A STAGE WITH THREE KINGS: EDTECH, SOVEREIGNTY, AND THE FUTURE OF TRANSATLANTIC DATA LAW

QIFAN ZHANG*

TABLE OF CONTENTS

INTRODUCTION: THE THREE KINGS AND THEIR DOMAINS

The landmark *Microsoft Ireland* case highlights the limits of U.S. law enforcement authority to compel access to data stored abroad during criminal investigations. In 2013, a magistrate judge in the Southern District of New York ordered Microsoft to produce emails held on a server in Dublin, Ireland under the Stored Communications Act of 1986.[1] Microsoft released domestic data but withheld the rest, arguing that U.S. courts had no jurisdiction over foreign servers.[2] Thus, what started as a routine drug trafficking investigation exposed a deeper jurisdictional tension between cloud computing's borderless nature and traditional territorial sovereignty.[3] *Microsoft Ireland* raised worldwide concerns about data access in criminal investigations, with 289 groups from 37 countries supporting Microsoft's position.[4] The tension between borderless cloud infrastructure and territorially bounded authority exists in nearly all technology domains. For global education technology platforms, cross-border data storage raises similar questions as those raised in *Microsoft Ireland* about who can access student information and under what legal regime.

Educational technology, or "EdTech," refers to the digital platforms that schools increasingly rely on for instruction and assessment.[5] Because these platforms handle vast amounts of important student information, they play a central role in today's debates over privacy and cross-border data laws.[6] Many operate within global data infrastructures, where private companies collect, process, and analyze student data across borders to enable real-time

---

* I am a J.D. candidate at UCLA School of Law and hold a Ph.D. in Philosophy and Education from Teachers College, Columbia University. I own tremendous thanks to Professor Maximo Langer, and to my editors at the *Washington University Law Review*—Geremia, Amanda, and Emma—whose support were essential to this piece.

1 In Microsoft Corp. v. United States, the Second Circuit held that the Stored Communications Act did not authorize U.S. law enforcement to compel Microsoft to produce emails stored on a server in Ireland. 829 F.3d 197, 222 (2d Cir. 2016). The Supreme Court later deemed the case moot after Congress enacted the CLOUD Act, which amended the Stored Communications Act to require providers to disclose data within their possession, custody, or control, regardless of the data's physical location. United States v. Microsoft Corp., 584 U.S. ___ (2018). Microsoft ultimately complied with a new warrant issued under the revised law. *Id.*

2 *Microsoft Corp.*, 829 F.3d at 201.

3 Paul De Hert & Johannes Thumfart, *The Microsoft Ireland Case, the CLOUD Act and the Cyberspace Sovereignty Trilemma: Post-Territorial Technologies and Companies Question Regulatory State Monopolies*, 21 JUSLETTER IT 373, 374, 386–87 (2020).

4 *Id.* at 375.

5 David P. Grosso, Michelle R. Bowling, Starshine S. Chun & Brooke M. Delaney, *The Development of AI and Protecting Student Data Privacy*, ARENTFOX SCHIFF LLP (Feb. 22, 2024), https://www.afslaw.com/perspectives/ai-law-blog/the-development-ai-and-protecting-student-data-privacy [https://perma.cc/9SJP-QEUY].

6 *Id.*

decision-making at both individual and systemic levels.[7] Yet legal regimes still struggle to regulate these data flows, balancing privacy rights, cybersecurity, and expanding data usage.[8]

Because data crosses borders, it is often unclear who controls it and which laws apply. This has resulted in a battle between "three Kings." EdTech companies (King Innovation) want data to flow freely; national regulators (King Sovereignty) want to keep it at home; and law enforcement agencies (King Authority) seek authority to obtain data regardless of where it is stored. This struggle shapes privacy rights, legal compliance, national security, and investigative powers. Like Lear's daughters, each King vies for the crown—control over educational data.

This Note focuses on a key flashpoint in the battle: how the United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act) challenges domestic and international privacy laws governing EdTech. Section I introduces the three Kings and explains how each competes for control of cross-border data. For example, when student data becomes evidence in a criminal investigation, EdTech companies, domestic privacy regulators, and cross-border law enforcement authorities all demand control. To understand why these entities compete, Section II then examines the foundational legal and philosophical differences underlying three jurisdictions: the United States, the European Union, and China. These differences, reflected in distinct approaches to privacy rights, state power, and data governance, shape how each jurisdiction regulates EdTech platforms. Section III then discusses how these philosophical differences manifest in specific domestic privacy laws, including the United States' Family Educational Rights and Privacy Act (FERPA), and Children's Online Privacy Protection Act (COPPA), the European Union's General Data Protection Regulation (GDPR), and China's Personal Information Protection Law (PIPL). Section IV presents that when EdTech operates globally, these frameworks may collide with the CLOUD Act, which permits expanded access by U.S. authorities to data stored abroad. Finally, in Section V, I propose reforms to harmonize these laws, such as expanding safe-harbor certification frameworks to provide predictable, government-approved standards for cross-border compliance.

---

7 *See* Ben Williamson, *Digital Education Governance: Data Visualization, Predictive Analytics, and 'Real-Time' Policy Instruments*, 31 J. EDUC. POL'Y 123, 127–29 (2016).

8 *See infra*, Section III.

I. THE THREE KINGS

A. King Innovation: EdTech Platforms

EdTechs are rapidly expanding in the U.S. pre-K-12 market.[9] Because their services rely on student information, EdTech platforms process data about learning information, behaviors, preferences, and performance. This data-intensive model results in privacy concerns, especially when tools are used to target minors and capture personal information, including learning disabilities, emotional responses, behavioral patterns, and biometrics.[10] Modern analytics can generate sensitive inferences from routine student interactions, creating risks—such as privacy-invasive and discriminatory inferences that can affect students' opportunities and reputations—that existing data-protection laws do not fully address.[11] And regulators like the FTC have warned that AI-driven data collection tools may misuse student data without strong safeguards.[12] The potential sensitivity of this data becomes especially important when law enforcement agencies seek access to it during investigations, requiring EdTech firms to comply with data access requests while protecting student privacy.[13] Because schools grow more dependent on these platforms,

---

9 *See, e.g.*, Natasha Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, N.Y. TIMES (Oct. 7, 2014), http://www.nytimes.com/2014/10/07/business/microsoft-and-other-firms-pledge-to-protect-student-data.html [https://perma.cc/47AN-5KDN]; *see also U.S. Education Technology Market Size & Outlook, 2025-2030*, GRAND VIEW HORIZON DATABOOKS, https://www.grandviewresearch.com/horizon/outlook/education-technology-market/united-states (last visited Nov. 23, 2025) ("The education technology market in the United States is expected to reach a projected revenue of US$ 90,606.5 million by 2030. A compound annual growth rate of 11.1% is expected of the United States education technology market from 2025 to 2030.").

10 *See, e.g.*, Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming*, EDUC. WK. (May 30, 2019), https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05 [https://perma.cc/8KJ4-UD8J] (discussing how platforms like Social Sentinel, Securly, and Gaggle monitor students' digital content, social media, and even emotional cues); Jason Kelley, *Students Are Pushing Back Against Proctoring Surveillance Apps,* ELEC. FRONTIER FOUND. (Sept. 25, 2020), https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps [https://perma.cc/TT7Y-UFVW] (discussing student petitions against Honorlock, Proctorio, Respondus, and ProctorU for invasive uses of facial recognition, voice tracking, and other biometric monitoring).

11 Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019(2) COLUM. BUS. L. REV. 494, 505–12 (2018).

12 Jody Godoy, *FTC's Holyoak Concerned AI Collecting Children's Data*, REUTERS (Nov. 15, 2024), https://www.reuters.com/technology/artificial-intelligence/ftcs-holyoak-concerned-ai-collecting-childrens-data-2024-11-14/ [https://perma.cc/39QN-38TZ].

13 *See infra*, Section I.C (discussing how EdTechs may have to navigate law enforcement demands while protecting student privacy).

companies also shape the practical rules governing student data.[14]

For EdTechs, privacy compliance is both a legal duty and a business priority.[15] They must satisfy parental trust and regulatory requirements while maintaining the data access necessary to deliver their services. This tension is a defining feature of King Innovation's role in the educational data ecosystem.

B. King Sovereignty: Domestic Privacy Laws

Domestic privacy laws guard personal data, reflecting deep security concerns and often blocking foreign access to educational records.[16] In the United States, this protection operates primarily through two federal statutes.[17] FERPA protects student education records and generally requires parental or student consent for disclosure.[18] Similarly, COPPA safeguards the privacy of children under thirteen by requiring parental consent before online services collect, use, or disclose their personal information.[19]

Internationally, other national privacy laws have asserted even stronger control. The EU's GDPR sets strict rules for transferring personal data abroad.[20] GDPR holds companies accountable with detailed compliance requirements and imposes penalties for violations, up to 20 million euros or 4 percent of global annual revenue.[21] And China's PIPL gives authorities broad discretion to decide how information held in China may be collected and shared,[22] requiring government approval before responding to foreign legal requests.[23] These national privacy laws establish legal

---

14 T. Philip Nichols & Ezekiel Dixon-Román, *Platform Governance and Education Policy: Power and Politics in Emerging Edtech Ecologies*, 46 EDUC. EVAL. & POL'Y ANALYSIS 309, 310, 312 (2024).

15 *See infra*, Section I.C; *see also infra*, Section III.A (detailing FERPA and COPPA compliance requirements).

16 *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1640–42 (2013) (noting that national privacy laws can restrict or block cross-border access to personal data).

17 *See infra*, Section III.A.

18 *See generally* 20 U.S.C. § 1232g (1974); 34 C.F.R. § 99.30 (2024).

19 16 C.F.R. § 312.5 (2025).

20 *See infra*, Section III.B.

21 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), art. 44–50, 83, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

22 *See infra*, Section III.C; *see* Rogier Creemers, *China's Emerging Data Protection Framework*, 8 J. CYBERSECURITY 1, 1 (2022); *see also* Igor Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, 5 SMART CITIES 1129, 1130 (2022).

23 Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), chs. III–IV, 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1117 (China).

boundaries that restrict the movement of educational data, setting the stage for potential conflicts when foreign law enforcement authorities seek access.

C. King Authority: Law Enforcement Under the Cloud Act's Extraterritorial Reach

The remaining dynamic concerns law enforcement's efforts to access student data across borders despite national restrictions.[24] In the United States, this authority is articulated in the CLOUD Act of 2018, which allows U.S. authorities and partner countries to demand access to digital information relevant to criminal investigations without relying on the slower Mutual Legal Assistance Treaty (MLAT) process.[25] For EdTechs, this means that even though FERPA and COPPA generally restrict disclosure without consent, the CLOUD Act can still require service providers to disclose educational data directly to U.S. or partner-country authorities.

This statutory assertion of authority can conflict with competing claims of sovereignty—a tension this Note seeks to clarify. The CLOUD Act reflects a unilateral U.S. approach to cross-border data access.[26] This broad authority is likely to drive countries to adopt stricter localization laws as defensive measures.[27] The EU's GDPR specifically regulates foreign access to personal data, and China's PIPL sets even stricter limitations on foreign access.[28] Therefore, the CLOUD Act represents King Authority's claim that U.S. law enforcement may reach educational data held abroad. This conflicts with King Sovereignty's insistence on maintaining control over information within national borders and King Innovation's reliance on stable, cross-border data flows.

The struggle plays out in two arenas: domestically, where privacy rules limit or altogether prohibit law enforcement access to student data, and internationally, where foreign laws limit or

---

24 While the European Union and China have developed their own cross-border access frameworks, this Note focuses on the CLOUD Act's extraterritorial reach and its conflict with national privacy laws governing educational data.

25 The MLAT process requires formal, government-to-government requests, with the requested state reviewing and executing the request under its own domestic law and procedural requirements—often involving prosecutorial and judicial oversight—a multi-layered process that typically takes months or longer. *See* U.S. DEPT.ARTMENT OF JUST.ICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 3–4 (Apr. 2019), https://www.justice.gov/criminal/media/999601/dl?inline [https://perma.cc/PG3M-RJEP].

26 Secil Bilgic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, 32 HARV. J.L. & TECH. 321, 335 (2018).

27 *Id.*

28 *See infra*, Sections III.B and III.C.

altogether prohibit the transfer of data to foreign authorities.[29] These are not separate battles, but two stages of the same struggle over who ultimately controls educational data.

II. THE ORIGINS OF RIVALRY: DIFFERENCES IN DOMESTIC LEGAL PRINCIPLES

The three Kings all compete for control over data, but their struggle is complicated—and often escalated—by different countries' respective approaches to privacy rights and state authority, which shape the power each King can exercise. The United States follows a Fourth Amendment framework that guards against unreasonable searches but allows for numerous exceptions.[30] The EU elevates privacy to "a fundamental right" under Article 8 of the EU Charter.[31] And China implements a data sovereignty doctrine that prioritizes national security and state control and requires data localization to maintain government oversight.[32] These differing foundations complicate the struggle between EdTech platforms, national regulators asserting territorial control, and law enforcement authorities seeking access across them.

A. The United States: Privacy as a Balanced Interest

Under the Fourth Amendment, the United States typically uses a balancing test that flexibly weighs individual rights against other compelling government interests.[33] This framework is rooted in the "reasonable expectation of privacy," a standard that ties privacy protection to society's continually evolving judgments about what

---

29 *See infra*, Sections III (discussing domestic privacy framework), IV (analyzing international conflicts over cross-border data access).

30 *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places."); United States v. Leon, 468 U.S. 897, 925 (1984) (establishing the good-faith exception to the exclusionary rule).

31 *See* Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326 art. 8) 391 ("Everyone has the right to the protection of personal data concerning him or her."); *see also* Digital Rights Ireland Ltd. v. Minister for Commc'ns, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238, ¶ 54 (Apr. 8, 2014) (invalidating the EU Data Retention Directive (Directive 2006/24/EC) , which required telecom and internet service providers to retain traffic and location data for law enforcement purposes, for disproportionate surveillance).

32 *See* Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法). (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 37, *CLI.1.286536(EN)* (requiring critical information infrastructure operators to store personal and important data within China); *see also* Data Security Law of the People's Republic of China (中华人民共和国数据安全法) (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), art. 2, *CLI.1.483071(EN)* (establishing China's data sovereignty framework).

33 U.S. CONST. amend. IV.

counts as reasonable.[34]

This balancing approach is reflected in two key doctrines that shape how educational data receives protection. The Third-Party Doctrine limits constitutional protections for data shared with service providers, potentially removing student data held by EdTech platforms from Fourth Amendment coverage.[35] Educational search exceptions further limit protections: *New Jersey v. T.L.O.* requires only "reasonable suspicion" for school searches [36] and *Board of Education v. Earls* permits "suspicionless" drug testing for extracurricular activities.[37] Together, these context-based doctrines create a framework where students' data receives context-dependent, often attenuated protection.

In these ways, the U.S. approach—treating privacy as a balanceable interest—has long guided how U.S. or foreign courts assess government claims to access information. The CLOUD Act, which allows U.S. law enforcement to demand access to data stored abroad, is compatible with this tradition.[38] By placing the executive agreement process entirely within the Department of Justice's control "without any transparency or input from outside stakeholders or judicial oversight," the Act prioritizes government access over individual privacy rights.[39] This differs dramatically from the EU's rights-based framework and China's sovereignty-driven approach.[40]

B. The European Union: Enshrining the Right to Respect for Privacy

Unlike the U.S. model, which treats privacy as a negotiable interest subject to a balancing test, the EU treats privacy as an inalienable human right. Article 8 of the European Convention on Human Rights establishes a broad right to respect for private life that extends across diverse contexts, including public surveillance, corporate data monitoring, and cross-border transfers. [41] This

---

34 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

35 *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that individuals have no reasonable expectation of privacy in information voluntarily conveyed to third parties, thus placing such data outside Fourth Amendment protection); United States v. Miller, 425 U.S. 435 (1976) (holding that a bank depositor has no reasonable expectation of privacy in checks and deposit slips since they are business records of the bank and information voluntarily shared with third parties is outside Fourth Amendment protection).

36 New Jersey v. T.L.O., 469 U.S. 325, 345 (1985) (holding that school officials may search students' belongings based on reasonable suspicion rather than probable cause)

37 Bd. of Educ. Of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822 (2002).

38 *Supra* note 26; *see also infra*, Section IV.A (discussing the CLOUD Act's extraterritorial reach).

39 Miranda Rutherford, *The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access*, 34 BERKELEY TECH. L.J. 1177, 1202 (2019).

40 *See infra*, Sections II.B, C.

41 *See* Charter of Fundamental Rights of the European Union, *supra* note 31.

principle forms the foundation for the GDPR.

In *Uzun v. Germany*, the ECtHR ruled that, while surveillance may serve legitimate security interests, it must be proportionate, necessary, and subject to judicial oversight.[42] This contrasts with U.S. courts, which often prioritize law-enforcement interests. In this case, though, the court emphasized that privacy should be the default that deserves presumptive protections, and the burden is on the authorities to prove why that privacy should be compromised.[43]

C. China: The State as Data Guardian

Data sovereignty is core to China's approach to data governance. China emphasizes state control over data, regulating how platforms manage consumer information to prevent cybercrime and ensure government oversight.[44] This model reflects China's emphasis on public safety,[45] and its collectivist tradition, where individual rights are shaped by, and exist within, the broader interests of society, as the state defines them.[46] Whereas the United States provides avenues for government access through balancing tests, and the EU imposes strong privacy obligations on companies, China's model empowers the state to both regulate private data practices and access digital information itself.

III. THE RIVALRY DEEPENS—DIFFERENT PHILOSOPHIES PRODUCE DIVERGENT REGULATORY AND ENFORCEMENT REGIMES IN EDTECH

When applied to the EdTech industry, where student data crosses border frequently, these distinct legal frameworks produce divergent regulatory regimes that place EdTech companies, national regulators, and law enforcement agencies in tension, if not direct conflict.

---

42 App. No. 35623/05, Eur. Ct. H.R. § 78 (2010).

43 *Id.* at ¶ 80 ("Against this background, the interference by the applicant's additional surveillance via GPS thus necessitated more compelling reasons if it was to be justified.").

44 *See, e.g.*, Cyberspace Admin. of China, Administrative Penalty Decision on Didi Global Inc. (July 21, 2022), *translated in* Todd Liao, *Cyberspace Administration of China Issues Statement on Didi's $1.2B Fines for Cybersecurity Law Violations* MORGAN LEWIS (July 28, 2022), https://www.morganlewis.com/pubs/2022/07/cyberspace-administration-of-china-issues-statement-on-didis-1-2b-fines-for-cybersecurity-law-violations [https://perma.cc/T477-PPEG] (imposing 8.026 billion yuan [$1.2 billion] fine for violations of the Cybersecurity Law, Data Security Law, and PIPL, citing risks to "the nation's crucial information infrastructure and data security").

45 Liming Liu & Yiming Chen, *A Triple-Layered Comparative Approach to Understanding New Privacy Policy Practices of Digital Platforms and Users in China After Implementation of the PIPL*, SOC. MEDIA + SOC'Y, Oct.-Dec. 2024, at 1.

46 *See Id.*; Calzada, *supra* note 22, at 1130.

A. The United States: FERPA and COPPA

Enacted in 1974, FERPA is among the most important U.S. laws governing access to student data. It limits the disclosure of education records containing personally identifiable information and generally requires written consent from parents or eligible students.[47] It applies directly to federally funded schools and places requirements on EdTech companies which handle large amounts of student data through school contracts.[48]

Due to amendments in 2008 and 2011, FERPA now permits schools, under certain circumstances, to disclose student records to law enforcement agencies, contractors, consultants, and private companies without student or parental consent.[49] FERPA also requires compliance with judicial orders or subpoenas,[50] and in such cases schools must make reasonable efforts to notify the student in advance.[51] In addition, FERPA allows schools to share "directory information" unless students opt out.[52] Records created and maintained by a school's law enforcement unit fall outside of FERPA's protection, meaning they may be shared with EdTech contractors without FERPA restrictions.[53] Together, these exceptions create a disclosure regime that offers schools considerable flexibility, which can make it easier for EdTech vendors to receive and process student data through school contracts. Furthermore, FERPA's enforcement system offers limited practical deterrence, as its main penalty—cutting federal funding—exists in theory but is rarely enforced.[54] This weak enforcement environment leaves EdTech vendors with few consequences for noncompliance.

Enacted in 1998, COPPA extends privacy protections to children under thirteen by regulating how websites and online services, including EdTech platforms, collect, use, and share their personal data.[55] It requires EdTech platforms to obtain verifiable

---

47 *See generally* 20 U.S.C. § 1232g (1974); 34 C.F.R. § 99.30 (2024).

48 34 C.F.R. § 99.31(a)(1)(i)(B).

49 Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 360, 371 (2016).

50 § 99.31(a)(9) (allowing disclosure).

51 § 99.31(a)(9)(ii) (requiring "a reasonable effort to notify the parent or eligible student" in advance of compliance).

52 *Compare* 34 C.F.R. § 99.37 (permitting disclosure of directory information without consent) *with* GDPR, *supra* note 21, art. 4(1) (defining personal data to include identifiers such as names and addresses), 6(1) (requiring one of six legal bases for processing, including consent under 6(1)(a)), 7 (setting conditions for valid consent). While GDPR permits processing under legitimate conditions or other bases, educational institutions sharing directory information internationally would typically require consent absent a specific legal obligation or public interest justification.

53 34 C.F.R. § 99.8.

54 Dylan Peterson, *EdTech and Student Privacy: California Law as a Model*, 31 BERKELEY TECH. L.J. 961, 979–80 (2016).

55 15 U.S.C. §§ 6501–6506.

parental consent before collecting data, such as names, addresses, geolocation, or persistent identifiers;[56] to publish clear privacy policies outlining their data practices;[57] to collect only that information which is necessary for a child's participation in online activities;[58] and to implement security measures that protect data from unauthorized access or disclosure.[59] COPPA also allows for safe harbor programs enabling industry groups to create approved self-regulatory guidelines.[60] These requirements become relevant to cross-border governance when U.S. law enforcement seeks access to children's data held by EdTech platforms.[61]

B. The European Union: The General Data Protection Regulation (GDPR)

The GDPR, effective since May 2018, treats privacy as "a fundamental right," not a mere regulatory issue.[62] This view of privacy is perhaps best represented by its rules on automated decision-making in education, which require human oversight whenever sensitive data is used or shared.[63]

The GDPR allows free data flow only to countries with "adequate" protections.[64] Transfers to inadequate countries like the United States, require safeguards such as standard contractual clauses (contractual commitments ensuring that transferred data receives GDPR-level protection).[65] Thus, when the CLOUD Act compels U.S. providers to access data stored in Europe, the GDPR allows such transfers only under strict safeguards, making the two regimes uneasy to reconcile.[66]

---

56 16 C.F.R. § 312.5 (2025); *see also* JOEL R. REIDENBERG, N. CAMERON RUSSELL, JORDAN KOVNOT, THOMAS B. NORTON, RYAN CLOUTIER ET AL., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 9–10 (2013).

57 16 C.F.R. § 312.4.

58 *Id.* §§ 312.7, 312.10.

59 *Id.* §§ 312.3, 312.8.

60 *Id.* § 312.11.

61 *See infra*, Section IV.A

62 GDPR, *supra* note 21, recital 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

63 *Id.* arts. 15–18, 22.

64 *Id.* art. 45.

65 *Id.* arts. 44–46. In 46(2)(c)-(d), The GDPR refers to these as "standard data protection clauses," though they are often known as standard contractual clauses.

66 The EU Law Enforcement Directive explicitly requires strong safeguards when sharing data with non-EU countries, such as binding agreements or narrow public interest exceptions. Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, arts. 35, 38, 2016 O.J. (L 119) 89.

C. China: The Personal Information Protection Law (PIPL)

China's PIPL, enacted in 2021, prioritizes state sovereignty. Its defining feature is strict data localization: unlike the GDPR's conditional transfer system, China's PIPL makes cross-border data transfers dependent on explicit government security reviews.[67] It also explicitly prohibits organizations from providing personal data stored in China to foreign judicial or law enforcement authorities without government approval. [68] This sovereignty-centered model differs sharply from the CLOUD Act's access-oriented philosophy.[69]

For EdTechs, these rules pose unique challenges from those raised by differences between the U.S. and EU. Companies serving Chinese students may be designated "critical information infrastructure operators" and face stricter oversight and mandatory local data storage.[70]

Taken together, the U.S., EU, and Chinese models form the dominant regulatory triad driving today's fragmented data-governance landscape. These conflicting frameworks create significant challenges for global EdTech operations.[71]

IV. CROSS-BORDER JURISDICTIONAL CONFLICTS

Different national privacy frameworks become highly consequential once the CLOUD Act compels U.S. EdTech companies to disclose data stored overseas, only to encounter foreign privacy and data localization laws that insist the data remain at home.

A. The CLOUD Act puts EdTech Privacy Duties in Conflict with Foreign Law Enforcement

Enacted in March 2018, the CLOUD Act allows U.S. law enforcement to compel providers to disclose data stored overseas.

---

67 PIPL, art. 40 ("Critical information infrastructure operators and the personal information processors that process personal information up to the amount prescribed by the national cyberspace department shall store domestically the personal information collected and generated within the territory of the People's Republic of China."); *see also* Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 37, 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. [FIRST PAGE] (China) ("Personal information and important business data collected and produced by critical information infrastructure operators during their activities within the territory of the People's Republic of China, shall be stored within the territory . . . .").

68 Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法) [PIPL] (promulgated by Standing Comm. Nat'l People's Cong. Aug. 20, 2021, effective Nov. 1, 2021), art. 41.

69 *See infra*, Section IV.B.

70 *See* PRC's Personal Information Protection Law, *supra* note 68, at art. 40.

71 *See infra*, Section IV.B.

Passed quickly as a part of an omnibus spending bill without formal hearings, it was a direct response to *Microsoft Ireland*.[72] Under this framework, approved foreign governments can bypass the slower MLAT process by requesting data directly from U.S. companies through executive agreements, subject to Department of Justice approval and limited judicial oversight.[73] The U.S.–UK Data Access Agreement of 2019, which allows U.S. service providers to respond directly to legal requests from UK authorities, is an example of this new model.[74]

While the Act speeds up investigations, it creates a practical tension for EdTechs trying to balance FERPA's and COPPA's respective parental consent requirements with law enforcement demands.[75] FERPA and COPPA reflect a commitment to transparency via consent, but the CLOUD Act authorizes law enforcement to compel data from service providers pursuant to the requesting country's legal process.[76] Whether notice is provided to account holders depends on the requesting country's law.[77] This means that if the requesting country's law permits orders without parental consent, schools and families may not learn of data disclosure, bypassing consent and notice requirements.[78]

As such, EdTechs are trapped between multiple duties. On one hand, they risk CLOUD Act non–compliance. But if they comply with the CLOUD Act, schools and parents may abandon them for platforms that refuse to compromise student privacy.

---

72 Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. §§ 2511, 2520, 2523, 2713.

73 Rutherford, *supra* note 39, at 1184–89.

74 Office of Public Affairs, *U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online* U.S. DEPARTMENT OF JUSTICE (Oct. 3, 2019), https://www.justice.gov/archives/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [https://perma.cc/7DCP-NMBB].

75 *Id.*

76 *See* U.S. Dep't of Justice, *CLOUD Act Frequently Asked Questions*, at 16, https://www.justice.gov/criminal/media/999616/dl?inline ("CLOUD Act agreements do not create any obligations or restrictions on providers; they simply remove legal restrictions that would otherwise conflict with compliance with covered orders. Providers issued orders covered by a CLOUD Act agreement are subject to the domestic requirements of the issuing country, and the issuing country's law governs whether or how notice to an account holder by the provider may be prohibited.").

77 *Id.*

78 In U.S. practice: FERPA traditionally channels law-enforcement requests through school districts, which provides schools and families an opportunity for notice. COPPA likewise assumes parental involvement. However, CLOUD Act authority allows law enforcement to request data directly from EdTech companies, bypassing schools and potentially families. If the order includes a nondisclosure order, companies cannot notify parents. This means U.S. law enforcement can access U.S.-stored student data—even from students who are U.S. citizens with parents in the U.S.—without the transparency safeguards that FERPA and COPPA require.

B. The U.S. CLOUD Act Creates Practical Tensions with the EU's GDPR and China's PIPL in Cross-Border-Data Access.

The CLOUD Act's mechanism of direct provider access creates procedural misalignment with foreign privacy laws. Although the Act permits bilateral executive agreements, these deals often favor U.S. interests, reflecting the United States' technological dominance and bargaining leverage.[79] The Act's core mandate that U.S. providers disclose data within their "possession, custody, or control," even when stored abroad, creates potential conflicts with foreign data-security and localization laws.[80]

GDPR overall requires that data transfers meet strict standards of necessity, proportionality, and adequacy.[81] It restricts cross-border transfers to adequacy decisions, safeguards, or narrow derogations.[82] It also obliges companies to build privacy protections into their systems, get parental consent for users under sixteen, and conduct Data Protection Impact Assessments.[83] These steps aim to protect minors from the higher risks of profiling, automated decisions, and large-scale data usage in settings such as IoT-based smart homes.[84] The same principles apply to EdTech platforms, which also rely heavily on data collection.[85] Tensions may grow in cross-border cases, where platforms face foreign law enforcement demands, likely without consideration of GDPR's necessity and proportionality requirements.

---

79 De Hert & Thumfart, *supra* note 3, at 376 ("Whilst the bilateral nature of the CLOUD Act is problematic because it infinitely increases the bargaining power of the US, where most tech firms are situated, the included provisions can be regarded as an important step towards the development of a post-territorial legal framework for the obtaining of e-evidence.").

80 STEPHEN P. MULLIGAN, CONG. RSCH. SERV., CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT, 8 (2018).

81 Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd.*, 2020 ECLI:EU:C:2020:559 (July 16, 2020).

82 GDPR allows transfers of personal data to third countries through three mechanisms. Adequacy decision under Article 45 allows transfers to countries the European Commission has determined provide protection essentially equivalent to the EU standards such as respect for fundamental rights, limits on public-authority access, and availability of independent oversight and judicial redress. The Commission has so far recognised the United States (commercial organisations participating in the EU-U.S. Data Privacy Framework) as providing an adequate level of protection. Appropriate safeguards under Article 46 permit transfers absent an adequacy decision where controllers implement legally binding mechanisms such as Standard Contractual Clauses. Finally, Article 49 derogations permit transfers in narrow and exceptional circumstances, including explicit consent, important public interest, or the establishment of legal claims. *See* 2016 O.J. (L 697) arts. 45 (adequacy decisions), 46 (appropriate safeguards), & 49 (derogations); *see also* Eur. Comm'n, *Adequacy Decisions* (last visited Dec. 18, 2025), https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

83 *See* GDPR, *supra* note 21, arts. 25, 8, and 35.

84 Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou, Yutaka Ishibashi, & Kostas E. Psannis, *Preserving Minors' Data Protection in IoT-Based Smart Homes According to GDPR Considering Cross-Border Issues*, 17 J. COMMC'NS 180, 181-83 (2022).

85 *See supra*, Section I.A.

In 2020, the Court of Justice of the European Union (CJEU) held that U.S. data protection measures do not provide an adequate level of protection for EU personal data.[86] The court identified three fundamental deficiencies. First, U.S. surveillance laws—particularly FISA Section 702 and Executive Order 12333— fail to satisfy necessity and proportionality because they permit government access to personal data in excess of that permitted by the GDPR.[87] Second, these laws lack clear and precise rules about when and how government authorities may access data, failing to ensure that surveillance is limited to what is strictly necessary and proportionate.[88] Third, EU citizens lack an effective judicial remedy to challenge U.S. government surveillance, undermining the fundamental right to an effective remedy.[89] Because U.S. law fails on these counts, the CJEU concluded that the adequacy requirement isn't met.[90]

Under the CLOUD Act, U.S. law enforcement may compel providers to disclose data stored in the EU.[91] Such compelled access can constitute an EU-U.S. transfer under the GDPR, a transfer for which it remains unclear whether the GDPR's specific safeguards can be adequately satisfied.[92] If the transfer is ultimately found non-compliant, the company could face severe GDPR penalties.[93]

The GDPR offers strong safeguards against foreign access to personal data. However, it protects only personal data, not corporate information.[94] This gap highlights Europe's broader challenge in building sovereign cloud infrastructure and legal safeguards—a vulnerability shared globally.[95] This challenge has driven a global shift toward data sovereignty, with countries tightening cross-border controls, as seen in GDPR-inspired GCC rules and other new privacy laws.[96]

Meanwhile, differences between the U.S.' CLOUD Act (U.S.) and China's PIPL create an even sharper tension. Most notably, PIPL keeps sensitive data in China without government approval.[97] This absolute commitment to data localization directly challenges the

86 *Supra* note 81.
87 *Id.* at ¶ 166–67.
88 *Id.* at ¶ 176.
89 *Id.* at ¶ 197.
90 *Id. See also* Rizou et al., *supra* note 84, at 180.
91 *Supra* note 80.
92 *See* GDPR, *supra* note 21; *see also supra* note 81.
93 *Supra* note 21.
94 Emmanuelle Mignon, *The CLOUD Act: Unveiling European Powerlessness*, 1 LA REVUE EUROPÉENNE DU DROIT 108, 120–25 (2020).
95 *Id.*
96 Hamad Hamed Alhababi, *Cross-Border Data Transfer Between the GCC Data Protection Laws and the GDPR*, 13 GLOB. J. OF COMPAR. L. 178 (2024).
97 PIPL, *supra* note 68.

CLOUD Act's core objectives.

PIPL reflects China's broader data sovereignty doctrine, which prioritizes national security over digital information.[98] Article 38 enumerates four legal bases for transferring personal data outside China, including passing a security assessment conducted by state cyberspace authorities.[99] Yet, PIPL's cross-border requirements remain "still quite ambiguous," unlike the GDPR's clearer transfer rules, generating additional uncertainty for multinational companies.[100] Notably, this regulatory framework does not exist in isolation, operating instead alongside China's other data protection laws, including the Data Security Law (数据安全法) of 2021 and the Cybersecurity Law of 2017 (网络安全法).[101]

EdTech platforms that comply with U.S. demands risk severe penalties in China, including fines of up to 50 million RMB or five percent of annual revenue under the PIPL.[102] This standoff emphasizes the growing fragmentation of global data rules, the impact of which is significant. Apple's $1 billion investment in a Guizhou data center, for example, shows the lengths companies must go to meet China's data localization rules.[103]

V. PROPOSALS FOR HARMONIZATION

EdTechs sit at the crossroads of national regulation and law-enforcement access, facing conflicts that their cross-border operations cannot easily resolve.[104] Addressing this fragmentation requires interoperability that enables cross-border cooperation while still respecting core privacy principles. This section outlines three pathways: adopting international guidelines that provide shared standards, expanding safe-harbor certification frameworks that allow conditional compliance across legal systems, and developing industry best practices to support responsible data governance.

---

98 Creemers, *supra* note 22, at 1.

99 Gulbakyt Bolatbekkyzy, *Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation*, 11 GRONINGEN J. INT'L L. 129, 138 (2024).

100 *Id.* at 144.

101 *See supra* note 32.

102 Bolatbekkyzy, *supra* note 99, at 139.

103 Apple partnered with Guizhou-Cloud Big Data to construct a data center in China's Guizhou Province, aligning with China's Cybersecurity Law, which took effect on June 1, 2017 and requires foreign companies to store Chinese users' data on servers located within China. *See* Paul Mozur, Daisuke Wakabayashi & Nick Wingfield, *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html [https://perma.cc/8GSW-TJUY].

104 *See supra*, Section IV.

A. International Guidelines and Standards

International guidelines developed by the Organization for Economic Cooperation and Development (OECD) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) might offer a foundation for shared standards.

The OECD Privacy Guidelines, first adopted in 1980 and updated in 2013, established a global baseline that influenced later frameworks such as the EU's GDPR and Japan's Act on the Protection of Personal Information.[105] These guidelines set out eight core principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[106]

UNESCO's Recommendation on the Ethics of Artificial Intelligence, adopted in 2021, addresses ethical concerns arising from the use of AI systems in educational settings.[107] It requires that AI systems used in learning environments must be subject to strict requirements, particularly when monitoring or predicting student behavior, and that any data collected must not be misused or commercially exploited.[108]

These approaches have made an impact in multinational efforts to regulate data governance and ethical AI; the APEC Cross-Border Privacy Rules system, which operationalizes OECD principles, has facilitated data flows among diverse nations, including the United States, Japan, Singapore, and the Philippines.[109] This demonstrates that international guidelines can evolve into functional interoperability mechanisms when backed by regional cooperation.

Different data laws may create compliance dilemmas that companies cannot resolve through perfect adherence to all

---

105 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 7 (2013), https://legalinstruments.oecd.org/public/doc/114/114.en.pdf.

106 *Id.*

107 UNITED NATIONS EDUCATIONAL, SCIENTIFIC, AND CULTURAL ORGANIZATION, RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE (2022), https://unesdoc.unesco.org/ark:/48223/pf0000381137.

108 *Id.* at 34 ("AI systems used in learning should be subject to strict requirements when it comes to the monitoring, assessment of abilities, or prediction of the learners' behaviours. AI should support the learning process without reducing cognitive abilities and without extracting sensitive information, in compliance with relevant personal data protection standards. The data handed over to acquire knowledge collected during the learner's interactions with the AI system must not be subject to misuse, misappropriation or criminal exploitation, including for commercial purposes.").

109 *Global Cross-Border Privacy Rules Declaration*, U.S. DEP'T OF COM., http://www.commerce.gov/global-cross-border-privacy-rules-declaration [https://perma.cc/3D9H-LDHH]. *See also* Asia-Pac. Econ. Coop., *Benefits of the APEC Cross-Border Privacy Rules* 3 (2019).

frameworks.[110] International guidelines may influence, but cannot forcefully alter, domestic laws. However, OECD and UNESCO standards offer reliable common ground because they have already helped shape major regulatory frameworks.[111] As a result, they point to a core set of requirements on which broad consensus is likely to exist across jurisdictions.

Yet reliance on transnational standards faces an implementation challenge: because they are not binding law, they cannot compel participation or compliance.[112] Indeed, China's participation in global data-governance systems remains limited, even as its observer status at the OECD suggests potential for future engagement.[113]

B. Safe Harbor and Cross-Border Frameworks

Likewise, expanding safe-harbor provisions can offer a practical compliance pathway for EdTechs. COPPA already provides a model through its Safe Harbor program, which allows industry groups to create FTC-approved self-regulatory frameworks.[114] A broader system, such as an expanded safe-harbor certification, could similarly streamline cross-border compliance by giving EdTechs government-endorsed standards to follow. By meeting such standards, companies could reduce legal risk and provide clearer assurance of responsible data practices across borders.[115] And a multi-jurisdictional safe-harbor program could go further by setting shared benchmarks that help bridge differences across national privacy laws and that reflect core privacy principles.[116]

A modernized approach could build on the lessons of the EU–U.S. Data Privacy Framework (DPF), adopted in 2023, three years after the CJEU struck down the Privacy Shield in its July 2020 *Schrems II* decision.[117] The court had previously invalidated the Safe

110 *See supra*, Section IV.
111 *See supra* notes 105, 107.
112 *See, e.g., supra* note 105 ("Recommendations are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.").
113 *China (People's Republic of) and the OECD*, OECD, https://www.oecd.org/en/countries/china-people-s-republic-of.html [https://perma.cc/4M8N-94AY].
114 *See* 16 C.F.R. § 312.11 (2023).
115 *See supra*, Section IV (discussing potential cross-border compliance conflicts that expanded safe-harbor certification could help address).
116 *See id*; *see also supra* note 105.
117 *Questions & Answers: EU–U.S. Data Privacy Framework*, EUR. COM., (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752 [https://perma.cc/FR53-FLLA]. *See also supra* note 81.

Harbor Framework in its 2015 *Schrems I* ruling.[118] Both agreements were struck down due to concerns over U.S. surveillance and the lack of legal remedies for EU citizens.[119] While the Safe Harbor Framework and the Privacy Shield were early attempts at bridging regulatory differences, the successive invalidation highlights the challenges of achieving mutual recognition in cross-border data protection.[120]

In response, the DPF introduced stricter limits on U.S. government data access, requiring that intelligence requests be necessary and proportionate.[121] This aligns more closely with EU privacy standards.[122] The DPF also created an independent redress mechanism for EU individuals, including the establishment of a Data Protection Review Court (DPRC) within the U.S. Department of Justice.[123] This court operates independently from intelligence agencies and can investigate complaints and order corrective actions.[124] Similar frameworks might be extended to other jurisdictions or tailored to high-risk sectors like EdTech.

In addition, the Global Cross-Border Privacy Rules Forum, launched in 2022, represents initial progress toward interoperable privacy certification across jurisdictions, though it doesn't yet address the critical issue of law-enforcement access.[125] Similarly strong multi-jurisdictional certification frameworks might help create supervised channels for sharing data between authorities by offering a common baseline of vetted privacy safeguards.

C. Industry Self-Regulation and Best Practices

Industry-led self-regulation could offer a complementary approach to government regulation. By adopting international standards such as those developed by the International Organization for Standardization (ISO) and other recognized frameworks, EdTechs can establish consistent baseline privacy practices across

---

118 Shara Monteleone & Laura Puccio, *The CJEU's Schrems Ruling on the Safe Harbour Decision*, EUROPEAN PARLIAMENT THINK TANK (2015), https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2015)569050.

119 *See id.*; *see also* Case C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 ECLI:EU:C:2015:650, ¶¶ 94-95 (Oct. 6, 2015); Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd*, *supra* note 81.

120 *Id.*

121 *See supra* note 117.

122 *Id.*

123 *Id.*

124 *Id.*

125 *Global Cross-Border Privacy Rules Declaration*, U.S. DEP'T OF COM., https://www.commerce.gov/global-cross-border-privacy-rules-declaration [https://perma.cc/3D9H-LDHH]; *see also* https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Declaration-2022.pdf.

jurisdictions.[126] Voluntary measures such as transparency reports, now common among major tech firms like Google, can enhance credibility.[127] Notably, some EdTech providers have begun adopting these practices. Coursera, for example, maintains an ISO/IEC 27001:2013–certified information security management system and undergoes annual third-party independent audits, including SOC 2 Type II assessments and third-party penetration testing.[128]

EdTech platforms are not neutral tools but complex ecosystems that mediate social, technical, and political relationships.[129] Because they encode particular values and priorities, they actively shape students' educational experiences. Voluntary compliance mechanisms can help reduce the risks of biased algorithms and data misuse by promoting standards for fairness, data minimization, and transparency.[130] The Student Privacy Pledge, launched in 2014 and signed by nearly 400 companies before its retirement in April 2025, represents an early attempt at such collective self-regulation.[131]

Implementing meaningful self-regulation requires a multistakeholder approach as a "coalitional project."[132] Because no single actor fully understands or controls how educational data systems operate, effective governance depends on incorporating the perspectives of educators, students, administrators, policymakers, and civil society organizations. Self-regulatory efforts benefit from drawing on these diverse viewpoints to identify risks and define practical safeguards. In fact, the Future of Privacy Forum's work on student data consolidated diverse viewpoints to develop practical guidelines that balance innovation with privacy protection.[133]

Self-regulation can complement international guidelines and safe-harbor certification frameworks. For EdTechs subject to U.S., EU, and Chinese laws, strong self-regulatory practices signal

---

126 *See, e.g.*, ISO/IEC 27701:2019, *Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines*, INT'L STANDARD (Aug. 2019), https://www.iso.org/standard/71670.html.

127 *Transparency Report: Government Requests to Remove Content*, GOOGLE, https://transparencyreport.google.com/government-removals/overview [https://perma.cc/63M5-SFZG].

128 Coursera, Inc., *Annual Report Form 10-K* 59 (Dec. 31, 2024), https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_COUR_2024.pdf.

129 Nichols & Dixon-Román, *supra* note 14, at 322.

130 *See supra* note 128; *see also infra* notes 131, 133.

131 Future of Privacy Forum & Software & Information Industry Association, *About the Pledge*, Student Privacy Pledge (Apr. 25, 2025) https://studentprivacypledge.org/ [https://perma.cc/ZBE9-W4LR].

132 *Supra* note 129, at 323.

133 Future of Privacy Forum, *Future of Privacy Forum Releases Policymaker's Guide to Student Data Privacy*, FUTURE OF PRIV. F. (Apr. 5, 2019), https://fpf.org/press-releases/future-of-privacy-forum-releases-policymakers-guide-to-student-data-privacy [https://perma.cc/LM29-N3R4].

responsible data handling and good-faith compliance while as broader legal harmonization efforts remain uncertain.

CONCLUSION

The cross-border conflict over educational data reflects competing approaches to data governance in today's digital world. The three kings—EdTech companies, national regulators, and law enforcement agencies—all pursue valid goals: companies seek sustainable business operation, regulators aim to protect citizens' rights, and law enforcement wants to investigate crimes. Nevertheless, as this Note has attempted to show, their respective approaches may create legal tensions that leave platforms caught in compliance uncertainties.

Digital governance requires cooperation, flexibility, and shared infrastructure. International guidelines can provide common languages to bridge legal differences; safe-harbor certification frameworks offer lawful, transparent paths for cross-border data sharing; and strong industry standards can create consistent recognized standards beyond legal requirements.

Getting there will take compromise. EdTech companies can adopt privacy-by-design principles and greater transparency; regulators should respect diverse regulatory systems; and law enforcement agencies should accommodate oversight and operate within frameworks that include clear safeguards. As AI technologies increasingly mediate education, the stakes for student privacy and cross-border data governance will grow higher. This isn't a choice between privacy and innovation, but a challenge to design systems that uphold rights while enabling the responsible use of data to support modern learning. The curtain isn't falling on this debate—it's rising on the next act of global data governance.