Navigating Children Privacy Laws in Cross-Border Digital Advertising: United States and India Regulatory Challenges and Solutions

Submission: *Policy Brief*
Author: *Ayushi Kapoor*

Acknowledgement

The author wishes to acknowledge the invaluable mentorship of Laurie Miller, Capstone Instructor, Cornell University, whose expertise in public policy and steadfast support were integral to the development of this policy brief. Her critical insights and encouragement significantly shaped the research focus and strengthened the analytical depth of this work.

The author also extends sincere thanks to Sara Akbar, Senior Director for Legislative Affairs and Technology Policy, US-India Strategic Partnership Forum, whose oversight and strategic input meaningfully informed the policy framework and contributed to the clarity and coherence of the recommendations.

Gratitude is further extended to the industry and policy experts who generously shared their insights during interviews and consultations; their identities remain confidential in accordance with their preference for anonymity. Their nuanced understanding of the evolving AdTech ecosystem and regulatory challenges in both the United States and India provided essential context that informed this comparative analysis.

The author is responsible for any errors or oversights. It is hoped that this policy brief contributes meaningfully to the ongoing dialogue around data protection, child safety, and responsible digital innovation.

Introduction

Cross-border promotional campaigns have become important for businesses aiming to expand their global footprint. The marketing efforts amplify beyond the national or domestic boundaries, leveraging digital advancements to engage with international audiences. Cross-border commerce is projected to reach $7.9 trillion by 2030, showcasing the significance of the growing global market. This expansion offers businesses the chance to explore new markets, expand their customer base, and enhance brand visibility worldwide (GameCloud, 2024).

The evolution of cross-border e-commerce indicates the driver of global economic growth (Wei et al., 2019). In recent years, cross-border e-commerce research has gained increasing attention due to the industry's rapid expansion. Furthermore, the early adopters of third-party platforms in cross-border e-commerce create benefits of learning effects and lower conversion costs through online search and data mining (Deng and Wang, 2016). This kind of edge helps them address challenges related to costs, technology, and market inconsistencies more effectively than late candidates (Zhu et al., 2025). For decades, children and teenagers have been targeted through various media advertising channels. The advertising expenditure for teens and children reached $3.2 billion for traditional media and $900 million for digital platforms in 2018 (Radesky et al., 2020).

Children's Online Privacy in a Data-Driven World

Ensuring online safety has become a priority in regulatory efforts across many societies. However, managing digital risks remains a complex structure due to various international, national, public, and private stakeholders. While addressing online risks for children, it is imperative to create a balance between safeguarding them from harm and upholding their fundamental rights and freedom. Moreover, regulations should not only protect children from threats by the digital industry but also promote a supportive environment where they can explore, learn, develop skills, and engage with the internet safely and meaningfully.

Data on children is collected throughout their education, and this entire process has been intensified with the increasing use of educational technologies for teaching, safety, and administration. This kind of data is often sensitive, covering areas such as race, family hardship, mental health, and disabilities, and can be analyzed to uncover personal details about each child. Whether mandated by the government or chosen by schools, this data often ends up in a global commercial ecosystem, extending far beyond the educational system. However, the expected benefits, such as personalized learning or learning analytics, do not always come to fruition (Livingstone et al., 2024).

Research on children's privacy and data protection is evolving, yet critical gaps remain in understanding the role of technology in shaping privacy norms. As global tech companies play a role in shaping policy and culture, it is essential to examine whether they are unifying or diversifying cultural attitudes toward children's privacy. Their influence goes beyond data collection to shaping the very foundations of future privacy policies. Currently, the challenge lies in balancing innovation with ethical responsibility– how can children not only benefit from the data collected about them, but also have a say in shaping the policies that govern their digital lives (Livingstone et al., 2024)? Understanding this dynamic will be the answer

to ensure privacy frameworks that protect children's rights while adapting to advertising technology.

Advertisement Technology in Global Marketing Strategies

The global privacy landscape is evolving with different regulatory frameworks across the world, which are aimed at restricting data usage, creating significant challenges for the AdTech industry which heavily relies on data-driven insights (Parekh, 2025).

Cultural and behavioral differences are important to understand the global markets, as strategies that work in one region may not be effective in another. AdTech companies use data analytics to bridge the gaps, providing insights into regional preferences, consumer behavior, and trends. They create hyper-personalized campaigns by adapting to the creative content, adjusting to the local language and cultural symbols, tailoring messages to regional purchasing habits and interests, and testing ad formats to identify the most effective approach for specific demographics (The Strategy Story, 2024).

Furthermore, the cross-border data flow restrictions vary from outright bans on international data transfers to requirements for prior consent or maintaining local copies. While governments determine their acceptable risk levels, data localization is often viewed as counterproductive, as it can stifle economic growth and trade. It has been identified that such restrictions can significantly undermine domestic investment, slow economic development, and reduce exports (Meltzer & Lovelock, 2018).

Differences in the United States and India

In the United States, the Family Educational Rights and Privacy Act (FERPA) safeguards the privacy of students' educational records by emphasizing informational privacy and requiring parental consent for data disclosure. Consequently, this places the responsibility of protecting children's data primarily on parents, which is debatable whether they can effectively provide informed consent in today's data-driven environment. In December 2023, the Federal Trade Commission (FTC) proposed updates to the Children's Online Privacy Protection Act (COPPA), which could impact EdTech providers by banning commercial use of children's data and implementing additional protective measures (Livingstone et al., 2024).

Another component is Section 230 of the Communications Act of 1934, enacted through the Communications Decency Act of 1996, that offers limited immunity to online platforms and users from liability for third-party content. It shields platforms from various lawsuits based on their decisions to host or remove user-generated content, but it does not protect them from liability for content they create themselves. This immunity is defined by two main provisions: Section 230(c)(1), which prevents platforms from being treated as the publishers of user-generated content, and Section 230(c)(2), which protects platforms from liability when they remove content deemed harmful or objectionable in good faith. However, there are exceptions, including those for federal criminal law, intellectual property, certain privacy laws, and sex trafficking regulations. The courts have broadly interpreted Section 230, sparking debates about whether its protections are too expansive. Proposals for reforms have emerged, ranging from limiting immunity to encourage content removal to narrowing protections for content takedown to safeguard free speech. Any changes to Section 230 also open controversies to the First Amendment, particularly regarding the interventions by the government with editorial discretion or liability for speech-related decisions. Essentially,

even if Section 230 were to be repealed, the First Amendment could still offer some protections for content moderation practices (Gov Info, n.d; Department of Justice, 2023).

In India, the laws concerning children's online privacy are insufficient. The key regulation is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which requires entities collecting sensitive information or data, which includes children's information, to provide a privacy policy outlining the data's purpose and usage. Additionally, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose certain obligations on social media platforms to protect users, including children. However, these regulations are not comprehensive for protection (Mone & T., 2023).

Children's Privacy for Tech Industry Laws: United States and India

United States

1. **Children Online Privacy Protection Act (COPPA), 1998:**

   The Act protects children's privacy by giving parents control over the collection of their children's personal information. As part of the Act, it requires websites and online services targeting children under 13– or knowingly collecting their data, to: a) Inform parents about data practices. b) Get verifiable parental consent, c) Let parents stop data collection or use, d) Allow parents to access their child's information, e) Limit data collection to what is necessary. f) Keep children's data secure. Furthermore, the Act also encourages industry self-regulations through a "safe harbor" provision, letting companies and organizations create their own compliance guidelines (15 USC 6501: Definitions, n.d.).

2. **COPPA (Amendments), 2013:**

   The Amendments of 2013 to the COPPA rule focused on and addressed evolving digital behaviors among children, especially the increased use of mobile devices and social media. The key revisions included broadening the definition of "operators" to cover third-party services like plug-ins and ad networks that collect data from child-directed sites, and expanding what constitutes a "child-directed website." They also allowed certain mixed-audience websites to differentiate users by age and comply only with those under 13. The definition of "personal information" was updated to include geolocation data, media files with a child's image or voice, and persistent identifiers. Parental notice requirements were streamlined for timeliness and clarity, and the list of approved methods for obtaining the required verifiable parental consent was expanded. The amendments introduced new exceptions for internal operational use of persistent identifiers and reinforced data security obligations, including strict rules on data sharing, retention, and deletion. Lastly, the Federal Trade Commission (FTC) enhanced oversight of COPPA-approved self-regulatory safe harbor programs (Children's Online Privacy Protection Rule, 2013).

3. **COPPA (Updates), 2025:**

   The updated COPPA Rule, designed to protect children's privacy online, will come

into effect on June 23, 2025. Online operators subject to the rule will have until April 22, 2026, to achieve full compliance with the new requirements. The following are the key changes (Children's Online Privacy Protection Rule, 2025):

A) Introduction of a new definition for "mixed audience website or online service" allowing operators to collect personal information for limited purposes-such as providing parental notice, responding to a child's specific request, or protecting a child's safety— without obtaining parental consent before determining age, provided the information is not used or disclosed for another purpose.

B) Modification of the definition of "online contact information" to include mobile telephone numbers, provided they are used solely to send text messages to parents in connection with obtaining parental consent.

C) Expansion of the definition of "personal information" to include biometric identifiers (example: fingerprints, retina patterns, facial templates), and government-issued identifiers (example: passport numbers, state ID numbers, birth certificates).

D) Enhanced notice requirements mandating that operators provide parents with detailed information about third-party data sharing and specific data collection purposes. Operators must identify third-party data recipients by name and category and disclose data retention policies in online notices.

E) Introductions of new consent mechanisms, including the "Text Plus" method, allowing parents to give consent via text messages if paired with additional verification steps (example: confirmatory text, or follow-up via postal address or phone call), and requiring notice that consent can be revoked.

F) Requirement for operators to establish and maintain a written data retention policy concerning children's personal information and to implement comprehensive information security programs.

G) The COPPA Safe Harbor program permits industry groups to develop self-regulatory guidelines that align with or surpass COPPA Rule protections, subject to FTC approval. Under recent amendments, approved programs must now publicly disclose their membership lists and provide additional reporting to the FTC.

4. **Kids Online Safety Act (KOSA):**

The KOSA bill, which has been introduced, sets out requirements to protect minors from online harms. The requirements apply to covered platforms, which are applications or services (example: social networks) that connect to the internet and are likely to be used by minors. However, the bill exempts internet service providers, email services, educational institutions, and other specified entities. Covered platforms must take steps to protect minors by designing and operating their services to prevent harms like sexual exploitation and bullying. They must offer safeguards for minors' data and tools for parents to supervise use. The platforms are also required to

disclose their use of personalized recommendations and advertising, allow harm reporting, avoid promoting age promoting age-restricted products to minors, and report annually on potential risks. A large website, search engine, and internet applications must inform users about algorithmic content delivery and provide a version that does not rely on user-specific data. The enforcement of this act falls to the FTC and the states. The bill has also called for the National Academy of Sciences study, set up an advisory council, and study the risks of harm to minors by the use of social media and other online platforms. (S.1409 - Kids Online Safety Act, n.d.).

5. **Kids Off Social Media Act (KOSMA):**

   The KOSMA 2025 bill has been introduced and is designed to protect children and teens from the harmful effects of social media. It prohibits children under 14 from having social media accounts and requires platforms to delete their data and provide it upon request within 90 days of account termination. For users aged 12-16, the Act bans the use of personal data in personalized recommendation systems but allows the use of limited non-personal data. Platforms are not required to externally verify the age unless necessary for compliance, and enforcement is overseen by the FTC and the state attorney general. Title II, the Eyes on the Board Act, mandates federally funded K-12 schools to block student access to social media on school networks and devices, with strict compliance deadlines and reporting requirements to the FCC. Title III ensures that if any part of the Act is invalidated, the rest remains enforceable (S.278 - Kids off Social Media Act, 2025).

India

1. **Digital Personal Data Protection Act (DPDP Act)- (Mali, n.d.):**

   A) Section 9 of the DPDP Act outlines the obligations of Data Fiduciaries when processing children's personal data. It mandates that verifiable consent must be obtained from a parent or lawful guardian before processing such data. The section clarifies that "parent consent" includes that of a lawful guardian. It prohibits any data processing that could negatively impact a child's well-being and specifically bans tracking, behavioral monitoring, or targeted advertising directed at children. However, exemptions may apply to certain classes of Data Fiduciaries or for specified purposes under prescribed conditions. Additionally, the Central Government may exempt a Data Fiduciary from the obligations of obtaining consent or avoiding tracking/advertising if it deems the data processing is conducted in a verifiably safe manner and specifies an exemption age threshold.

   Explanation: Digital platforms used to serve the children, like social media, educational tools, games, and health applications, must follow strict rules to protect minors' personal data. These platforms are required to obtain parental consent before allowing users under 18 to register, make purchases, or share sensitive information such as names, preferences, or health data. This responsibility places a greater burden on Data Fiduciaries who must implement systems for verifying consent, manage compliance costs, and avoid legal and reputational risks. At the same time, parents (as Data Principals) play a key role in overseeing their children's digital interactions to safeguard their privacy. Core protections include mandatory parental consent, a ban on behavioral targeting

for ads, limits on data collection, secure storage and encryption, and deletion of data once it's no longer needed or the child reaches adulthood (all explained in clear and child-friendly terms).

B) Section 16 empowers the Central Government to restrict, via notification, the transfer of personal data by a Data Fiduciary to any specified country or territory outside India. However, the provision does not affect the applicability of any existing Indian laws that provide greater protection or impose restrictions on such cross-border data transfer.

C) Rule 12(4) states that Significant Data Fiduciaries must ensure that certain categories of personal and traffic data, as identified by the Central government based on committee recommendations, are not transferred outside India.

D) Rule 14 states that any transfer of personal data outside India whether processes within India or abroad in connection with offering good or services to individuals in India– is allowed only if the Data Fiduciary complies with specific requirements set by the Central Government. These restrictions focuses on Data Sovereignty, Cross-Border Risks and National Security.

Explanation: It governs the cross-border data transfers to safeguard the personal data of Indian customers to suggest products and transfer that data to its international servers; it must follow any restrictions set by the Indian government. Similarly, tech companies that collect user behavior data and share it with international teams must comply with strict conditions to prevent data misuse. Payment platforms that store transaction details on foreign servers are also required to align with India's privacy regulations. While the rule strengthens data protection, it can pose challenges for companies, such as increased compliance costs due to the need for advanced data systems, potential delays in operations due to regulatory approvals, and legal conflicts between Indian laws and those in other countries.

E) Rule 11 outlines the exemptions from certain obligations when processing children's personal data. Specifically, the requirements under sub-sections (1) and (3) of Section 9 of the Act, which pertain to obtaining parental consent and prohibiting tracking or targeted advertising, do not apply in two cases: i) when the processing is done by specific classes of Data Fiduciaries listed in Part A of the Fourth Schedule, subject to stated conditions; and ii) when the processing is for specific purposes listen in Part B of the Fourth Schedule, also subject to the specified conditions.

Explanation: The designated categories of Data Fiduciaries– such as schools or healthcare providers listed in Part A of the Fourth Schedule are not required to obtain verifiable parental consent or strictly limit data use to lawful purposes when processing children's data. These exemptions facilitate essential functions like enrollment or immunization, provided the entities meet the stringent conditions set in Part A to safeguard against misuse. Similarly, Rule 11(2) allows exemption for specific purposes detailed in Part B of the Fourth Schedule, such as public welfare initiatives, national security, or vital functions. This enables smoother implementation of government programs like welfare distribution or

issuing age-based certifications, as long as the processing aligns with the conditions defined in Part B.

Note: The consultation period for draft rules ended on February 18, 2025.; extended by March 5, 2025. S. Krishnan, the Ministry of Electronics and IT Secretary, mentioned that the final rules of the DPDP Act are likely to be out within six to eight weeks.

Comparative Understanding of the Laws

1. **Key Takeaways:**

   Both the United States and India prioritize protecting children's personal data online through verifiable parental consent, prohibition on behavioral targeting, and a strong emphasis on data security and minimization. They share a common intent: ensuring digital platforms operate responsibly when dealing with minors. Both frameworks aim to limit misuse, enforce accountability, and require that platforms clearly communicate how children's data is handled.

2. **Key Differences:**

   A stark difference lies in the age threshold- COPPA protects children under 13, while DPDP covers individuals under 18, making India's framework broader in scope. EdTech and mixed audience site consideration are more mature and detailed under COPPA, while DPDPA lacks explicit details in these areas. Furthermore, in terms of data transfer, COPPA allows international data flow under compliance, whereas DPDP introduces strict localization rules and government oversight for cross-border data transfers. Additionally, COPPA includes a Safe Harbor mechanism where industry groups can self-regulate under FTC approval, while DPDP operates through government notifications and rule-based exemptions, without formal safe harbor protections.

Key Findings

Conversations with a Former United States Government Privacy Laws and Technology Affairs Expert and a Technology Industry Council Expert have shaped the key findings.

1. **Global Privacy Standards and EU Influence**:

   A) Companies in the industry largely rely on compliance measures set by the European Union (EU), but they do not fully implement what the General Data Protection Regulation (GDPR) mandates, as the EU operates on an opt-in model while the U.S. follows an opt-out approach. This difference in approach creates challenges in aligning global frameworks effectively. Compliance standards are largely regional, with varying rules and frameworks depending on the geographic area, which makes it difficult for companies to adopt a unified global privacy strategy.

B) The EU's GDPR has become a global compliance standard for privacy laws, especially as it sets a comprehensive framework for protecting personal data. While many companies initially embraced GDPR as a roadmap, there has been growing resistance, particularly from U.S. companies, who view it as an overreach and an imposition. Countries like Brazil and India have adopted select parts of the GDPR framework, which introduces further complexity for multinational firms. Additionally, there is a noticeable shift in the perspective of U.S. companies toward data localization, given the growing number of international regulations that impact their operations. The ongoing tension between the U.S. and EU, particularly in light of tariffs and trade wars, makes alignment on global privacy standards increasingly difficult.

2. **Impact of Ad-Tech Regulations:**

A) Ad-Tech regulations such as COPPA, KOSA, KOSMA, and India's DPDP Act are generally not seen as stifling innovation but rather as creating a more level playing field for companies. Many organizations welcome these regulations as they help establish clear standards for the industry. However, COPPA, in particular, has been criticized for being outdated and not evolving quickly enough, with delays in its update due to bureaucratic processes.

B) In India, there is still uncertainty about the DPDP Act and how it is being enforced, creating challenges for companies in the ad-tech space.

3. **Geo-location, Data Sensitivity, and Reporting:**

A) While companies recognize the business value of collecting user data, they are becoming increasingly aware of the associated risks and liabilities, especially regarding the storage of sensitive information. If governments request access to private data, companies have established processes for handling such requests. Cyber incident reporting timelines also vary significantly between countries, with India requiring reports within 6 hours, while the U.S. allows up to 72 hours. This discrepancy has led to push back from companies, questioning whether the focus should be on securing the system or reporting the incident. Additionally, governments often lack ideal frameworks for overseeing data deletion processes, making effective oversight and accountability challenging.

4. **Business Incentives for Compliance in Protecting Children's Data:**

A) Companies are increasingly motivated to go beyond the minimum legal compliance in protecting children's data, especially as stricter regulations can lead to higher user engagement and trust. Civil penalties, such as those under COPPA, force companies to adhere to the rules to avoid fines. Companies conduct cost-benefit analyses, weighing the potential financial consequences of non-compliance against the costs of ensuring compliance, which ultimately drives them to implement stronger privacy protections for children's data.

5. **U.S.–India collaborations in Privacy Laws:**

A) U.S. privacy laws are sectoral, with distinct regulations for sectors such as finance, education, and health. California's privacy law (CCPA) is a key example of significant state-level regulation. U.S.–India collaborations primarily focus on cross-border data flow and the impact of data localization, particularly regarding India's DPDP Act. U.S. companies have raised concerns about data localization, arguing that it hinders innovation and operational feasibility. Enforcement mechanisms are evolving, with international collaborations like the Global Cross-Border Privacy Rules Forum (CBPR Forum). However, discussions on India joining the CBPR under the Biden administration have yielded limited results. U.S. regulations, particularly through the Department of Justice (DOJ), categorize data into "prohibited" (national security-related) and "restricted" categories, which further complicates international data governance.

6. **India Market- Regulatory Opportunities and Challenges:**

A) Privacy law negotiations and regulatory requirements in India remain complex and unpredictable, with the potential for regulatory shifts. One significant discussion currently underway is lowering the digital age of consent to 16, which contrasts with the U.S. debate focusing on children's mental health, phone usage, and the banning of phones in schools. In response to these discussions, companies like have begun reconsidering the 13+ age benchmark for digital platform use, signalling a global recalibration on how youth privacy is handled.

7. **Existing Collaborations:**

A) International collaborations, particularly those between the U.S. and other countries, play a significant role in privacy law discussions. For instance, the FTC has participated in regional conferences like the Asia Pacific Privacy Authorities (APPA), where cross-border data protection and mutual priorities are discussed. These collaborations involve enforcement actions and data protection exercises, similar to how military organizations conduct routine exercises. However, achieving consensus can be challenging and time-consuming due to the different technological development paces in various countries. Organizations like the Organization for Economic Development (OECD) also contribute by managing regional networks, but the complexity of aligning multiple stakeholders can slow the progress.

Recommendations

1. **Launch Bilateral "Joint Data Sweeps" modeled on Joint Military Exercises**:

Drawing from the military domain where nations routinely engage in joint naval or air force drills to build interoperability and mutual trust, U.S. and India should institutionalize "Joint Data Sweeps". These cyber drills would involve coordinated audits of AdTech firms, especially those targeting children, to detect violations and inconsistencies in data protection practices. These sweeps should consider the following: a) Simulate real-world scenarios, such as child data breaches or algorithmic profiling to test how platforms respond. b) Include a randomized audit protocol to verify whether companies have deleted children's data when requested or upon account closure while addressing the growing concern of "dark retention". c)

Develop cross-verifiable deletion standards where metadata or logs related to deletion processes can be reviewed by both nations without breaching secrets.

A) It incentivizes India to join the Action Plan for the Global Privacy Enforcement Network (GPEN) for showcasing India's digital privacy infrastructure.

B) The joint drills must be led by the U.S. FTC and India Ministry of Electronics and Information Technology (MeitY).

C) In light of China's expanding technology and AI influence, this bilateral collaboration can serve as a counterweight, promoting accountability, democratic data norms and safeguarding the digital future.

2. **Create Adaptive, One-Page Compliance Protocols for Technology-Focused Companies:**

With the pace of technological advancement in AI-powered advertising and behavioral tracking, children's privacy laws must be easy to comprehend.

A) Develop standardized one-page compliance summaries that clearly outline obligations under COPPA and DPDP Act specific to children's privacy laws, and any emerging bilateral frameworks.

B) These summaries should be co-branded by both governments.

C) Simplified resources lead to a boost in compliance rates, especially among startups and mid-sized platforms.

3. **Use Bilateral Tech Engagements to Incentivize Privacy-First Business Models:**

The recent removal of India's 6% equalization levy or "Google Tax" (India Today, 2025) signals a more cooperative digital trade environment with the U.S., especially as both nations align through the Global Minimum Tax (OECD) framework (Organisation for Economic Co-operation and Development, n.d.). This signaled the following: a) India is moving toward international cooperation rather than unilateral digital taxation. It gave global tech firms greater predictability in tax compliance which encourages U.S. companies to engage in India with fewer obstacles. This shift reduces compliance friction for U.S.-based AdTech companies and creates a more collaborative policy space.

A) Leverage this momentum to embed children's privacy safeguards into trade and tax agreements: companies that demonstrate strong child data governance should receive tax incentives/credits or be prioritized in fast-track compliance approvals.

4. **Facilitate Cross-Border Regulatory Sandboxes for Children-Centric AdTech:**

Encourage the establishment of cross-border regulatory sandboxes for companies innovating in the children's digital ecosystem (example: educational applications,

children-focused cloud platforms). These sandboxes, supported by both governments, would allow the firms to:

A) Test new technologies under bilaterally agreed privacy constraints.

B) Access feedback from both regulatory regimes in real-time.

C) Reduce go-to-market friction and ensure ethical product development.

D) It can also anticipate new threats and recommend timely legislative updates.

5. **Empower existing bilateral and multilateral forums and agreements:**

   To improve the U.S.-India engagement on privacy laws, U.S.-India COMPACT (Catalyzing Opportunities for Military Partnership, Accelerated Commerce & Technology), and U.S.-India Initiative Critical and Emerging Technology (iCET) should be leveraged to foster focused discussion on AdTech and evolving privacy regulations. Additionally, the QUAD forum can play a strategic role in aligning data policy priorities among member countries, including U.S. and India, to promote a framework incorporating broader digital and manufacturing cooperation, leading to a unified approach to privacy and data security.

<u>Drawbacks and mitigation strategies</u>

1. **Launch Bilateral "Digital Privacy Sweeps" Modeled on Joint Military Exercises:**

   Drawback:
   While joint data privacy sweeps can promote accountability, they may encounter significant diplomatic and operational resistance. Unlike military drills that are governed by formal treaties and long-standing security alignments, data audits intrude into corporate systems, raising legal concerns around data localization, cross-border access, and intellectual property. India, which prioritizes digital sovereignty under its DPDP Act, may view U.S. regulatory involvement as foreign interference in domestic digital governance. Meanwhile, U.S. firms may resist Indian scrutiny over proprietary algorithms or retention systems. Without mutual legal infrastructure or enforceable cooperation agreements, these sweeps risk becoming symbolic rather than substantive, and could provoke backlash from industry lobbies citing overreach and data protection conflicts.

   Mitigation:
   Reframe Digital Privacy Sweeps as Confidence-Building Measures: Model bilateral audits after joint military exercises, focusing on transparency, reciprocity, and pilot-phase collaboration to demonstrate mutual accountability while avoiding bureaucratic sprawl.

2. **Create Adaptive, One-Page Compliance Protocols for Tech Companies**:

   Drawback:
   Simplified compliance summaries may help companies navigate fragmented legal systems, but they risk oversimplifying nuanced obligations, especially in sectors like AdTech where rules vary significantly across jurisdictions and evolve rapidly.

Startups and small firms might rely solely on these documents, bypassing full legal reviews and inadvertently exposing themselves to non-compliance penalties or litigation. Moreover, these one-pagers could create a false sense of regulatory assurance without capturing technical requirements like encryption protocols, age-verification standards, or third-party data transfer clauses. Regulatory bodies may then face legal liability for omissions or inaccuracies, especially if companies cite these tools as evidence of attempted good-faith compliance.

Mitigation:
Layer Compliance Without Overcomplication: Keep one-pagers as a front-facing tool, but smartly link them to expandable guidance tailored to legal and tech teams. A light compliance affirmation process preserves simplicity while reinforcing seriousness.

3. **Use Bilateral Tech Engagements to Incentivize Privacy-First Business Models:**

Drawback:
Tying privacy standards to bilateral economic incentives, such as market access or tax benefits, is a compelling strategy-but it may lead to regulatory capture and selective enforcement. Large AdTech firms could influence policy design to suit their own privacy interpretations, creating inconsistent enforcement or competitive disadvantages for smaller companies with fewer lobbying resources. Additionally, verification of "privacy-first" claims--such as behavioral ad restrictions or ethical data minimization-requires robust technical audits, which few agencies currently have the capacity or tools to conduct regularly. This approach also risks politicizing privacy compliance, turning it into a negotiable trade asset rather than a non-negotiable rights-based mandate.

Mitigation:
Privacy Incentivize Without Overregulation: Anchor business incentives in clear, independently assessed privacy standards and transparency metrics. Avoid excessive certification by leveraging existing privacy labels and focusing on public-facing impact disclosures.

4. **Facilitate Cross-Border Regulatory Sandboxes for Child-Centric AdTech**

Drawback:
Cross-border regulatory sandboxes may promote innovation in safe-digital environments, but they face practical and jurisdictional limitations. Regulatory sandboxes typically rely on temporary waivers or exceptions from standard laws, which may not be recognised across national boundaries. For instance, a child-facing app cleared in a U.S.-India sandbox may still violate the EU's GDPR or fail COPPA's evolving interpretations. There is also a danger of these sandboxes being exploited as experimental loopholes where companies can test intrusive techniques under the guise of innovation. Without harmonized child data definitions, agreed ethical frameworks, and active public oversight, these sandboxes may undermine core privacy protections, especially for vulnerable user groups like children.

Mitigation:
Contain Sandbox Risk, Don't Cripple It: Structure regulatory sandboxes with minimal

viable guardrails-limited duration, ethical review checkpoints, and post sandbox evaluations-to preserve their agility and real-world testing value.

5. **Leveraging Platforms like COMPACT and iCET for Privacy Law Dialogue:**

   Drawback:
   While the U.S.-India COMPACT and iCET initiatives offer diplomatic frameworks for technology cooperation, expanding their scope to include child privacy and AdTech could dilute their current focus and lead to bureaucratic stalling. COMPACT is primarily oriented toward trade facilitation and digital economy development, while iCET focuses on critical technologies like AI, quantum computing, and defense tech. Introducing consumer-level regulatory issues-especially contentious ones like behavioral advertising-into the platforms may trigger institutional pushback from stakeholders unwilling to expand their mandates. There's also a risk that such dialogues become high-level and non-binding, lacking actionable outcomes for companies and regulators on the ground.

   Mitigation:
   Leverage existing frameworks like COMPACT and iCET to establish focused, high-impact working groups on child-centric AdTech. Embed Track 1.5 diplomacy-involving think tanks, academia, and civil society-to bridge technical nuance with diplomatic dialogue. Industry-regulator advisory councils should be institutionalized within these groups to moderate expectations, ground policy in operational realities, and ensure that privacy-forward innovation remains both commercially viable and rights-aligned.

Conclusion

For industry and government stakeholders, aligning AdTech practices with child privacy standards is critical to building trust and avoiding regulatory backlash. In the U.S., compliance with COPPA and growing scrutiny of behavioral advertising demand proactive transparency, while India's DPDP Act signals a shift toward consent-based data governance. Cross-sector collaboration and investment in privacy-preserving technologies will be key to ensuring ethical innovation and regulatory alignment.

References

15 USC 6501: Definitions. (n.d.). https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

Action Plan for the Global Privacy Enforcement Network (GPEN) | Global Privacy Enforcement Network. (n.d.). https://privacyenforcement.net/node/2

Children's online Privacy Protection rule. (2013, January 17). Federal Register. https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule

Children's online Privacy Protection rule. (2025, April 22). Federal Register. https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule

DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996. (2023, May 8). https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996

GameCloud. (2024, October 14). *Cross-Border Promotional Campaigns: the future of global marketing*. GameCloud. https://gamecloud-ltd.com/cross-border-promotional-campaigns-the-future-of-global-marketing/

Radesky, J., Chassiakos, Y. R., Ameenuddin, N., & Navsaria, D. (2020). Digital advertising to children. *PEDIATRICS*, *146*(1), e20201681. https://doi.org/10.1542/peds.2020-1681

Global Cross-Border Privacy Rules Declaration. (n.d.). U.S. Department of Commerce. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

GovInfo. (n.d.). https://www.govinfo.gov/app/details/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec230/summary

India Today. (2025, March 25). India likely to remove 6% Google tax from April 1, tech giants to benefit. *India Today*. https://www.indiatoday.in/business/story/india-to-remove-6-percent-google-tax-what-is-it-how-does-it-impact-tech-giants-2698623-2025-03-25

Kids Off Social Media Act | U.S. Senator Brian Schatz of Hawaii. (n.d.). Brian Schatz. https://www.schatz.senate.gov/kosma

Livingstone, S., Lievens, E., Graham, R., Pothong, K., Steinberg, S., & Stoilova, M. (2024). Children's Privacy in the Digital Age: US and UK Experiences and Policy Responses. In *Handbook of Children and Screens* (pp. 491–497). https://doi.org/10.1007/978-3-031-69362-5_67

Mali, A. P. (n.d.). *Authentic source of the DPDPA, 2023*. DPDPA. https://dpdpa.com/

Meltzer, J. P., & Lovelock, P. (2018, March 20). Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia. *Brookings*.

https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/?utm_source=chatgpt.com

Mone, V., & T., A. (2023). Online Privacy and Children in India: A Socio-Legal Study of Parental Concerns, Regulations and Education. *Madhya Pradesh Journal of Social Sciences*, *28*(3), 143–156 https://research-ebsco-com.proxy.library.cornell.edu/c/u2yil2/viewer/pdf/ey5pzy5fwr

Parekh, V. (2025, February 13). *Council Post: How big incoming privacy laws and trends will shape AdTech*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2025/02/13/how-big-incoming-privacy-laws-and-trends-will-shape-adtech/

Rubinstein, I. (n.d.). PRIVACY AND REGULATORY INNOVATION: MOVING BEYOND VOLUNTARY CODES. *NYU School of Law*. https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00103/544506-00103.pdf

Organisation for Economic Co-operation and Development. (n.d.). *Global Minimum Tax*. https://www.oecd.org/en/topics/global-minimum-tax.html

S.1409 - Kids Online Safety Act. (n.d.). Congress.gov. https://www.congress.gov/bill/118th-congress/senate-bill/1409

The Strategy Story (2024, December 5). How Adtech companies drive global brand expansion - The Strategy Story. *The Strategy Story - Simplifying Business Strategies*. https://thestrategystory.com/blog/how-adtech-companies-drive-global-brand-expansion/

Wei, K., Li, Y., Zha, Y., & Ma, J. (2018). Trust, risk and transaction intention in consumer-to-consumer e-marketplaces. *Industrial Management & Data Systems*, *119*(2), 331–350. https://doi.org/10.1108/imds-10-2017-0489

Zhu, X., Chen, H., Xiang, E., & Qi, Y. (2025). *Digital transformation and corporate green technology transfer: The moderating effect of executive green cognition*. https://www.sciencedirect.com/science/article/pii/S1544612325002995?via%3Dihub