 of 6 January 1978 on Information Technologies, Data Files and Civil Liberties (consolidated version as of 27 August 27 2011)] <https://www.loc.gov/law/help/online-privacy-law/2012/france.php> accessed 12 February 2018. Unofficial English version available on CNIL <http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf> accessed 12 February 2018.

60 Id and Williams (n 23) 59.

61 Id 73.

China's Regulatory Model

The regulatory model for personal data protection in China is still uncertain. In structure, China tends to follow the EU model and is ready to develop uniform legislation. China's readiness is clearly demonstrated in the expert's advisory draft by the Chinese Academy of Social Sciences adopting an EU-type model.[62] Moreover, the principles of personal data protection adopted in both the Guidelines and the Provisions are very closely modelled on those of the EU Directives. However, given the fact that there is no personal data protection law yet, China has issued regulations on student data protection that are similar to the practices in the US. Therefore it seems in this respect, China is more likely to follow a hybrid legal approach where the legislative model of 'Harmonising + Self-Regulation + Citizen Participation' as suggested by Zhang Xinbao,[63] integrates EU and US regulatory-model characteristics.

Personal data has been protected under the existing Chinese civil-law framework and received protection under the umbrella of general privacy judicial practices. However, considering the varied forms of damage that occur such as data disclosure, distortion, economic loss etc, it is not easy for personal data to be protected efficiently in this way. In recent legal developments, it is clear that personal data has been distinguished from general privacy in certain Chinese Supreme Court interpretations and more importantly in GDCL,[64] though scholars remain divided on whether there exists an independent personal data right.[65] The multiple approaches are preferred. For example, some civil law scholars suggest that more rights that are influential should be granted;[66] while other public law scholars argue for the need to protect personal data by the constitutional, administrative, and even criminal legal approaches to cover the shortage of the private law approach.[67]

---

62 cf Zhou Hanhua, *Personal Data Protection Law (Expert's Advisory Draft) and Its Legislative Research Report* (Law Press China 2006).

63 Xinbao (n 52) 53.

64 Privacy and other personal data were covered by 'Provisions of the Supreme People's Court on the application of laws concerning the use of information networks in the infringement of personal rights and interests in civil disputes' (art 12); in the GPCL, the right to privacy is regulated in art 110, while the personal data protection is regulated in art 111.

65 Some scholars hold that art 111 of the GPCL just provides a remedy to solve personal data issues by a tort liability approach. See Xue Jun, 'No Conflicts Exist Between "right to personal data" and "right to privacy"', Role of Law Weekend Edition, 9 April 2017. On the other hand, some scholars hold that an independent 'right to personal data' is established by the GPCL. See Huang Chunlin, 'The Brief Comment on the Personal Data Right under GPCL' <http://article.chinalawinfo.com/ArticleFullText.aspx?ArticleId=99179> accessed 10 October 2018.

66 See Guo Yu, *Study on the Personal Data Protection* (CUPL Press 2012) 90.

67 For example, Zhao Hong points out that the public law research on the information disclosure should be turned to the information protection. cf Zhao Hong, 'From the Information Disclosure to the Information Protection the Wind Direction and Core Issue of Public Law Research on Information Protection' (2017) 2 Journal of Comparative Law 31.

South Africa's Regulatory Model

South Africa's legislative response to data protection clearly favours the EU model over the more flexible US model. When it comes to children's personal information, South Africa's POPI Act has adopted a stricter regime than the EU. In the first instance, a competent person must give consent to processing personal information relating to children that are younger than eighteen years.[68] The EU's GDPR has set the age limit at sixteen years, which can be lowered by member states to thirteen years when appropriate.[69]

The processing of personal information may also take place if the child, with the consent of a competent person, has deliberately made the information public.[70]

The general principles such as accountability, fairness, proportionality, relevance, and that only adequate, relevant and non-excessive data can be processed subject to proper security safeguards govern the processing of data subject information in a similar fashion to that of EU data protection trends.[71]

THE SCOPE OF STUDENT DATA PROTECTION

Scope of Student Data Protection under US Federal and State Laws

The scope of protected student data used to be limited to education records but has been expanded further in recent US legal developments. Under FERPA, the data regulated is that which relates to education records and includes those records, files, documents, and other materials which: (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.[72] The provision also enumerates exceptions such as records maintained for purpose of law enforcement.[73] Schools may, however, disclose without consent, so-called 'directory information' such as a student's name, address, telephone number, date and place of birth, honours and awards, and dates of attendance, although an opt-out system is provided and schools are required to tell parents about the directory information and allow them to request that the school not disclose such information.[74] In general, FERPA only protects the student data contained in the education records maintained by an educational agency. It does not protect those directly obtained from a student or teacher through an online tool not subject to a contract with the

---

68 See definition of child in s 1 read with ss 34–35 of POPI.
69 Article 8(1) GDPR.
70 Section 35(1)*(e)* of POPI.
71 Sections 8–25 of POPI.
72 Section 20 USC 1232f (a)(4)(A).
73 Id 1232f (a)(4)(B).
74 Id 1232g (a)(5).

educational agency, despite the fact that the students also create marketable profiles when they take surveys or standardised tests in school.[75]

When compared to FERPA, Californian laws have interpreted the concepts in different ways and further expanded the scope of protected student data. On the one hand, the definition of operators is expanded. Under SOPIPA, the 'operator' means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.[76] On the other hand, the student data included in its scope constitutes a wide array of information and includes so-called 'covered information' and persistent unique identifiers.[77] FERPA excludes such items as data collected by education technology websites and applications and 'pupil-generated content' (essays and so on), while the Californian interpretations include almost all the possible student data available.

Unfortunately, the operators can maintain and use de-identified or anonymous student data to develop or improve their own educational products and services, which means that only PII (Personal Identifiable Information) is covered by the law. Yet, it has been shown that in many circumstances de-identified information (non-PII) can be linked to individuals; that it can be re-identified; and that there is a risk that information deemed non-PII at one point in time could be transformed into PII at a later juncture.[78] Thus,

---

75 Molnar and Boninger (n 4) 9.

76 SOPIPA, 22584(a). 'K-12 school purposes' means purposes that customarily take place at the direction of the K-12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school (SOPIPA, 22584(k)).

77 SOPIPA, 22584(i). 'Covered information' means personally identifiable information or materials, in any media or format that meets any of the following: (1) is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12 school purposes; (2) is created or provided by an employee or agent of the K-12 school, school district, local education agency, or county office of education, to an operator; (3) is gathered by an operator through the operation of a site, service, or application described in subdivision (a) and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

78 See Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University LR 1814.

the question as to how to respond to this dilemma has become an intense debate.[79]

Scope of Student Data Protection under EU Law

In the EU, the protective scope relating to student data is no different from that of the general personal data and only the PII of students is protected. However, when compared to the US, the EU Directives take an expansionist approach to PII, by defining 'personal data' as information relating to an identified or identifiable natural person.[80] Whether the information 'relates to' a person is determined by the content, purpose, or result of the data.[81] However, in order to determine whether a person is identifiable, all the means likely to be reasonably used, either by the controller or by any other person, to identify a person should be taken into account.[82]According to the Data Protection Directive 95/46/EU, the student data refers to any information relating to an identified or identifiable student. An identifiable student is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factor(s) specific to his physical, physiological, mental, economic, cultural, or social identity.[83] The definition of the data covered in the GDPR is similar to the Data Protection Directive, except in so far as it lists more cases of PII or identifiers and includes the biometric identity of a natural person.[84] In this sense, the EU is considered more in tune with technology than the reductionist approach of the US, which considers PII to be the only information that refers to a currently identified person.[85]

Scope of Student Data Protection under China's Law

Chinese scholars hold different opinions on how to define the concept of 'personal data' and the different points of departure can be generalised as 'privacy information', 'important data', 'data relating to personal dignity',

---

79 Some scholars suggest abandoning PII as a central concept in information privacy law, for example, Paul Ohm argues that the concept of PII is unworkable and unfixable, and the attempt to define PII is as futile as the classic carnival game of 'whack-a-mole'. See Paul Ohm, 'Broken Promises of Privacy' (2010) 57 UCLA LR 1702–1704; considering PII's crucial function to have established the boundaries of privacy regulation, Paul Schwartz and Daniel Solove hold that abandoning PII is problematic and that we should opt for a reconceptualisation of a standard for PII, cf Schwartz and Solove (n 78) 1871.

80 'An identifiable' person is defined as 'one who can be identified, directly, or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity', Council Directive 95/46, on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, art 2(a) 1995 O.J. (L 281) 31, 38.

81 cf *Durant v Financial Services Authority* [2003] EWCA Civ. 1746.

82 Recital 26 Directive 95/46/EU.

83 Article 2(a) Directive 95/46/EU.

84 Article 4 Definitions in GDPR Regulation 2016/679.

85 Schwartz and Solove (n 78) 1875.

'good information', 'real information', and other forms of personal information.[86] As far as the legislative responses go, the 'Provisions' separately defines 'personal data' and extracts its core legal characteristics as personally identifiable data. Personal data in this context refers to the data collected by the telecom operators and internet service providers in the process of providing the services. These include the user's name, date of birth, address, identity number, phone number, account number and password, which can be used alone or in combination with other information to recognise the user's identification information, user service information, as well as the time and location.[87] The data included is 'identified information' and 'user service information'.

A full legal understanding of personal information is formed in the CSL, adopting a combination of generalised and enumerated approaches. Under its Article 76(5), personal data refers to various data recorded through electronic or other means, which can be used individually or in combination with other data to identify natural persons. These include, but are not limited to: the natural person's name, date of birth, ID number, personal biometric information, address, and telephone number.[88] Notably, the Draft of Minors' Online Protection Regulations provides a specific definition of data pertaining to minor students, and clarifying the scope of the data. The kind of data recorded by electronic or other means, which used alone or in combination with other information can be used to identify the identity of minors. These include, but are not limited to: the minor's name, location, date of birth, address, contact, account name, ID number, personal biometric information, and portrait of students.[89] Thus, a specialised scope of protected student data has been given.

Scope of Student Data Protection under South African Law

The data processing protection afforded by the POPI Act in South Africa relates to personal information of a natural living identifiable person. Thus, like in the EU, in South Africa, the PII of children is protected in the same way that general PII is protected. It also follows an expansionist approach by defining personal information as information relating to an identifiable person, which includes various indicators such as biometric identifiers,

---

86 Guo Yu, *Legal Protection of Personal Data* (Peking University Press 2012) 123–125.
87 Article 4 of the Provisions.
88 Article 76(5) of the CSL.
89 Article 35(3) of the Draft of Minors Online Protection Regulations.

notably information relating to education history, and any identifying numbers or symbols.[90]

DUTIES IMPOSED ON SCHOOLS OR OPERATORS

A Binary Duty Approach in the US Law

Schools oversee student records and are in a key position to control the related risks, and thus the school-duty model has proven to be an efficient legal approach for student data protection in the US. FERPA grants schools rights and imposes duties. In summary, it provides the parents with certain rights with respect to their children's education records, including the right to inspect and review the student's education records maintained by the schools, and requests that a school correct records which they believe to be inaccurate or misleading. Schools must have written permission from the parent in order to release any information from a student's education record and must notify parents annually of their rights.[91] In addition, the California Assembly Bill 1442 imposes further duties on a school.[92] It requires a school district, county office of education, or charter school that considers a programme to gather or maintain in its records any information obtained from social media of any enrolled pupil,[93] to first notify students and their parents or guardians about the proposed programme to gather or maintain the information and provide an opportunity for public comment at regularly scheduled public meetings before the adoption of a programme.[94] Moreover, the law requires the school district to only gather and maintain data that pertains directly to the school or student safety, providing a student with access to any data obtained from social media and destroying the data

---

90 Section 1 of POPI defines personal information as meaning information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—*(a)* information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; *(b)* information relating to the education or the medical, financial, criminal or employment history of the person; *(c)* any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; *(d)* the biometric information of the person; *(e)* the personal opinions, views or preferences of the person; *(f)* correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; *(g)* the views or opinions of another individual about the person; and *(h)* the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

91 Section 20 USC 1232f (a)(2)(A).

92 Assembly Bill No 1442 Chapter 799, An Act to add Section 49073.6 to the Education Code, relating to pupil records, approved 29 September 2014. To some extent aiming to play a joint role with SOPIPA.

93 Id S49073.6(2)(b) and (3)(A).

94 Id S49073.6(c)(3)(B).

as required.[95] This legislation also provides a detailed list of duties imposed on schools.[96]

Evidence from practice suggests that unregulated operators tend to make profits from the improper collection and use of the student data and the operator-duty model is used as the second protective approach. At the federal level, the operators have been subjected to duties mainly under COPPA, which has been applied to the online collection of personal data by persons or entities from children under the age of thirteen years. COPPA details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian and what responsibilities an operator must take to protect children's privacy and safety online.[97] The Federal Trade Commission (FTC) is authorised to issue and enforce the regulations. For example, it has brought a number of actions in the past years against the website operators for the failure to comply with COPPA.[98] Given the complex nature of technology, the issues and problems are not resolved through one action alone and it is indispensable that the FTC keeps continuous supervision over the application of the laws and maintains revisions of the law to meet new data protection requirements.[99] As an example of this, the 2013 COPPA revision creates the additional parental notice and the consent requirements amends definitions[100] and imposes more obligations on operators.[101]

At state level, SOPIPA, the first state privacy law that shifts the responsibility of appropriate data use to the vendor, is regarded as a breakthrough and is described as the 'stiffest U.S. bill to protect K-12 students' online data' and the 'first truly comprehensive student-data-

---

95 Id S49073.6(c).

96 For example, the school district shall destroy data gathered from social media and maintained in its records within one year after a pupil turns eighteen years of age or within one year after the pupil is no longer enrolled and shall provide notice to the third party about it. See Id S49073.6(c)(3)(A).

97 FTC, 'Complying with COPPA: Frequently Asked Questions' (FTC Business Center, Federal Trade Commission, 20 March 2015) <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 12 January 2018.

98 For example, FTC, 'Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act, Companies' Apps Shared Kids' Information with Ad Networks; Will Pay $360K In Civil Penalties', 17 December 2015 <https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens> accessed 12 January 2018.

99 Anna Wade, 'The Children's Online Privacy Protection Act: Can Website Regulations be Applied to Mobile Phone Apps?' 8 (2014–2015) Federal Courts Law Review 197, 213.

100 Among the changes are several expanded definitions closing loopholes that previously allowed third parties to collect personal information from children via 'plug-ins'.

101 For example, the operators must post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from persons under the age of thirteen; make reasonable efforts to provide direct notice to parents; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information.

privacy legislation'.[102] It prohibits an operator of an internet website or online service from knowingly using, disclosing, compiling, or allowing a third party operator to use, disclose, or compile the personal data of a minor for the purpose of marketing or advertising specified types of products or services.[103] According to SOPIPA, the online service providers must implement and maintain reasonable security procedures and practices appropriate for the nature of the protected student data, to protect the data from unauthorised access, destruction, use, modification, or disclosure, and to delete a student's protected data at the request of a school or district.[104]

Duties on the Schools and Operators in EU Law

In the EU, the GDPR regime applies to the data 'controller' and 'processor' but does not differentiate between a public body and a private body.[105] Under the GDPR, all controllers, processors, and third parties are 'the natural or legal person, public authority, agency or any other body',[106] including the schools who should undertake the duties imposed. In addition, the consent mechanism under the GDPR imposes significant duties on schools. In order to ensure that consent is freely given, it should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. In particular where the controller is a public authority and it is therefore unlikely that consent would be freely given in all the circumstances of that specific situation.[107] As a result, consent is presumed not to have been given freely if it does not allow separate consent to be given to the particular student data processing despite it being appropriate in the individual case, or if the performance of a contract is dependent on the consent despite such consent not being necessary for such performance. No doubt, the criterion of judgement under the GDPR is stricter than that under the Directive 95/46/EU, with consent, which must be concrete, clear, and freely made by the user on the premise of full knowledge.

---

[102] It is expected to become a model for other states around the country, and the technology companies spearheaded a voluntary pledge to protect the student privacy. Future of Privacy Forum and the Software & Information Industry Association (2014) <http://studentprivacypledge.org> accessed 10 October 2018.

[103] USC 22584.(b).

[104] USC 22584.(d).

[105] Article 4(7)–(8) describe a 'controller' as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by union or member state law, the controller or the specific criteria for its nomination may be provided for by union or member state law and a 'processor' as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[106] Article 4(7) and 4(8).

[107] Recital 43 Regulation 2016/679.

In contrast to the very clear operator-duty approach taken by the US, the GDPR provides a strong rights-based system instead of directly imposing duties on the operators. Under this system, the data subject has rights of access, rights to rectification and erasure, restriction of processing, data portability, objection and control over automated decision-making, and so on.[108] However, rights and duties go hand in hand, and the more rights data subjects have, the more the duties are imposed on the operators. In comparison to the former Directive, the GDPR also imposes stricter duties on the data controller and processor. For example, under its recital (64) it is stated that the controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and identifiers.[109] In addition, the controller shall maintain a record of processing activities under its responsibility; implement appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed; maintain a level of security appropriate to the risk; and carry out an assessment of the impact of the envisaged processing operations on the protection of (student-data-included) personal data.[110] The GDPR provides new requirements for data processors and expands the liabilities of controllers to the processors (who mainly acquire duties through contract).[111]

Duties on Schools and Operators under China's Laws

Chinese laws relating to student data collection and privacy are expanding across numerous agencies and through several abstract provisions. In general, the K-12 schools should follow the compliance regime set under the special regulations; legally obtaining the student data, ensuring the security of such data; and being forbidden to illegally collect, use, process, or transmit the student data; or illegally market, provide or disclose the information.[112] More specifically, the Draft of Children Online Protection Law imposes duties on schools under Articles 11 and 12, requiring schools (together with other public places, for example, the cultural centres or adolescent venues) to install minors' online protection software and to educate them on the safe and reasonable use of the internet.[113] Those who breach Article 11 will receive a warning and a fine could be imposed through their administrative bodies.[114]

However, there are very few specialised provisions governing student data protection, as China's legal policy tends to impose duties on the operators.

---

[108] Articles 15–18, 20–22 Regulation 2016/679.
[109] Recital 64 Regulation (EU) 2016/679.
[110] Articles 25, 30, 32, 35 Regulation 2016/679.
[111] Articles 3, 28–31 and Recitals 22–25, 81–82 Regulation 2016/679.
[112] Article 111 GPCL.
[113] Articles 11–12 of the 2016 Draft of Minors Online Protection Regulations.
[114] Id art 31.

The Provisions forbid telecom operators and ISPs from collecting and using the student data without consent.[115] The purpose, mode, and scope of the collection and use of data, the channels for inquiring and correcting data, and the consequences of refusing to provide data should be clearly communicated to the users.[116] Further, operators or ISPs are not allowed to collect or use the user's personal data outside of the necessary scope or purpose of their service. In addition, operators and ISPs should not deceive, mislead or use coercion in violation of laws or administrative regulations or the agreements.[117] They should maintain the secrecy of the collected or used data and take reasonable measures to prevent the data from being disclosed, destroyed, altered, or lost.[118] Once the duty is breached, the telecom administration should order the wrongdoer to correct it within a given timeframe and, together with the warnings given, they could face possible fines of between ten and thirty-thousand RMB.[119] The provisions put these agencies under the supervision and administration of the operators and made operators responsible for their agency's behaviours relating to student data collection or use.[120] This is in accordance with the principle of 'he who operates is responsible' or 'he who entrusts is responsible', and is based on the agency system in the Chinese civil law.

The internet operators are required by CSL to follow the principles of legality, justice, necessity, and openness when collecting and using student data, clarifying the purpose, manner and scope, and obtaining the consent of the owner of the data.[121] They are forbidden from disclosing, altering, or destroying the collected data.[122] They should also not collect data that is irrelevant to the service provided.[123] In this respect, China takes a very similar view to that of the Assembly Bill 1442 of California, aiming to form a boundary for data collectors. Moreover, under the Draft of Minors Online Protection Regulations, those who collect and use student data online are required to mark warning signs in an eye-catching position, indicating the source, content, and use of the collected information and obtaining the consent of the minor or his/her guardian.[124] The minor student or his/her guardian also has the right to request an ISP to delete data or shield the network space relating to the data.[125]

---

115 See art 9(1) of 'Provisions for the Protection of Personal Information of Telecommunications and Internet Users'.
116 Id art 9(2).
117 Id art 9(3).
118 Id arts 10 and 13.
119 Id arts 23.
120 Id art 11.
121 Article 41(1) CSL.
122 Id arts 42 and 43.
123 Id art 41(2).
124 Article 16 Draft of Minors Online Protection Regulations 2016.
125 Id art 18.

Duties on Schools and Operators under South African Law

The duty to comply with the lawful processing of personal information under the POPI Act falls squarely on the 'responsible party' who is described as a public or private body or any other person that alone, or in conjunction with another, determines the purpose of and the means of processing personal information.[126] Thus, schools would clearly have to conform to the duties imposed by the Act. The consent-based regime of the POPI Act does not consider the imbalance between data subjects and data controllers as the EU's GDPR does. However, it still ensures that the principle of informed consent applies. The consent must emanate from a person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child or a natural person under the age of eighteen years, who is not legally competent to take any action or decision in respect of any matter concerning him- or herself.[127]

In contrast to the operator-duty approach taken by the US, POPI in South Africa follows the direction of data protection in the EU and the Act provides a strong rights-based system. Under this system, the data subject has, among others, rights of access, rights to rectification and erasure, restriction of further processing, and objection and control over automated decision-making.[128] In addition, the controller/responsible party should maintain a record of processing activities under its responsibility; implement appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed; and maintain a level of security appropriate to the risk.[129]

BALANCING-OF-INTERESTS POLICIES

The US Balancing-of-Interests Policies

The US has been struggling to follow a balancing-of-interests legal policy. The struggle has significantly intensified with the prevalence of big-data and data-mining technology.[130] In summary, the competing factors that restrict the protection of student data include the rights and freedoms under the First Amendment, national security, and innovations in technology. Among them, the conflict between national security and student privacy is especially prevalent. One camp holds the view that national security takes priority and persistently fixes the gaps that exist in law. The other camp holds

---

126 Sections 9 and 1 definition of responsible party in POPI.

127 cf s 1 definitions for 'competent person' and 'child', ss 34–35 in POPI.

128 cf ss 23, 24, 25, 15 and 71 in POPI.

129 cf ss 17, 10, 13–14 and 19–22 in POPI.

130 Big data analytics and artificial intelligence systems have made it possible to gather, combine, analyse and indefinitely store massive volumes of data. 'Big data' refers to the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions. cf EDPS Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 10 October 2018.

the view that information privacy is a top priority and they sharply criticise the government's unwelcome invasion of privacy.[131] As for the difficulty of maintaining the balance between public interest and data protection, Hoang suggests examining whether the government's use of data is acceptable to the community, especially when the personal data collection is large-scale, and the degree of harm caused to the public may lead to greater data protection interest than the government's security concerns.[132]

An additional concern is how to protect student data while leaving enough space to educate the students in technology and innovation. Current detailed regulations have partly achieved this. The most important aspect of the legal developments in California signal that educators and legislators must work together to strike a balance with student privacy, technological innovation, and student data needs. The final legislation, SODPPA, does include some key accommodations to industry concerns, such as specifying that operators be allowed to maintain and use de-identified or anonymous student data to develop and improve their own educational products and services. For example, it explains that this balancing of interests' policy is achieved by allowing limited exceptions[133] and thus leaves room for new technological developments.

EU Balancing-of-Interests Policies

To achieve the goal of balancing rights, it clearly requires a reconciliation of competing fundamental rights with the student privacy interests. The EU courts are frequently called upon to weigh these competing interests and as a result, they do not always decide in favour of personal data or privacy. For example, the European Court of Justice (CJEU) held in the case of *Volker und Markus Schecke v Land Hessen* that the right to protection of personal data is not an absolute right, but must be viewed in relation to its function in society and be balanced with any other fundamental human rights based on the principle of proportion.[134] It allows limitations on the exercise of fundamental rights. However, limitations are only allowed if they are necessary and genuinely meet the objectives of general public

---

131 See Daniel Solove and Paul Schwartz, *Information Privacy Law* (4 edn, Wolters Kluwer: Law and Business 2011) 247–248.

132 Carolyn Hoang, 'In the Middle: Creating a Middle Road between U.S. and EU Data Protection Policies' (2012) 32 J National Association of Admin L Judiciary 811, 853–854.

133 SODPPA claims that: the law itself does not limit the ability of an operator to use student data for adaptive learning or customised student learning purposes; does not limit internet service providers from providing internet connectivity to schools or students and their families; shall not be construed to prohibit an operator from marketing educational products directly to parents so long as the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section. USC s 22584 (k)–(p).

134 cf Williams (n 23) 13.

interest recognised by the EU.[135] In the different member states of the EU, law might restrict the rights relating to student data in order to strike a balance with the freedoms and rights of others and with the general public interest, subject to the principle of proportionality and the legal systems of the member states.[136]

The last ground for processing of personal data under the Directive 95/46/EC requires a balancing act between the interests of the data subject and those of the controller or third parties to whom the data has been disclosed.[137] Not surprising, both Directive 95/46/EC and the GDPR have made efforts to achieve a proportionate balancing of interests through the imposition of restrictions. Under the Directive 95/46/EC, the member states may adopt the legislative measures to restrict the scope of the obligations and rights (in Articles 6(1), 10, 11(1), 12, 21) when such a restriction constitutes a necessary measure that should be safeguarded.[138] The GDPR reinforces this and adds a few more restrictive factors, such as social security pertaining to important economic or financial interests, the protection of judicial independence and judicial proceedings and the enforcement of civil law claims.[139]

Generally speaking, the EU adopts a pragmatic approach to meet the data protection requirements by balancing these protection requirements with their feasibility, while scholars would favour clearer statutory rules for the purpose of balance.[140]

China's Balancing-of-Interest Policies

Like the US and EU, China has also acted to strike a balance between the student data protection and other interests, to improve the development of the economy; encourage technology innovation; and maintain the important interest in national security. Some scholars tend to support the principles that are aimed at a 'win-win result and the maximization of total utility'.[141]

---

135 ibid.

136 Id 3.

137 Directive 95/46/EC had provided six legal grounds for processing, including 'to pursue legitimate interests by the controller or third parties who have become privy to such data, unless the protected interests of the data subject override those of the controller or third parties.' See also Senate Committee Report (April 2011) 21–22.

138 A restriction can be: national security; defense; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of a member state or of the European Union, including monetary, budgetary and taxation matters; a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in *(c)*, *(d)* and *(e)*; the protection of the data subject or of the rights and freedoms of others. Directive 95/46/EC, art 13(1).

139 Article 23(1) Regulation (EU) 2016/679.

140 cf Williams (n 23) 78.

141 cf Han Dayuan, 'The Concurrence and Conflict of Fundamental Rights' (1996) 4 Translation Review of Foreign Law 80.

Included among them is the principle of proportionality, which has been transplanted from EU law (especially after it was clearly written into the GDPR). The principle of proportionality has become a very popular ideology in China, although it still has a long road ahead before it is fully integrated into mainstream Chinese judicial practice.[142]

To find more practical ways, Zhang Xinbao has put forward a theory described as '… to strengthen two subjects and balance three parties'. This theory focuses on protecting personal sensitive private data and more general personal data separately; protecting the personal core interests; meeting the legitimate requirements; and maintain the balance among personal data protection, operators and national interest.[143] It is also suggested that the government and other public bodies should be strictly constrained, while giving other operators some latitude to operate without interfering with the rights to freedom of speech.[144] In general, it seems that Chinese scholars are suggesting a middle path between US and EU policies or ideologies, stricter than the US regulatory path but not quite as restrictive as EU regulation. Practically though this may be difficult to achieve.

South Africa's Balancing-of-Interest Policies

The POPI Act is not fully in force in South Africa yet and so it is difficult to draw any significant insights into how the balancing of interests may play out through the judicial procedures. However, the ideology relating to processing PI proportionally through the exceptions to the consent doctrine (such as in section 12(2)*(a)–(f)*) are encapsulated in the specific provisions relating to children's information. In section 35, the processing of a minor's information is permissible when it is necessary for the establishment, exercise, or defence of a right or obligation in law or when it is necessary to comply with an obligation of international public law, for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned. The prohibition is also lifted if it appears to be impossible or would involve a disproportionate effort to ask for consent, but sufficient guarantees need to be provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent.[145]

---

142 The principle of proportionality has not been written into the Chinese law yet, but many Chinese scholars accept it as a tool to balance the personal data protection and its conflicting interests. Opinions can be found in articles provided by Li Chengliang, 'Boundary of the Personal Data Protection' (2016) 4 J of Philosophy and Social Science; Pei Wei, 'Construction of Procedural Rules for Electronic Investigation and Evidence Collection: From the Perspective of Proportionality Principle' (2017) 1 Global LR.

143 cf Xinbao (n 52) 53.

144 Qi Aimin, *To Save the Personality in the Information Society* (Peking University Press 2009) 100.

145 Section 35(1)*(b)–(d)* of POPI.

CONCLUSION

This article analyses the legal policies and arguments on K-12 student data protection from a comparative perspective, focused upon the legal developments in the US, EU, China and South Africa. It examines key issues such as the legislative framework, legal pathways, the scope of protected student data, duties imposed on either the schools or operators, and how to achieve an equitable balance of interests. Based on the analysis, it identifies the similarities while considering cultural and legal differences that exist among the jurisdictions compared. It finds that, despite the differences in language, legal traditions, and cultural and social values, there has been a broad measure of agreement on the common topic of student data protection. The US, EU, and China remain consistent on the key issues of student data protection, providing the possibilities to learn from each other. It shows that, with the public concerns increasing, there is a common trend that all the states in this study are following by pursuing further legislative efforts or legal reforms, which are necessary to face the new challenges in the context of the internet and big-data related technology. As the response, the scope of student data protected by law has been (or is being) largely expanded and multiple duties have been imposed in the states mentioned above. It is also widely accepted that technology should facilitate the free flow of data while ensuring a high level of protection for personal data. Thus, it is inevitable that to maintain a balancing-of-interests policy, the issue remains on the extent that this policy should be implemented which has to be weighed within the respective contexts. In the meanwhile, each country preserves its specificities deeply rooted in their distinct cultures and historical, political and economic contexts. This has and will continue to result in the relative legal policies best suited to meet the different requirements. For example, as for the legal framework and pathway, the US produces more specialised regulations and flexible policies on K-12 student data protection, while the EU insists on a general pathway, uniform but with less efficiency and specificity. As the representative of a third newly developed and hybrid law style, China is trying to find a middle course, following the EU in structure, while also mixed with US practical characteristics of making more specialised laws. South Africa has adopted an approach that is arguably a more restrictive one than that of the EU, by following a policy of more generalised, wide ambits of scope, omnibus type of legislation, relying on constitutional rights to fulfil the balancing of interests requirements, such as freedom of expression or access to information. Policymakers could take note of the benefits of specialised focused legislation and the flexibility to adapt to new technology.