SAFE HOUSE
PROJECT

Safe House Project Policy Spotlight

Translating Emerging Federal and State Policy into Practice

Ethical AI and Technology in the Fight Against Human Trafficking

Advancing Responsible, Survivor-Centered Identification and Response Infrastructure

June 2026
Policy Brief

Executive Summary

Human trafficking is increasingly technology-enabled, adaptive, and cross-jurisdictional, yet the systems designed to identify and respond to victims have not kept pace (Bureau of Justice Statistics [BJS], 2025; Europol, 2023). Trafficking networks now rely heavily on digital platforms, encrypted communication channels, and online marketplaces to recruit, control, and exploit individuals (U.S. Department of State, 2025). At the same time, technology presents one of the most significant opportunities to improve victim identification, strengthen reporting pathways, and enable coordinated, real-time response across systems.

Despite this potential, many existing reporting and referral systems still rely heavily on single-channel or limited-access reporting models that do not fully reflect how victims and frontline professionals actually seek help today. Safe House Project's own Simply Report platform demonstrates the scale of unmet demand: individuals identified and connected to services grew from 534 in 2023 to 1,529 in 2024 and 2,466 in 2025—a nearly fivefold increase in three years—yet these figures represent only a fraction of actual trafficking activity due to persistent barriers in access, safety, and reporting (Safe House Project, 2026). These structural limitations contribute to persistent gaps in victim identification, delays in response, and fragmented coordination across agencies. As a result, significant federal and state investments in anti-trafficking efforts are not achieving their full impact.

At the same time, policymakers are increasingly focused on the role of technology in both enabling and combating trafficking. Emerging legislative efforts, including proposals such as the App Store Accountability Act, reflect growing concern regarding platform accountability, data governance, and the need for stronger safeguards in digital environments.

This policy brief examines the intersection of technology, policy, and trafficking response, outlining the need for a modern, ethical framework that ensures technology is deployed in ways that are secure, accountable, and centered on the needs of survivors. It also highlights how multi-channel, real-time reporting and coordination platforms can strengthen the front end of the response when aligned with policy, survivor safety, and existing system capacity.

Problem Statement

Human trafficking victims in the United States continue to be significantly under-identified and underserved, despite sustained investment across federal, state, and local systems. In FY2023, more than 2,300 individuals were referred to U.S. Attorneys for human trafficking offenses, yet these figures represent only a small portion of actual victimization nationwide (Bureau of Justice Statistics [BJS], 2025). In parallel, Safe House Project's own Simply Report platform identified and connected 534 individuals to services in 2023, growing to 1,529 in 2024 and 2,466 in 2025, a nearly fivefold increase in three years, underscoring both the unmet scale of demand and the persistent gap between identification, referral, and effective response when accessible, multi-channel reporting infrastructure is in place (Safe House Project, 2026). Research further indicates that victims often interact with multiple public-facing systems, including law enforcement, healthcare, education, and child welfare, prior to identification, yet too often are not recognized or connected to services at critical moments (National Academies of Sciences, Engineering, and Medicine [NASEM], 2020).

A central driver of this gap is the misalignment between how individuals seek help and how systems are designed to receive and respond to that information. Many existing reporting structures rely on a single access point, such as a hotline or centralized intake mechanism, which may not account for the realities of trafficking victims' experiences. Victims often face surveillance, restricted communication, language barriers, and safety constraints that limit their ability to engage through traditional channels (NASEM, 2020). As a result, systems that rely on a single reporting pathway risk excluding individuals who are unable to safely or effectively access those channels.

In addition to access limitations, systemic challenges persist in how information is shared and acted upon. Reporting and referral pathways are often fragmented across jurisdictions and agencies, resulting in delayed responses, inconsistent data sharing, and missed opportunities for intervention (U.S. Department of Justice, 2023). These gaps reduce the likelihood that victims will be connected to services when they are most vulnerable and limit law enforcement and service providers' ability to coordinate effectively.

At the same time, trafficking operations have become increasingly sophisticated and technology-driven. Traffickers leverage social media platforms, messaging applications, and digital financial systems to expand reach and evade detection (Europol, 2023). While technology is accelerating exploitation, many public systems have not yet adapted to fully leverage technology as part of the response.

Background

The United States' anti-trafficking framework was established through the Trafficking Victims Protection Act (TVPA), which created a comprehensive, victim-centered approach organized around prevention, protection, and prosecution. Over the past two decades, Congress has strengthened this framework through bipartisan reauthorizations and complementary legislation aimed at improving victim services, expanding detection, and enhancing coordination across systems.

A central component of the federal response has been the development of national reporting and referral infrastructure, including the National Human Trafficking Hotline. While centralized

reporting systems provide critical nationwide access, consistency, and 24/7 coverage, they are not designed to function as the sole entry point for all victims or reporters. Increasingly, individuals rely on multiple communication methods shaped by safety, access, and situational constraints, highlighting the need for complementary, multi-channel approaches within a coordinated ecosystem rather than replacing existing infrastructure.

At the same time, trafficking has become significantly more technology-enabled, with perpetrators leveraging social media platforms, encrypted messaging applications, and online marketplaces to recruit, advertise, and control victims (Europol, 2023). This shift has prompted growing concern among policymakers regarding the role of digital platforms in facilitating exploitation and the need for stronger safeguards, oversight, and accountability mechanisms.

Emerging legislative proposals, including the proposed App Store Accountability Act, reflect this shift. Although the proposal is still evolving, it signals growing interest in requiring greater oversight within digital app marketplaces, including stronger developer verification, increased transparency, and more deliberate risk mitigation for applications that may facilitate exploitation or other unlawful activity (Congressional Research Service, 2026). Policy discussions around the proposal have focused on measures such as:

- Mandatory developer identity verification and traceability requirements
- Platform responsibility to assess and mitigate high-risk applications
- Enhanced transparency and reporting obligations for app distribution ecosystems
- Requirements for app stores to take reasonable steps to prevent distribution of applications linked to criminal exploitation

These provisions signal a broader policy shift toward proactive platform accountability, moving beyond reactive enforcement to address systemic risk within digital ecosystems (Congressional Research Service, 2026).

This focus aligns with a broader set of federal legislative efforts aimed at strengthening detection, coordination, and survivor outcomes. The Enhancing Detection of Human Trafficking Act (H.R. 4307 / S. 2241), reported out of the House Education and Workforce Committee in February 2026, would require the Department of Labor to train its employees to identify trafficking victims, refer potential cases to the Department of Justice, and report annually to Congress on training effectiveness and case referral outcomes. The Trafficking Survivors Relief Act (Pub. L. No. 119-73) is now enacted law, creating a federal process for survivors to vacate convictions and expunge arrest records tied to offenses committed as a direct result of their trafficking. The Frederick Douglass Trafficking Victims Prevention and Protection Reauthorization Act of 2025 (H.R. 1144), passed out of committee by voice vote in July 2025 and still awaiting a House floor vote as of June 2026, would reauthorize the centerpiece of the federal anti-trafficking framework, expanding annual funding, establishing a survivor employment and education program, and strengthening prevention grants in high-trafficking areas. In April 2026, a bipartisan coalition of lawmakers, advocates, and survivors held a Capitol Hill press conference urging Speaker Johnson to bring the bill to the floor. A nearly identical version of the bill passed the House in 2024 with a 414–11 margin, reflecting broad bipartisan support (United States Congress, 2025).

Beyond trafficking-specific legislation, a wave of technology accountability measures in the 119th Congress is directly reshaping the digital environment in which trafficking operates. The App

Store Accountability Act (H.R. 3149 / S. 1586), introduced in May 2025 and advanced out of the House Energy and Commerce Committee in March 2026, would require app stores to verify user ages, mandate parental consent for minors' downloads, and establish platform accountability for high-risk applications (United States Congress, 2025). The STOP CSAM Act of 2025 (H.R. 3921 / S. 1829), which passed out of the Senate Judiciary Committee in June 2025, would pierce Section 230 immunity and create a civil cause of action allowing trafficking and exploitation victims to sue platforms that knowingly host, promote, or facilitate such offenses, with minimum damages of $300,000 plus attorney fees (United States Congress, 2025). The Kids Online Safety Act (S. 1748 / H.R. 6484), reintroduced in May 2025 with bipartisan Senate leadership, would require covered platforms to exercise reasonable care to prevent harms to minors, explicitly including sex trafficking of children among the covered harms triggering platform obligations (United States Congress, 2025).

These provisions signal a decisive shift in federal policy: platforms and app marketplaces are increasingly being treated as responsible actors within the trafficking prevention and response ecosystem.

Broader technology policy developments further reinforce this direction. State-level data privacy laws such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA), along with emerging artificial intelligence governance frameworks, reflect increasing expectations for transparency, accountability, and responsible data use. Updated California privacy regulations effective January 1, 2026, further reinforced requirements related to sensitive personal information, purpose limitation, and consumer control over certain data uses. Ongoing VCDPA implementation reinforces data minimization obligations and heightened protections for high-risk information processing. In the context of trafficking response, where data is both highly sensitive and time-critical, these standards underscore the need for technology solutions that are intentionally designed to protect privacy, ensure accountability, and build trust across systems.

State Attorneys General are also treating technology-facilitated exploitation, child endangerment, and online platform design as integral to the larger policy environment in which trafficking identification and prevention now operate and that role has grown substantially more consequential in the past year. Most significantly, the New Mexico Attorney General's landmark case against Meta Platforms, originally filed in 2023, went to trial in February 2026 and resulted in a jury verdict against Meta in March 2026, with the jury finding Meta violated New Mexico's consumer protection law and ordering the company to pay $375 million in civil penalties (New Mexico Department of Justice, 2026). The New Mexico Attorney General had alleged that Meta failed to protect children from sexual abuse, online solicitation, and human trafficking, and that the company's algorithms directed adults toward content posted by teenage users while concealing internal findings about those risks (New Mexico Department of Justice, 2026). The verdict is the first of its kind from a state AG trial against a major social media platform and carries significant implications for how platform design is assessed as a contributing factor to trafficking risk.

In February 2026, the Texas Attorney General filed an additional lawsuit against Snap Inc., alleging the platform exposed minors to explicit content and made deceptive safety claims (California Department of Justice, 2024; National Center for Missing & Exploited Children, 2024). More broadly, protecting minors on social media platforms has emerged as a leading

bipartisan AG enforcement priority, with state AGs actively coordinating across party lines on investigations, litigation, and legislative advocacy (National Association of Attorneys General, 2024). Most recently, a bipartisan coalition of 44 state attorneys general formally objected in May 2026 to a House version of a children's online safety bill that would have weakened state enforcement authority, urging Congress to preserve states' ability to pursue independent actions against platforms that harm minors (National Association of Attorneys General, 2026).

These actions collectively reflect a decisive shift: state AGs have become primary enforcement leaders in holding technology companies accountable for platform design choices that enable trafficking and exploitation, and their role continues to expand.

Taken together, these federal policy and state-led developments point to a critical inflection point: ***technology is no longer peripheral to trafficking; it is central to both the problem and the solution.*** Yet while policy momentum is accelerating, operational systems have not fully adapted to leverage technology in ways that are coordinated, ethical, and survivor-centered.

Analysis of the Issue

Human trafficking remains significantly under-identified across the United States, and this gap is increasingly shaped by the intersection of technology and system design. While enforcement activity has increased, these downstream indicators do not address the upstream challenge that many victims are never identified early enough to receive support (BJS, 2025). Safe House Project's own Simply Report data further illustrate both the scale of unmet demand and the limitations of existing systems: the platform connected 534 individuals to services in 2023, growing to 1,529 in 2024 and 2,466 in 2025—yet these figures still represent only a fraction of actual trafficking activity due to persistent barriers to reporting, access, and identification (Safe House Project, 2026).

At the same time, reporting and referral systems remain fragmented across jurisdictions and sectors. Information may be captured in one system but not shared effectively with others, and referrals are not always routed in real time (U.S. Department of Justice, 2023). These gaps are particularly problematic in cases that span multiple jurisdictions or require rapid intervention.

The growing role of technology introduces both opportunity and risk. While digital tools can improve identification and coordination, they also raise critical concerns related to privacy, data security, and ethical use. Without clear standards, technology solutions risk being implemented inconsistently or in ways that undermine trust. These harms may be especially acute where survivors have limited control over devices, communications, location visibility, or the downstream sharing of their information across systems.

One of the most significant barriers to adoption is trust. Stakeholders frequently express concern about system security, data-handling practices, and the sustainability of technology solutions, particularly those offered at no cost. These concerns must be addressed through transparent governance, strong data protections, and demonstrated outcomes.

In addition to structural and technological challenges, the use of AI-enabled systems introduces survivor-specific risks that must be addressed explicitly. These include false positives that may trigger unwanted law enforcement involvement, false negatives that delay intervention, algorithmic bias that may under-identify certain populations (including labor trafficking victims,

male survivors, and rural communities), and data exposure risks that could increase vulnerability to retaliation or legal consequences. Ethical deployment requires proactive mitigation of these risks through system design, policy, and oversight.

Ethical AI in Trafficking Response: Core Safeguards and Standards

To move from principle to practice, "ethical AI" in trafficking response must be clearly defined through enforceable safeguards. In this context, ethical AI refers not only to the use of advanced technologies but to how those technologies are governed, constrained, and evaluated when applied to highly sensitive survivor data and decision-making processes. At a minimum, ethical AI in trafficking response should include the following:

Human Oversight for Consequential Decisions

AI systems may support screening, triage, translation, and routing, but should not independently determine victim status, service eligibility, law enforcement action, or threat prioritization. This includes any decision that could materially affect a survivor's access to services, interaction with law enforcement, or exposure to legal, immigration, or family court consequences.

Transparency and Explainability

Systems must clearly disclose when AI is used, for what purpose, and with what limitations, including to partner agencies and oversight bodies.

Bias Testing and Equity Review

Algorithms must be regularly evaluated for disparate impact across gender, age, race, language, nationality, trafficking type (labor vs. sex), geography, and other factors.

Trauma-Informed Design

Systems must minimize re-traumatization by reducing repetitive disclosures, avoiding coercive data collection, and allowing flexible engagement pathways.

Data Minimization and Purpose Limitation

Only essential data should be collected, stored, and shared for clearly defined purposes tied to victim identification and response.

Consent and Survivor Agency

Survivors should have a meaningful understanding of how their data is used and, where possible, the ability to limit or opt out of certain uses. In cases involving minors, third-party reports, or acute safety threats, systems should clearly distinguish between survivor consent, reporter consent, and legally required disclosures.

Redress and Contestability

Mechanisms must exist to correct errors, challenge misclassification, and address harmful outcomes resulting from system use.

Independent Oversight

Ethical AI systems should be subject to external review, including survivor-informed advisory input.

Without these safeguards, technology adoption risks reinforcing existing inequities, introducing new harms, and undermining trust across systems.

Why This Matters Now

The convergence of rapid technological advancement, evolving policy priorities, and increased state-level engagement creates a critical, time-sensitive opportunity to modernize the national response to human trafficking. Trafficking networks are already operating in a digitally enabled environment, leveraging speed, anonymity, and scale in ways that outpace traditional response systems (Europol, 2023). At the same time, policymakers are increasingly focused on platform accountability, data governance, and responsible use of emerging technologies, as reflected in recent federal legislation and state-level enforcement actions.

States, particularly Attorneys General's Offices and multidisciplinary task forces, are actively seeking scalable, practical solutions to improve victim identification and coordination without creating entirely new systems. However, in the absence of coordinated policy guidance, technology adoption risks occurring in fragmented and inconsistent ways, leading to duplication, interoperability challenges, and uneven protections for sensitive data.

This moment presents a clear inflection point. With intentional alignment across policy, technology, and practice, technology can serve as a force multiplier to enable earlier identification, real-time coordination, and stronger service connection. But those gains will only be realized if systems are deployed within clearly defined governance structures that ensure safety, interoperability, and accountability.

Policy Options

Option A: Status Quo with Incremental Improvements

Continue relying on existing reporting and referral systems, making limited enhancements to current processes without fundamentally redesigning system architecture. While this approach may appear less disruptive and easier to implement in the short term, it largely preserves existing structural limitations. Incremental improvements, such as minor technology upgrades or expanded training, do not address the core issues of fragmented reporting pathways, delayed coordination, and limited access for victims. This approach also risks reinforcing existing inequities, as populations already under-identified, such as labor trafficking victims, male victims, and non-English speakers, are least likely to benefit from incremental improvements to systems not designed for their engagement. In practice, this approach risks preserving a system in which increased awareness does not translate into improved access, faster referrals, or more consistent victim recognition.

Limitations:

- Does not address structural misalignment between system design and real-world victim behavior

- Maintains siloed data systems and delayed response timelines
- Continues reliance on single-channel reporting models
- Limits ability to scale or adapt to evolving technology-enabled trafficking dynamics

Option B: Technology Adoption Without Ethical Framework

Expand the use of digital tools and platforms to improve reporting and coordination, but without establishing clear standards for ethical design, data governance, or system accountability. This approach may accelerate innovation and deployment, but it introduces significant risks if not guided by consistent policy frameworks. Without clear standards, technology solutions may vary widely in quality, security, and effectiveness, creating confusion among stakeholders and potentially harming vulnerable populations. This approach may also create a fragmented technology landscape in which multiple, non-interoperable systems operate simultaneously, increasing confusion for frontline responders and potentially resulting in duplicated or missed referrals. It also increases the likelihood that survivor data will be governed by private vendor terms, inconsistent retention practices, or opaque model development processes rather than by clear public-interest standards.

Risks:

- Inconsistent data privacy and security protections across systems
- Lack of interoperability between platforms and jurisdictions
- Increased risk of misuse or unintended exposure of sensitive victim data
- Erosion of trust among law enforcement, service providers, and survivors
- Difficulty scaling or sustaining solutions without shared standards

Option C: Ethical, Multi-Channel Technology Deployment

Adopt a coordinated, policy-aligned approach that integrates ethical, survivor-centered technology into existing anti-trafficking systems while establishing clear standards for implementation and use. This approach recognizes that technology must be both operationally effective and responsibly designed, ensuring that it enhances, not undermines, the broader response. It prioritizes accessibility, speed, coordination, and trust, while aligning with emerging policy frameworks on data protection and platform accountability.

This includes:

- Multi-channel reporting access, allowing individuals to engage through safe and appropriate communication methods
- Real-time coordination capabilities, enabling immediate routing and response across agencies
- Strong data governance and privacy protections, aligned with evolving federal and state standards
- Integration with multidisciplinary frameworks, including task forces, Attorney General Offices, and service providers
- Scalability and interoperability, ensuring consistency across jurisdictions

Recommended Approach

The most effective path forward is a coordinated policy and implementation strategy that advances ethical, multi-channel technology solutions within existing anti-trafficking frameworks. This approach moves beyond isolated tools or any single access pathway and instead focuses on building a connected, responsive infrastructure that reflects how trafficking occurs and how victims seek help.

Operational platforms that meet these criteria, such as multi-channel, real-time reporting and coordination systems, demonstrate how this model can be implemented in practice. These platforms illustrate how these principles can be operationalized to expand access, support real-time routing, and strengthen coordination when aligned with ethical standards and policy frameworks. Importantly, this approach does not replace existing infrastructure. Instead, it strengthens and connects current systems, including Attorney General offices, task forces, and multidisciplinary partnerships, enhancing both identification and response while aligning with federal and state policy priorities.

To operationalize this approach, federal and state policymakers should consider the following actions:

1. Establish minimum standards for trafficking-response technologies in federal grantmaking and state procurement, including requirements for data protection, human oversight, and system transparency
2. Require survivor safety impact assessments prior to deployment of new technology systems
3. Prohibit fully automated decision-making in victim identification, referral, or enforcement actions
4. Mandate independent audit and oversight mechanisms, including survivor-informed review
5. Ensure interoperability requirements to prevent fragmentation across jurisdictions
6. Prohibit secondary commercial use of survivor data and strictly limit any use for model training, analytics, or product development absent clear legal authority, survivor-informed safeguards, and independent oversight
7. Incorporate trauma-informed digital design standards into all federally supported systems

Implementation Plan

Implementation of this approach requires deliberate alignment across policy, technology, and practice. At the federal level, policymakers can support the development of standards for ethical technology use, strengthen data governance frameworks, and align funding mechanisms to incentivize modernized reporting and coordination systems. Implementation should also include a clear delineation of roles across agencies, including what information is shared, when, and for what purpose, to prevent both overexposure and under-coordination of sensitive data.

At the state level, implementation can be integrated into existing structures, including multidisciplinary task forces and Attorney General-led initiatives. This includes establishing clear

protocols for data sharing, defining roles across partner agencies, and ensuring alignment with state privacy and technology laws.

Successful implementation also requires:

- Training and onboarding for law enforcement, service providers, and partners
- Phased deployment strategies to allow for testing, refinement, and trust-building
- Clear communication regarding system security, data use, and operational benefits
- Ongoing evaluation and feedback loops to ensure continuous improvement

Building trust across stakeholders is critical. Transparency, consistency, and demonstrated outcomes will be key to sustaining adoption and scaling impact. At the same time, technology modernization alone will not improve outcomes without sufficient staffing, referral capacity, training, and access to trauma-informed services at the state and local levels. ***Digital infrastructure must be paired with human capacity to translate identification into meaningful support.***

Expected Outcomes

A coordinated, technology-enabled approach to trafficking identification and response is expected to contribute to earlier identification of victims, particularly in frontline systems where indicators are often missed, while improving the consistency and speed of coordinated response. It will enable faster, more coordinated responses by improving real-time information sharing and reducing delays in referral and intervention. In the near term, this approach is expected to improve operational outputs, including timelier routing, stronger interagency visibility, and more consistent referral pathways. Over time, and only when paired with sufficient service capacity and governance, those operational gains may contribute to earlier victim identification, stronger service connection, and more consistent survivor-centered outcomes.

This approach will also strengthen connections to services, ensuring that victims are not only identified but effectively supported through recovery. Improved data visibility will enhance policymakers' ability to understand trends, allocate resources, and design prevention strategies. Over time, this model will contribute to a more integrated, effective, and survivor-centered national response, one that reduces fragmentation, improves accountability, and strengthens public safety outcomes.

Conclusion

Human trafficking continues to evolve in complexity and scale, and the systems designed to respond must evolve with it. Technology is now central to both exploitation and response, making it an essential component of any effective strategy. The question is no longer whether to use technology, but how to govern it. Policymakers have a clear opportunity to define that framework, one that strengthens identification, improves coordination, and keeps survivor safety at the center. Without modernization, gaps in identification and response will persist. With modernization grounded in governance, accountability, and survivor-informed safeguards, the nation can build a more coordinated, effective system equipped for today's trafficking landscape.

References

Bureau of Justice Statistics. (2025). *Human trafficking data collection activities, 2025*. U.S. Department of Justice. https://bjs.ojp.gov/library/publications/human-trafficking-data-collection-activities-2025

California Department of Justice. (2024). *Attorney General actions involving online platform safety and child protection*. https://oag.ca.gov

Congressional Research Service. (2026). *Digital platform accountability and emerging legislation*. Congressional Research Service.

Europol. (2023). *Exploiting isolation: Offenders and victims of online child sexual exploitation*. Europol. https://www.europol.europa.eu

National Academies of Sciences, Engineering, and Medicine. (2020). *Estimating prevalence of human trafficking in the United States: Considerations and complexities*. National Academies Press. https://nap.nationalacademies.org

National Association of Attorneys General. (2024). *Multistate efforts on online safety and platform accountability*. https://www.naag.org

National Association of Attorneys General. (2026). *Bipartisan coalition of 44 state attorneys general opposes House children's online safety bill*. https://www.naag.org

National Center for Missing & Exploited Children. (2024). *Online enticement and sextortion trends report*. https://www.missingkids.org

New Mexico Department of Justice. (2026). *Jury finds Meta liable in child sexual exploitation trial; $375 million verdict entered*. https://nmdoj.gov

New Mexico Department of Justice. (2025). *Court denies Snap Inc.'s motion to dismiss in child exploitation lawsuit*. https://nmdoj.gov/press-release/attorney-general-raul-torrez-secures-major-legal-victory-against-snap-inc-in-fight-to-protect-children/

Safe House Project. (2026). *Simply Report internal data analysis*. Safe House Project.

Trafficking Survivors Relief Act, Pub. L. No. 119-73. (2026). https://www.govinfo.gov/app/details/PLAW-119publ73

United States Congress. (2025). *Enhancing Detection of Human Trafficking Act* (H.R. 4307 / S. 2241, 119th Cong.). https://www.congress.gov/bill/119th-congress/house-bill/4307

United States Congress. (2025). *Frederick Douglass Trafficking Victims Prevention and Protection Reauthorization Act of 2025* (H.R. 1144, 119th Cong.). https://www.congress.gov/bill/119th-congress/house-bill/1144

United States Congress. (2025). *App Store Accountability Act* (H.R. 3149 / S. 1586, 119th Cong.). https://www.congress.gov/bill/119th-congress/house-bill/3149

United States Congress. (2025). *Kids Online Safety Act* (S. 1748 / H.R. 6484, 119th Cong.). https://www.congress.gov/bill/119th-congress/senate-bill/1748

United States Congress. (2025). *Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2025* [STOP CSAM Act] (H.R. 3921 / S. 1829, 119th Cong.). https://www.congress.gov/bill/119th-congress/senate-bill/1829

U.S. Department of Justice. (2023). *Federal human trafficking report*. U.S. Department of Justice.

U.S. Department of State. (2025). *2025 trafficking in persons report*. https://www.state.gov/reports/2025-trafficking-in-persons-report/

Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575 to 59.1-585. (2026). https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

California Privacy Protection Agency. (2026). *California Consumer Privacy Act regulations*. https://cppa.ca.gov/regulations/