Documents for the Record
12.11.2025 Commerce, Manufacturing, and Trade Subcommittee Markup

Majority

1. Letter from the American Principles Project to Chairmen Guthrie and Bilirakis.
2. Letter/statement from the National Sheriff's Association to Members of the Committee.
3. Letter from the U.S. Chamber of Commerce to Chairman Bilirakis and Ranking Member Schakowsky.
4. Letter from the undersigned coalition child safety advocates to Chairmen Guthrie and Bilirakis.
5. Statement for the record from the Age Verification Providers Association.
6. Letter from the Alliance for Safe Online Pharmacies to Chairmen Guthrie and Bilirakis and Ranking Members Pallone and Schakowsky.
7. Letter from the Major County Sheriffs of America (MCSA) and the Association of State Criminal Investigative Agencies (ASCIA) to Chairmen Guthrie and Bilirakis and Ranking Members Pallone and Schakowsky, submitted by Rep. Evans.

Minority

1. Letter from ACLU to CMT Subcommittee Members in opposition to HR 1623, HR 3149, HR 6484, HR 2657, HR 6291 (December 10, 2025)
2. Letter from Center for Democracy & Technology to Chairman Guthrie, Chairman Bilirakis, Ranking Member Pallone, Ranking Member Schakowsky
3. Memo from Common Sense Media on HR 6484
4. Blog post entitled Why the Parents Over Platforms Act is the Better Path for Protecting Young People (December 8, 2025)
5. Letter from coalition of education associations to Chair Guthrie, Chair Bilirakis, Ranking Member Pallone, Ranking Member Schakowsky (December 11, 2025)

December 10, 2025

Dear Chairman Guthrie, Chairman Bilirakis, and members of the House Energy and Commerce Committee,

I want to thank you for your commitment to finding the most practical solutions to protect children's innocence and strengthen parents' rights online. Having helped pass age verification laws for online pornography websites in 24 states, we know even the simplest attempts to protect children in the digital realm still face enormous pushback. Accordingly, we urge your committee to prioritize two workable models that have already succeeded at the state level: the SCREEN Act and the App Store Accountability Act.

As it stands, children are often just one or two taps away from exposure to violent and inappropriate content online. We've seen kids driven to suicide by manipulative AI chatbots like Character.AI that hijack their emotions and isolate them from family life. We've seen disgusting amounts of increasingly extreme pornography reach young kids, normalizing crude violence and distorting men's attitudes toward women. All of it is unacceptable—but, with pro-family, privacy-preserving safeguards, most of this harm is preventable.

No tech company, whether an AI developer or porn-tech conglomerate, should profit from stealing children's innocence. Congress can end this pernicious practice in one fell swoop by passing the SCREEN Act and the App Store Accountability Act and – two complementary age verification measures that cordon off kids' access to inappropriate material at two key chokepoints: pornography websites and app stores.

There is no question that young kids' easy access to online adult content is an emergency that must be addressed—according to one recent study, the average age of first exposure is now just 12 years old. Responding to the well-documented harms associated with pornography use, the SCREEN Act requires commercial porn websites to implement age verification measures to prevent underage access, requiring secure and transparent collection of verifiable age data.

By forcing porn companies to take seriously their responsibility to ensure graphic depictions of sexual encounters do not reach impressionable minors, the bill aligns commercial practices online with widely accepted real-world standards. We expect even the seediest adult store on the side of the highway not to sell sexual products to an unaccompanied minor; the same standard should apply online.

Currently, meaningful age-verification is also wholly absent from today's app stores. A kid taps "agree and install," and suddenly a developer has access to their microphone, location, data, and camera. This isn't just an unconscionable invasion of privacy—it's a violation of basic tenets of contract law and an erosion of parental rights.

The App Store Accountability Act has a simple premise: like any local corner store, Apple's and Google's app stores should be responsible for verifying a user's age before allowing access to potentially inappropriate or age-restricted content.

Recognizing that content and privacy risks are not always cut and dry, the App Store Accountability Act holds all platforms—including social media companies, AI chatbots, and every other app available for download—to the same standards while avoiding blanket censorship and empowering parents to determine whether a platform aligns with their child's maturity and family's values.

This family-centered posture and responsible use of age data that Apple and Google already collect makes the App Store Accountability Act technically feasible, narrowly tailored, and minimally burdensome.

These two measures work together; even with pornography websites locked down, disgusting nudifying apps, violent video games, and predatory anonymous messaging platforms remain readily available, systematically mislabeled, and deceptively marketed to kids on app stores. And seemingly harmless apps can contain backdoor browsers that allow kids to bypass filters and access hardcore porn. That's why Congress must prioritize targeted age verification measures tailored to each landscape.

As the Supreme Court ruled this summer in *Free Speech Coalition v. Paxton*, age-verification is an "ordinary and appropriate" means of protecting kids online. By implementing age verification at two high traffic digital junctures—porn websites and app stores—Congress can defend kids' innocence and strengthen future generations of American families. I urge you to support and pass the SCREEN Act and the App Store Accountability Act this session.

Sincerely,

Terry Schilling
President
American Principles Project

NATIONAL SHERIFFS' ASSOCIATION

JONATHAN F. THOMPSON
Executive Director and CEO

December 10, 2025

On behalf of the National Sheriff's Association, I want to express our concerns with H.R. HR 6292 which is scheduled to be marked up tomorrow in the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce. We applaud the intention. Every sheriff in our membership recognizes the need to protect children in our increasingly complex and connected society.

Our concern is that the bill will impair our members' ability to investigate crimes against children, including abuse, human trafficking as well as missing and exploited children. NSA members depend on third-party data and analytics providers which supply essential investigative tools needed to do our job. This bill provides no exceptions for our members, their suppliers, and their mission to protect children and investigate crimes against them. We believe the bill needs more time and discussion before the committee takes a vote.

Sincerely,

Jonathan F. Thompson
Executive Director/CEO
National Sheriffs' Association

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

December 10, 2025

The Honorable Gus Bilirakis
Chairman
Commerce, Manufacturing &
Trade Subcommittee
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Commerce, Manufacturing &
Trade Subcommittee
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to provide comments on legislation being considered by the Commerce, Manufacturing and Trade Subcommittee, to protect children and teens online. We applaud many of the significant improvements that have been made to both H.R. 6291, the "Children and Teens' Online Privacy Protection Act" ("COPPA 2.0") and the Kids Online Safety Act ("KOSA") that would make these bills more certain and workable while increasing protections for kids. We believe it is critically important that Congress exercise its constitutional mandate to regulate interstate commerce by enacting a single national standard regarding children's online privacy and protection as well as app store usage.

I. Uniform National Standards Are Rooted in Constitutional Federalism

A single national standard is the appropriate mechanism to address children's online privacy and other harms given the internet is inherently interstate. The Founders enshrined in the United States Constitution the power of Congress to regulate commerce "among the several states"[1] and made federal legislation the supreme law of the land.[2]

The exclusive power of Congress to regulate interstate commerce is necessary to prevent regulatory confusion and conflicting regulations. James Madison noted in *The Federalist Papers*[3] that the purpose of Congress's authority to regulate interstate commerce was to facilitate economic harmony and prevent the economic defects that occurred when the United States operated under the Articles of Confederation. This

[1] U.S. Constitution Art. I § 8.
[2] U.S. Constitution Art. VI.
[3] Federalist 42

same concept rings true today and has been acted upon by Congress numerous times to instill uniformity.

The United States Supreme Court has upheld Congress' authority to regulate the channels and instrumentalities of interstate commerce as well as commercial activity that has a substantial impact on the national economy.[4] The Supreme Court has also affirmed on numerous occasions the ability of Congress to preempt state regulatory action that encroaches on Congress' ability to foster a uniform national economy.[5] In fact, Congress has successfully done so with enactment of national motor vehicle safety standards[6]; prohibitions on states regulating airline routes, service, and fares[7]; similar prohibitions on states regulating the scheduling or pricing of motor carriers[8]; and prohibitions on states imposing requirements that inhibit interstate communications.[9]

II. Uniform National Online Privacy and Protection Laws Are Necessary

A uniform national standard for children's online privacy and protection is necessary to eliminate confusion and potential conflicting state standards as well as foster certainty for parents and those providing online services. A single national approach to children and teen's *online* protections is legally appropriate, consistent with the Founders' approach to federalism, and is necessary to promote the modern economy. Online activity in today's connected digital world inherently relies on interstate commerce.[10] Much like it does not make sense for airlines to have to navigate fifty different service, pricing and safety rules, a patchwork of state privacy laws creates confusion and the potential for conflicting laws.

For example, in the broader privacy context, the State of Maryland recently enacted legislation that would prevent the collection of sensitive data[11]. In June 2026, Colorado's SB-205 will go into effect, barring companies from developing or deploying AI that has a disparate discriminatory impact.[12] Because of Maryland's law, many companies may be left without the data necessary to determine compliance with Colorado's AI statute. In the context of children's privacy, state attempts to ensure the

---

[4] *United States v. Lopez*, 514 U.S. 549, 558-59 (1995).
[5] *See* Congressional Research Service, "Federal Preemption: A Legal Primer" (2023) *available at* https://www.congress.gov/crs-product/R45825#.
[6] 49 U.S.C. § 30103(a)(b).
[7] 49 U.S.C. § 41713(b).
[8] 49 U.S.C. § 14501(a).
[9] 47 U.S.C. § 253(a).
[10] *See e.g.* United States v. Lewis, 554 F.3d 208, 215 (1st Cir. 2009).
[11] Maryland HB 567 (2024)
[12] Colorado SB 205 (2024)

design of products and services are safe for children could impede on another state's privacy protections.

From an economic perspective, a patchwork of online privacy laws would harm the national economy. According to one report, fifty different state privacy laws could cost the American economy $1 trillion over ten years, with small businesses incurring $200 billion of that burden.[13] The Chamber found that sixty-five percent of small business owners are concerned that out-of-state privacy laws will increase their litigation and compliance costs.[14]

It is imperative that Congress pass thoughtful, consistent, and seamless children's protection and privacy legislation that works as opposed to an uncoordinated and unharmonized system of state regulation.

III. States Should Have a Role in Enforcement

While we believe that a uniform national approach to setting the rules for online protections is necessary, states should continue to have a role in pursing enforcement against actors who violate the law. The Chamber fully supports the ability of state attorneys general to enforce comprehensive privacy legislation, as well as such legislation specifically protecting children and teens. As presented before the Committee, both COPPA 2.0 and KOSA would preserve the ability of state attorneys general to enforce violations against residents of their home states. State attorneys general are experts in consumer protection who understand the impact of online harms to their respective constituencies.

IV. Conclusion

Children and teens deserve online protections, and their parents need the tools to prevent harms that can occur online. At the same time, the best approach to ensuring all American children are protected is a uniform national standard. We look forward to engaging with Congress on this important issue to perfect COPPA 2.0 and KOSA.

---

[13] ITIF, "50-State Patchwork of Privacy Laws Could Cost $1 Trillion More Than a Single Federal Law, New ITIF Report Finds" (January 2022) *available at* https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.

[14] U.S. Chamber of Commerce, *Empowering Small Business: The Impact of Technology on U.S. Small Business*, (August 2025) *available at* https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf.

Should you have any questions, please do not hesitate to contact jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

December 10, 2025

The Honorable Brett Guthrie
Chairman of the House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman of the Subcommittee on Commerce, Manufacturing, and Trade
2123 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Guthrie, Chairman Bilirakis, and Distinguished Members of the Subcommittee:

We represent a coalition of child safety advocates that has advanced numerous state laws nationwide to create a safer online environment for children. Our coalition submitted pivotal amicus briefs supporting the Supreme Court's decision in *Free Speech Coalition v. Paxton* and has played a direct role in developing federal and state legislative models to address online harms facing young people. We have also supported key federal initiatives, including the Kids Online Safety Act and the TAKE IT DOWN Act, to promote child safety in the digital age.

Following more than 28 Congressional hearings on this issue, we appreciate the Subcommittee on Commerce, Manufacturing, and Trade's decision to schedule a December 11, 2026, markup on a package of bills – including the App Store Accountability Act – designed to provide long-overdue digital safeguards for America's children.

We are, nevertheless, alarmed by the inclusion of the Parents Over Platforms Act (POPA), which appears to offer solutions to problems created by app stores and developers but, in fact, emboldens them to continue their existing exploitative practices. As written, POPA would continue to allow billion-dollar companies to create contracts with minors, enable non-compliance with existing federal law, and depend on inaccurate age information.

Our basic principle of American law is that minors lack the legal capacity to enter binding contracts. That agreements with minors are voidable at the minor's election is a doctrine grounded in our nation's commitment to prevent children from being bound to obligations they cannot understand or negotiate.

This rule applies equally to digital agreements, which are no different in legal effect from any other contract. Yet, compared with the much stronger App Store Accountability Act, POPA disregards this principle by allowing minors to enroll in lengthy, non-negotiable terms of service that include arbitration clauses, liability waivers, recurring payment terms, and broad data collection permissions. These terms-of-service agreements often grant developers access to highly sensitive data, including a child's exact location, contacts, photos, microphone, camera, and device identifiers.

The Children's Online Privacy Protection Act (COPPA) restricts the collection, use, and sharing of personal information from children under 13 by requiring online services to obtain verifiable parental consent. Under POPA, platforms are not required to share this critical age data with developers, thereby undermining consistent COPPA compliance. POPA therefore preserves the status quo rather than offering a meaningful solution to this fundamental problem.

POPA's age verification framework, likewise, is insufficient. It relies on self-reported age at device account creation to determine whether a user is classified as an adult. This approach disregards two decades of advances in privacy-preserving age-verification technologies and reinforces a model that is both easily circumvented and technically outdated.

Furthermore, POPA undermines its own child safety objectives by relying on an honor system under which its core obligations apply only to applications that developers voluntarily classify as intended exclusively for adults or as providing different experiences for minors and adults. This reliance on self-designation places enforcement entirely in the hands of the regulated entities. By simply asserting that their content is appropriate for minors and uniform across age groups, developers can avoid classification as a Covered Application and thereby exempt themselves from the bill's safety requirements without consequence. The result is a powerful incentive for developers to opt out, undermining the very protections the bill purports to establish.

Not only does POPA undermine child safety objectives in existing law and other proposed bills in the markup, but unfortunately, supporters of the Parents Over Platforms Act are also actively opposing the App Store Accountability Act—a bill written over several years by multiple expert digital safety advocates and organizations. The App Store Accountability Act would ensure platforms comply with COPPA, actually enable protections for children, and close the gaps that POPA fails to address.

We respectfully urge the Subcommittee's leadership to exclude the Parents Over Platforms Act from markup. Families do not need another framework designed to protect platforms

from accountability. We need a real solution that puts families first, strengthens safeguards rather than weakens them, and affirms that the nation's laws are not for sale to companies they are meant to regulate. We instead urge you to support the App Store Accountability Act and the several other pieces of meaningful child safety legislation in the subcommittee's bill package.

Sincerely,

Protect Young Eyes
Institute for Family Studies
National Center on Sexual Exploitation (NCOSE)
Institute for Families and Technology
Digital Childhood Institute
Clare Morell, The Ethics and Public Policy Center
Family Policy Alliance
Scrolling 2 Death
David's Legacy Foundation
Parents Who Fight
KIDS TOO
Dr. Jill Manning, PLLC
Victims2SurvivorsUS
Paradigm Shift Training and Consulting
Yellowstone Human Trafficking Task Force
NH Traffick Free Coalition
The Stop Trafficking Project®
Greenway Recovery
Better Screen Time
Paving the Way Foundation
Digital Childhood Alliance
United Abolitionists, Inc
NC Stop Human Trafficking
All Girls Allowed
HeartDance Foundation
Chains Interrupted
Tin Man Ministries
ANEW Life International
Nurses United Against Human Trafficking
MORE TOO LIFE/MORE TO LIVING
No Trafficking Zone

Statement for the Record of

Iain Corby

Executive Director

The Age Verification Providers Association

For a hearing of

House Energy and Commerce Committee

Sub-Committee on Commerce, Manufacturing, and Trade

Legislative Solutions to Protect Children and Teens Online

11 December 2025

2123 Rayburn House Office Building, Washington, D.C.

The Age Verification Providers Association (AVPA) is the global trade body representing 34 suppliers of technology that enables users to prove their age online without disclosing their identity. Our members offer the full range of age assurance technologies[1], which based on the International Standards Organization's definitions fall into three categories:

1. Age verification – e.g. passport, driving license, bank or wireless carrier records.
2. Age estimation – e.g. facial, voice, hand movement, EKG, user-generated content.
3. Age inference – e.g. school year, commercial pilot's license, social media network contacts, email address and cell phone number usage records.

We have provided written and in-person testimony to multiple state legislatures considering bills that include age verification requirements. To date, this has primarily focused on adult websites (25 states have passed such laws[2]), but there is increasing legislative activity around social media, age-appropriate design, and, most recently, AI - with a particular concern about children's use of Chatbot AI companions.

We are politically neutral and do not presume to suggest to the U.S. Congress what should be age-restricted online, or at what age. We submit this statement solely to inform the Committee of the latest capabilities of age verification technology and to elucidate related policy discussions.

The State of the Art of Age Verification

Allow us to begin by describing how an age verification process is capable of operating today. A user can prove their age locally by using an app on their smartphone. This involves, for example, taking a photo of a physical ID, comparing that image to a selfie taken at the same time, extracting the date of birth and calculating if the user is over the required minimum age. Crucially, without any personal data leaving the palm of the user's hand, the app then shares a cryptographically signed signal with an app or website which divulges only that the current user is over that required age. This architecture makes it technically impossible for the service being accessed to obtain any personal data other than an age-range.

This is not rocket-science. Indeed, if American technology can put a man on the moon, it can certainly allow you to prove your age without disclosing your identity.

Importantly, this does not require the creation of any new central database of identity data. Modern privacy-preserving technologies rely on one-time checks, immediate deletion and token-based signals that cannot be repurposed or linked across services. The latest generation of international standards explicitly prohibits the retention, reuse or onward transfer of age-verification data for advertising,

[1] While the formal term used in international standards is 'age assurance', this statement will use the more commonly used term 'age verification' but unless specified, that should be read to include inference and estimation methods.
[2] https://avpassociation.com/4271-2/

profiling, or any unrelated purpose. This ensures a strict regime of data-minimization, purpose-limitation and anti-repurposing in line with global best practice.

Age verification is not a national digital identity system, nor can it function as one. The one-time, anonymous tokens used in modern systems cannot be used for authentication, tracking, or identification in any other context.

Legislative Recommendation: *Congress should mandate federal standards for privacy-preserving age signals (e.g., cryptographic tokens) in any required age assurance mechanisms, explicitly prohibiting data retention beyond the verification process and requiring FTC oversight of a certification mechanism for compliance with international standards, thereby aligning with the Committee's emphasis on data protections for both children and adults.*

Preserving Anonymity

Age verification first emerged to address the risk of children being exposed to obscene adult content online. In Europe, where the General Data Protection Regulations[3] (GDPR) were already in force, the structural separation of activities - using an independent third party to perform the check - was sufficient to allay privacy fears. As technology advanced, some EU regulators, notably the German regulator, the KJM, reviewed and published a list of over 100 approaches (spanning verification approaches and estimation approaches with a buffer) capable of being effective to assess age, to access adult in the German market. The French CNIL and Arcom, looked for technical measures that could reinforce the legal protections. They required a "double-blind" solution, meaning not only could the adult site not discover the identity of the user, but the AV provider should also not be able to track which adult sites a user was accessing.[4] [5]

In the U.S. context, states legislating for age verification have included measures to protect user privacy, primarily through a requirement to delete personal data once the age check has been completed.

Therefore, it is not accurate to claim, as the Center for Democracy and Technology (CDT) does in its submission to the Sub-Committee, that "Requiring users to prove their age to access content or services leads to more data collection, processing, and retention by already data-rich services."[6] Of course, it may do if age verification is carried out directly by the services themselves, and not through an independent third party with the technical and legal measures we have described to protect privacy. Nor do "users of all ages lose the ability to access the web anonymously when they have to provide

[3] https://gdpr-info.eu/
[4] CNIL (relevant guidance on age verification privacy, building on 2020 decisions): https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[5] Arcom (technical guidelines, updated 2024 from 2023 framework): https://www.arcom.fr/en/find-out-more/legal-area/legal-resources/technical-guidelines-age-verification-protection-persons-under-18-online-pornography
[6] Aliya Bhatia & Nick Doty, *Mitigating Risk to Rights with Age Verification: Privacy-Preserving Guardrails that Should Accompany Deployments of Age Verification Approaches*, Ctr. for Democracy & Tech. (Oct. 10, 2025), https://cdt.org/insights/mitigating-risk-to-rights-with-age-verification-privacy-preserving-guardrails-that-should-accompanydeploymentsof-age-verification-approaches/ Note 38

proof of age documents" if these basic structural protections are put in place. Congress has the opportunity to hardwire all these protections into statute and, in doing so, avoid any potential chilling effects on lawful expression.

Legislative Recommendation: *To address concerns on privacy risks, incorporate requirements for third-party, data minimised with the option of double-blind age assurance in any data-broker restrictions, enforced via FTC mandated periodic independent audits - ensuring anonymity while enabling safe access for verified adults and excluding minors from high-risk content.*

Biometric Data

There is, rightly, a particular sensitivity about biometric data. For adult content, minors are not required to share biometric data because they are not old enough to access the content. But for users of all ages, it is important to note that software designed to estimate age does not process the full photographic image of the user but rather a simplified mathematical map of facial features. It does not undertake 1:1 or 1:many facial recognition, it detects, analyses and deletes the image. At the point that this map is created, it is no longer unique to the individual, so cannot be used to re-identify them. Far more data is required for the process of unique recognition.

The data on which facial age-estimation calculations are based where there is no unique recognition or authentication no longer constitutes sensitive personal data - a point confirmed by the UK Information Commissioner.[7] Where that translation from image to mathematical map takes place sets the boundary for the extent to which biometric data is shared: it can even be converted on the user's own device. But where it is processed on a server, the image need never be saved at any point and is neither therefore retainable nor retained.

The industry has also developed strong anti-repurposing safeguards, aligned to data protection regimes elsewhere in the world, e.g. the EU, UK and Australia. Standards applied globally now prohibit the reuse of age-estimation outputs for surveillance, recognition, marketing or training unrelated AI models. Independent audits and certifications confirm that such data is deleted immediately after use and cannot be reconstructed or paired with other datasets.

Legislative Recommendation: *Include provisions requiring transparency as to the origin of datasets meeting data protection requirements in the jurisdiction, the requirement for injection detection and independent assessment of the bias of algorithms, classifying processed age-estimation maps as non-sensitive data under federal law, and prohibiting repurposing for AI training—directly mitigating SIIA's cyber risk concerns while supporting the staff memo's call for effective, evidence-based tools.*

[7] ICO Commissioner's Opinion (updated January 2024, based on 2023 analysis): https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/

Interoperability and Re-usable Age Tokens

A further advance in the maturity of the age-assurance ecosystem is the emergence of interoperable, privacy-preserving networks that allow a user to complete an age check once and then reuse that confirmation across multiple services without repeating the process or disclosing any additional personal data. This significantly reduces friction for users, minimizes processing by services, and strengthens privacy protections.

The Age Verification Providers Association has engaged with two complementary approaches: AgeAware, developed through the euCONSENT ASBL non-profit organization which shares trusted, certified age signals, now deployed in Europe,[8] and OpenAge[9], another initiative to make age private, reusable and globally interoperable. Both systems use cryptographically signed tokens that confirm only an age-range - for example “18+”- and reveal no underlying identity information. Tokens cannot be linked across services, and the issuing provider cannot see where they are later used, preserving the double-blind architecture described earlier.

Importantly, interoperability improves accessibility and inclusivity. Because a single age check can be reused, families without passports or driving licenses can rely on alternative methods (such as facial estimation with buffer ages or trusted records such as school year or mobile network age-tiering). Users are not locked into a particular device, app store, or operating system, and parents who are less digitally confident only need to complete the process once. Standards also require regular auditing for demographic performance to ensure accuracy across age, sex, ethnicity, and disability characteristics, reducing the risk of bias that can arise when systems operate in isolation.

Interoperability therefore ensures that age assurance remains practical, privacy-preserving, accessible to all families, and competitive, preventing any single platform, operating system, or app store from becoming the de facto gatekeeper of online age checks. As AI evolves (per the staff memo), interoperable AV can safeguard chatbots without stifling innovation.

Legislative Recommendation: *Include provisions requiring age-restricted digital services to preserve accessibility and inclusivity, and direct that regulations encourage the development of interoperable mechanisms for platform-based age verification.*

Circumvention and Robustness

As with all safety technologies, it is important that age-verification systems are designed to resist the most common forms of circumvention. The industry has developed a range of countermeasures that address the practical risks often cited in debates about feasibility.

Older Person Enablement: This is mitigated by liveness checks and friction-reducing user flows. Many providers now use single-use verification tokens bound to the individual at the time of verification,

[8] Project site: https://euconsent.eu/interoperability-through-ageaware-from-euconsent/

[9] https://openageinitiative.org/

meaning that once the token is issued, it is automatically tied to that user's device or session and cannot simply be handed over to another person. Passkeys also enable an increase in authentication. Users may be prompted to re-confirm their age at a time when an older co-conspirator is not available

Fake, Tampered or Forged IDs: These are addressed through modern document-authentication techniques. These include hologram analysis, embedded-chip verification where available, barcode and MRZ consistency checks, tamper detection, and cross-referencing with issuing-authority norms, plus face matching and liveness detection. Certified systems routinely identify the majority of forged IDs, particularly those that minors are most likely to obtain or develop.

AI-Generated Faces or Deepfakes: This risk is mitigated through mandatory liveness detection and anti-spoofing requirements. International standards and certification schemes require providers to demonstrate resistance to presentation attacks such as deepfakes, masks, screens, and replayed images. The Age Verification industry works with academic experts to mitigate the risks from these attacks and continuously evolve defenses.[10]

Taken together, these measures significantly constrain the realistic avenues for circumvention. While no safety measure is perfect, modern age verification is demonstrably capable of preventing the vast majority of casual bypass attempts, and particularly those most accessible to children.

Legislative Recommendation: *Incorporate anti-circumvention standards (e.g., liveness detection, device-bound tokens) into the FTC's enforcement toolkit, with requirements for annual efficacy reporting - bolstering SIIA's evidence-based approach and addressing emerging AI harms for robust, population-level safeguards.*

Standards, Audit and Certification

Not all age verification is created equal. There are examples of solutions on the market today that over-retain data, hold it on systems never designed for this purpose, or store it in jurisdictions without effective data-protection laws.

Solutions may vary not only in accuracy, but also in how well they are designed to preserve privacy and protect data. Independent audit against international standards allows legislation, or more commonly related regulations, to require that only certified solutions are adopted. Conformity Assessment Bodies, themselves approved by national bodies such as ANSI once they have demonstrated the specific expertise required, can assess the accuracy, privacy, and data security measures, amongst other features, on a periodic basis.

This allows regulators to focus their resources more effectively on services that do not use certified age verification solutions. It also provides a clear, consistent technical framework capable of operating regardless of whether Congress ultimately chooses a federal pre-emption model or a state-based approach.

[10] https://defaiproject.com/

Legislative Recommendation: R*equire ANSI-approved certification for all age assurance tools used by covered platforms, with mandatory periodic audits and penalties for non-certified systems—promoting the federal consistency advocated by SIIA while avoiding the state patchwork others warn against, without broad pre-emption.*

Proportionality

Not all harms are created equal either. Typically, age-verification providers adopt a waterfall approach, seeking sufficient proof of age by using progressively more rigorous methods in line with the nature of the harm. So, a facial-age estimation with a mean average error of ±1½ years may be considered adequate for age-appropriate design, but a stricter test may be required for adult content (noting that estimation techniques applied with a sufficient "buffer age" can yield equivalent or better results than some conventional age-verification checks, i.e. the German regulator, the KJM, states that testing someone appears to be over 21 is highly unlikely to allow a false positive for someone under 18).

This waterfall technique ensures users have a choice and can find a method that works for them, making the system both accessible and inclusive. Completion times typically range from 5–10 seconds, and success rates are well above 95 per cent. Bias-mitigation techniques, mandatory accuracy benchmarks, and demographic performance auditing form part of the modern certification regime and ensure that proportionality applies not only to risk but also to fairness and accessibility.

Legislative Recommendation: *Enable a "waterfall" proportionality framework for age assurance (e.g., estimation for low-risk features like educational content, verification or estimation with an adequate buffer age for high-risk like chatbots), with built-in bias audits and accessibility benchmarks, ensuring fairness across demographics as highlighted in the staff memo.*

Applying Age Verification: Targeting Harms, Not Services, in the Tech Stack

The liveliest debate around age verification is where best to apply it in the technical stack, and how narrowly. There are superficially attractive arguments in support of device-based checks, either in the operating system itself or through app stores. Most state laws for adult websites have required the entire site be subject to age verification if more than one third of its content is adult in nature. This approach could, in theory, lead to protected speech being age-restricted, even if it constituted almost two thirds of the content on a site. While Texas's HB 1181 takes this approach and survived scrutiny by the Supreme Court,[11] we do not think this is the most effective or narrowly tailored approach. It is better to apply age restrictions to prevent harm wherever it is found, but not at the level of the site or app as a whole.

We support a layered approach to protecting children, and controls at any level may help. However, the proximity principle is core to health and safety measures - placing the protection as physically close to the risk as possible. Online, as technology evolves rapidly, we access digital services in an ever-growing number of ways (apps, connected devices, browsers within other apps, etc.). An app-store control may be effective with apps, but has little impact on websites. Meanwhile, children are still

[11] https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf

exposed to inappropriate obscene content on general platforms which happen to host a proportion of adult content that is less than the threshold.

For the most harmful areas of online risk, such as obscene adult content or, some argue, AI chatbots, the most effective protective measures are implemented at source. This also mitigates constitutional concerns by applying checks only to categories of content that fall outside First Amendment protection, as clarified in cases such as Free Speech Coalition v. Paxton[12]. This approach directly answers constitutional concerns by ensuring AV applies only to unprotected categories of content or clearly defined high-risk features, and not to lawful expression accessed by teens.

Legislative Recommendation: R*equire proximity-based age checks at source for high-risk AI/chatbot features, adult content etc., narrowly targeting harmful aspects within platforms.*

Age Verification vs Parental Controls

Much of the legislation the Committee is considering shies away from age verification and reverts to parental controls. This reflects a policy distinction that merits review.

Age verification is a substantively different policy with distinct objectives from parental controls. The latter rely on parents being informed, capable, and determined to monitor, set up, adjust, and resist pester-power over their children's activities. The Committee's own hearing memo reflects the evidence that many parents do not, or cannot, consistently manage these tools. Therefore, parental controls alone cannot provide a reliable population-level safety mechanism. In addition, any regulatory model that assumes "one device = one user = one stable age setting" is structurally misaligned with household realities. Many children will access the internet via shared devices.

Age verification sets a safety-net for all children. Parents can always exercise their right to override that mechanism by allowing a child to use an account the adult creates for them, or, in many cases, where parental consent is more formally enabled, to permit access after it has initially been halted by an age check.

Legislative Recommendation: R*equire age verification as a complementary "safety net" to parental tools, with override mechanisms for consent when appropriate - empowering families while ensuring population-level protection is the default. Undertake research to ascertain the percentage of children accessing the internet not via individually configured devices, rather via shared or 'hand me down' devices. Self-reported surveys alone cannot guide regulatory design. The regulator could commission or require:*

- *verified statistics on how many parents complete device-level or app-store-level control setups,*
- *measured data on how long setup takes across typical households,*
- *platform-verified data on how many child accounts are actively supervised,*

[12] ibid

- *empirical evaluation of the effectiveness of parental controls in reducing children's exposure to harms.*

Such data are essential to determine whether and how upstream controls can play a meaningful role in statutory safety duties.

Conclusion and Summary

The Age Verification Providers Association believes that modern, privacy-preserving age assurance technology is not only technically feasible but is the most effective and constitutionally sound method for protecting children from high-risk online harms when narrowly targeted. The solutions we describe - based on cryptographically signed, re-usable tokens and independent, double-blind checks, independently audited and certified - directly address historical concerns regarding data retention, anonymity, and accessibility.

Age assurance is not a complete solution to the broad set of online harms outlined in this hearing, but it is a necessary component of a wider safety ecosystem that includes parental tools, education, design improvements, and platform accountability.

By adopting a federal mandate for certified, interoperable, and privacy-preserving age signals, Congress can create a robust safety net that:

- **Protects Anonymity:** Ensures identity data is never shared with content providers or tracked across services.
- **Improves Access:** Allows users a choice of verification methods, ensuring inclusivity for those without traditional government IDs.
- **Addresses Constitutional Concerns:** Applies age checks narrowly to specific, high-risk features rather than imposing site-wide burdens on lawful expression.
- **Creates Consistency:** Implements a single standard (via ANSI certification) that avoids a state-by-state regulatory patchwork.

December 11, 2025

The Honorable Brett Guthrie
Chair, House Energy & Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member, House Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chair, Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis and Ranking Member Schakowsky:

The Alliance for Safe Online Pharmacies (ASOP Global) is pleased to submit a statement for the Congressional Record for the Commerce, Manufacturing, and Trade Subcommittee mark up of 18 bills to protect children and teens online. ASOP Global is a nonprofit 501(c)(4) organization that seeks to protect patient safety globally and to ensure patient access to safe and legitimate online pharmacies in accordance with applicable laws. ASOP Global is active in the United States, Canada, Latin America, Europe, and Asia.

ASOP Global appreciates the Subcommittee's continued attention to the dangers lurking online. In doing so, the Committee is addressing online counterfeit markets and the health and safety risks associated with the sale of illicit drugs online. ASOP Global is supportive of actions to protect minors from drug sellers operating online and through social media platforms.

In September 2025, ASOP Global sent a letter to key Committees and stakeholders in the House of Representatives and Senate highlighting our ongoing concerns related to the illegal sale of drugs online. The September letter has been attached to this letter. In this correspondence, we specifically call out the worrying practices associated with making counterfeit and substandard drugs that are purchased by adults and minors alike. To the naked eye, many counterfeit medications can appear legitimate, while containing lethal doses of controlled substances like fentanyl or mismanaged or counterfeit active pharmaceutical ingredients (API). Adults and minors both use digital platforms to purchase drugs, but teenagers are particularly vulnerable. ASOP Global is supportive of legislative options that aim to close the loopholes being weaponized by drug dealers.

Since 2020, the ASOP Global Foundation has conducted a national survey on consumer perceptions and behaviors related to online pharmacies, including the expanding role of social media. The most recent iteration, released in October, examined this growing influence in greater depth. We've attached the full report and a fact sheet summarizing the social-media-specific findings, including data on how social platforms are used for advertising and how they shape consumer purchasing trends. Please note that the study is limited to adult respondents.

Should you or your staff have any questions related to illegal drug sales online and how platforms facilitate these dangerous practices, please view ASOP Global as a resource. We look forward to advancing public health and patient safety with you.

ASOP GLOBAL FOUNDATION

ASOP GLOBAL | ALLIANCE FOR SAFE ONLINE PHARMACIES

ASOP Global Foundation
2025 U.S. Consumer Behavior Survey
Snapshot: Impact of Social Media & Influencers

Impact of Social Media & Influencers

Social media is rapidly evolving as both a marketing tool and a sales channel for prescription medicines, especially in the weight-loss and wellness space. Although buying prescriptions directly through social platforms remains less common than using other online sources, these platforms are becoming increasingly influential, particularly among consumers who have purchased GLP-1 medications online, in shaping how people discover, assess, and interact with online sellers.

Awareness and Use of Social Media as a Source of Prescription Medications

- **24%** of Americans with experience ordering prescription medicines online have **heard of social media being used as a source for prescription medicines**, yet only **15%** report having personally used social media for this purpose.
- **Use of social media as a source for purchasing prescription medicines** is slightly higher among those who have purchased **GLP-1 medications online (19%)** compared to those who have purchased **other prescription medicines online (13%)**.

While online GLP-1 purchasers are only modestly more likely to use social media as a resource to purchase their medicines, they are more likely to have utilized certain sources that have relied heavily on social media and influencer partnerships to gain visibility and promote GLP-1 products.

- Compared to those who have purchased other prescription medicines online, online GLP-1 purchasers are more likely to use **online wellness-clinics or med-spas** (**28% vs. 13%**), **online compounding pharmacies** (**27% vs. 18%**), and **online specialty pharmacies** (**33% vs. 16%**) to purchase their GLP-1 medicines.

Social Media as a Source of Promotion

Social media plays a greater role in shaping awareness of online sources among GLP-1 purchasers than it does for those who buy other medications online. They are more likely to have first encountered online medicine sellers through social media ads, influencers, or online discussion forums.

- **33%** of Americans who have purchased **GLP-1 medicines online** said they first learned about online sources of prescription medicines through **ads on social platforms**, compared with **21%** of other online purchasers.
- **25%** of GLP-1 online purchasers said they were **introduced to online sources by another social-media user**, compared with **11%** of other online purchasers.

Influence of Social Media on Decision-Making

Social media exerts a modestly stronger influence on purchasing decisions among GLP-1 buyers compared with other online purchasers. However, GLP-1 consumers also rely on a wider range of external sources when deciding whether and where to buy, suggesting that they are not dependent on social media alone but rather use it as one of multiple inputs guiding their decisions.

- **23%** of Americans who have purchased **GLP-1 medicines online** said **ads on social platforms** influenced their decision to order or helped them decide which seller to use, compared with **12%** of other online purchasers.
- **22%** of online GLP-1 purchasers said **celebrities or social-media influencers** influenced their decision, compared with **15%** of other online purchasers.
- **18%** of online GLP-1 purchasers said **others in online forums** influenced their decision, compared with **13%** of other online purchasers.

Perceptions of Influencer-Driven Promotion and Risk

Although social media plays an expanding role in how consumers discover and assess online sellers, Americans remain broadly skeptical of influencer-driven claims and advice. Even among those who have purchased prescription medicines online—including GLP-1 buyers—most perceive influencer-based recommendations as risky.

- **87%** of U.S. adults report that **taking a prescription medicine based solely on a social-media influencer's recommendation** is risky.
- Among those who have **purchased prescription medicines online**, **84%** share this view. Similarly, among those who have **purchased GLP-1 medicines online**, **85%** consider it risky as well.

These findings indicate that while online GLP-1 purchasers are not necessarily more trusting of social-media sources, they are more immersed in digital ecosystems where social-media marketing amplifies exposure to a broader array of online sellers. When medications are in high demand, such as GLP-1 products, social media often serves as a gateway—connecting consumers not only to legitimate pharmacy services but also to potentially riskier online sources.

About / Methods

The *Alliance for Safe Online Pharmacies Foundation* (ASOP Global Foundation) is a charitable, not-for-profit organization dedicated to addressing the growing public health threat of illegal online drug sellers, concentrating its activities in research and education to inform consumers and policymakers. The ASOP Global Foundation conducted this survey to assess how Americans perceive, purchase, and evaluate the safety of prescription medicines sold online.

The survey was composed of 60 questions and was administered online from August 22 to 26, 2025 by *Abacus Data*, a full-service market and public opinion research agency.

ASOP Global Foundation
2025 U.S. Consumer Behavior Survey

Executive Summary

Online Purchasing Behavior:

- **38% of U.S. adults** have purchased prescription medicines online; among these purchasers, **55%** now **buy all or most** prescriptions online. Three-quarters (73%) began purchasing within the past three years.
- **73%** of those who have purchased prescription medicines online say it's **very important** the source they use is a **U.S.-licensed pharmacy** (79% among GLP-1 purchasers); **91%** say they **verify licensure at least some of the time**, but only **39%** use **official sources** (NABP, State BOP, LegitScript, or PCAB).
- **73%** of those who have purchased prescription medicines online say they **only trust U.S. sellers** and **76%** trust only medicines **intended for the U.S. market**, yet **59%** of online purchasers report buying medicines they believed were **shipped from or intended for sale outside the U.S.**; and **91%** knew/suspected this **before** purchase.

Perceptions of Risk:

- **66%** of U.S. adults consider using medicines purchased online **risky—a 22-percentage point increase** from 2023.
- **87%** of U.S. adults believe the **health consequences** of counterfeit or substandard online medicines would be **serious**.
- **47%** of those who have purchased prescription medicines online have taken a medicine purchased online **without being fully confident** it was as **safe** as the medicine they would find at their local pharmacy.
- **27%** of those who have purchased prescription medicines online report having personally received **substandard/counterfeit** medicine or being **harmed** by a medicine they bought online.

Public Misconceptions:

- **65%** of U.S. adults **falsely believe** all websites offering online Rx/health services are **reviewed/approved by FDA or state regulators**.
- **51%** of U.S. adults **falsely believe** that **only safe, verified sellers** appear on the **first page** of search results.
- **44%** of U.S. adults **falsely believe** an online pharmacy can sell a prescription **without a prescription** if medical-history information is provided.

GLP-1 Medications:

- **56%** of U.S. adults report seeing **GLP-1 ads frequently** (daily/weekly).
- **14%** of U.S. adults have taken **GLP-1 medications** for diabetes or weight loss. 25% of these individuals have bought GLP-1 medications online.
- **40%** of those who have purchased GLP-1 medications online report having personally **received substandard or counterfeit prescription medicines or been harmed by prescription medicine bought online**, nearly double the prevalence reported by online purchasers of all other medications.

About

The Alliance for Safe Online Pharmacies Foundation (ASOP Global Foundation) is a charitable, not-for-profit organization dedicated to addressing the growing public health threat of illegal online drug sellers, concentrating its activities in research and education to inform consumers and policymakers.

The ASOP Global Foundation conducted this survey to assess how Americans perceive, purchase, and evaluate the safety of prescription medicines sold online.

To allow for longitudinal analysis of trends, questions asked of respondents in similar surveys conducted in 2020 and 2021 were repeated in this survey.

Methods

The 2025 ASOP Global Foundation Consumer Behavior Survey was conducted to assess how Americans perceive, purchase, and evaluate the safety of prescription medicines sold online. It builds on prior surveys conducted in 2020, 2021, and 2023, with refined question wording to more precisely capture home-delivery purchasing behavior and consumer understanding of risk, safety, and trust.

The following definitions were applied in the 2025 survey:

- **Online Pharmacy:**
  Not specifically defined in 2025. The question wording excluded websites or apps used by local brick-and-mortar pharmacies to process refills or delivery.

- **Prescription Medication:**
  A prescription medicine is a drug that should only be obtained with approval from a licensed healthcare professional (physician, physician assistant, nurse practitioner) based on a medical evaluation. Prescription medications do NOT include over-the-counter (OTC) medicines, vitamins, minerals, or herbal supplements, which can be bought in stores without prior consultation with a licensed healthcare professional (physician, physician assistant, nurse practitioner).

- **GLP-1 Receptor Agonists (GLP-1 Drugs):**
  A type of prescription medication commonly used to treat type 2 diabetes and weight loss in individuals with obesity. Examples include Ozempic (semaglutide), Wegovy (semaglutide), Rybelsus (semaglutide), Mounjaro (tirzepatide), Zepbound (tirzepatide), Trulicity (dulaglutide), Saxenda (liraglutide), and Victoza (liraglutide).

Additionally, in 2025, the survey wording for questions on online purchasing was revised to clarify that "online purchase" refers to websites or apps used to order prescription medications for home delivery. The definition excludes purchases made online or through apps for local pharmacy pickup, which was intended to more accurately reflect consumer behavior specific to digital pharmacies and online marketplaces.

The survey was composed of 60 questions and was administered online from August 22 to 26, 2025 by Abacus Data, a full-service market and public opinion research agency. A random sample of panelists were invited to complete the survey from a set of partner panels based on the Lucid Exchange platform, which connects market research agencies with panel provider companies. Panel providers on Lucid Exchange employ a diverse set of recruitment/sourcing methodologies, ensuring that the collective panel is not overly reliant or dependent on any demographic or segment of the population. Panels are double opt-in and blended to manage out potential skews in the data from a single source. Respondents are sourced from a variety of methods including ads and promotions across various digital networks, search, word of mouth and membership referrals, social networks, online and mobile games, affiliate marketing, banner ads, TV and radio ads, and offline recruitment with mail campaigns. Incentives are also varied.

To ensure adequate statistical power for subgroup analyses, the 2025 survey included an intentional oversample of U.S. adults who reported currently or previously taking a GLP-1 receptor agonist. All survey results were subsequently weighted to match the demographic composition of the U.S. adult population by age, gender, region, and educational attainment based on the most recent U.S. Census data. In addition, a secondary weighting adjustment was applied to correct for the oversample of GLP-1 users so that their representation in the weighted dataset reflects their true incidence in the general

population (approximately 14%). This two-step weighting process ensures that national estimates are representative of all U.S. adults while maintaining sufficient analytic base sizes for GLP-1–specific analyses. Unless otherwise noted, n-values shown for GLP-1 users and GLP-1 online purchasers represent unweighted subgroup sizes, while percentages presented in the report reflect population-weighted results consistent with these adjustments.

Results were also compared with similar surveys of 1,500 American adults conducted May 19–21, 2021, and September 7–10, 2023.

The margin of error for a comparable probability-based random sample of the same size is ± 2.51 percentage points, 19 times out of 20.

All survey results were subsequently weighted to match the demographic composition of the U.S. adult population by age, gender, region, and educational attainment based on the most recent U.S. Census data.

Results

Online Prescription Purchasing in 2025

Prevalence of Online Prescription Purchasing, Types of Online Sources, and Referrals

Online purchasing of prescription medicines is increasingly common and habitual for many Americans.

- **38%** of U.S. adults have previously purchased prescription medicines online for themselves or a dependent.
- Of those who have purchased online, **55%** now buy *all or most* of their prescriptions online.
- **Three in four (73%)** Americans who have purchased medications online report first doing so **within the past three years**, highlighting the rapid growth of this behavior.

Most Americans who buy prescriptions online use multiple types of online sources, most commonly two to three.

- **54%** of online purchasers report experience with **more than one type** of online source (41.5% have used one, 38% have used two to three, and 16% have used four or more).
- On average, Americans who purchase medications online have experience with **2.3 different types** of online sources.

Home-delivery online pharmacies and telehealth prescription services dominate, but some consumers also turn to higher-risk and more unconventional channels.[1]

- **65%** have used an **online home-delivery pharmacy**, making it the most popular source.
- **29%** have used an **online telehealth prescription service**, **reflecting the growing popularity of integrated direct-to-patient (DTC) digital health platforms.**
- **24%** have purchased from an **online international pharmacy.**
- Other sources include:
    - **20%** – Online compounding pharmacy
    - **20%** – Online specialty pharmacy
    - **17%** – Online wellness clinic or medical spa
    - **15%** – Social media
    - **13%** – Online marketplace
    - **5%** – Messaging app

Consistent with 2023 survey results[2], Americans' decisions about where to buy prescriptions online are shaped by both healthcare professionals and people they personally know. Healthcare providers and pharmacists remain year over year—presumably valued for their expertise in medication safety—and family members, friends, and acquaintances, who are likely viewed as reliable first-person sources of experience.

- On average, respondents reported **2.4 different influences** affecting their decision to purchase medicines online or determine which sources to use.[3]
- **49%** said their **healthcare provider** recommended they try or use specific online sources.
- **31%** said their **pharmacist** made such a recommendation.
- **27%** said they were influenced by a **family member, friend, or acquaintance**, and another **27%** said their **health insurance** recommended the online source they use.

---

[1] ***Note:*** *Respondents could select multiple options; totals may exceed 100%.*

[2] https://asopfoundation.pharmacy/wp-content/uploads/2023/12/ASOP-Foundation-Consumer-Behavior-Survey-Key-Findings-2023.pdf

[3] ***Note****: Respondents could select multiple options; totals may exceed 100%.*

- Social and media influences are also prevalent:
    - **17%** – Celebrities or social media influencers
    - **15%** – Ads on social media
    - **15%** – Others in online forums
    - **13%** – Coach, trainer, or gym recommendation

Types of Medications Purchased

Consumers continue to buy a wide range of prescription medications online. However, the most common medications are for pain and nausea, cardiovascular conditions, mental health needs, metabolic conditions, and skin, hair, and eye conditions.[4] These trends are relatively consistent with 2023 survey results except for infectious disease medications, which saw a decline in prevalence and medications for weight management, which saw an increase.[5]

Also worth noting is the relatively high percentage of online buyers who report having purchased controlled substances, including opioid pain medications (12%) and benzodiazepines (8%) online.

- **Medications for pain and nausea:**
    - **19%** have bought **non-opioid pain medications** (gabapentin [Neurontin], baclofen [Lioresal])
    - **14%** have bought medications for **migraines** (sumatriptan [Imitrex], ubrogepant [Ubrelvy])
    - **12%** have bought **opioid pain medications** (oxycodone [OxyContin], tramadol [Ultram])
- **Medications for metabolic conditions and weight management:**
    - **16%** have bought **GLP-1 medications** online for diabetes or weight loss (semaglutide [Ozempic], liraglutide [Saxenda].[6]

---

[4] ***Note**: Respondents could select multiple options; totals may exceed 100%.*

[5] https://asopfoundation.pharmacy/wp-content/uploads/2023/12/ASOP-Foundation-Consumer-Behavior-Survey-Key-Findings-2023.pdf

[6] ***Note** – 16% of Americans who have purchased prescription medicines online reported having previously purchased GLP-1 medications online.*

    - **16%** have bought medications for diabetes (metformin [Glucophage], linagliptin [Tradjenta]

- **Medications for chronic cardiovascular or inflammatory conditions:**
    - **18%** have bought medications for **blood pressure or arrhythmia** (lisinopril [Prinivil], amlodipine [Norvasc], Diltiazem [Tiazac], Metoprolol [Lopressor], Apixaban [Eliquis])
    - **18%** have bought medications for **high cholesterol** (atorvastatin [Lipitor], rosuvastatin [Crestor])
    - **10%** have bought **asthma/COPD medications** (albuterol [ProAir], budesonide/formoterol [Symbicort])
- **Medications for mental and cognitive health:**
    - **17%** have bought medications for **depression** (sertraline [Zoloft], bupropion [Wellbutrin])
    - **12%** have bought medications for **anxiety** (buspirone [Buspar], propranolol [Inderal])
    - **8%** have bought **benzodiazepines** online
- **Medications for skin, hair, and eye conditions:**
    - **12%** have bought **acne and wrinkle medication** (tretinoin [Retin-A], spironolactone [Aldactone], tretinoin [Renova], niacinamide)
    - **12%** have bought **eczema medication** (tacrolimus [Protopic], crisaborole [Eucrisa])
    - **12%** have bought **hair loss medication** (minoxidil [Rogaine], finasteride [Propecia])

Most Americans report purchasing generic medicines (71%) and brand medicines (61%) online. But many Americans are also purchasing medications not FDA approved.

- **39%** report buying **compounded medications**
- **32%** report buying **personalized medications**
- **19%** of online purchasers report buying **peptides**
- **11%** report buying medications labeled **“for research purposes only”**

Who Purchases Prescription Medicines Online

Online purchasing of prescription medicines is more common among younger and middle-aged adults than older adults.

- Online purchasing of prescription medicines is equally prevalent among adults aged **18–34 (46%)** and **35–54 (46%)**, but only **24%** of adults **55 and older** have purchased prescription medicines online.
- Regionally, prevalence is relatively even: **South (39%)**, **West (38%)**, **Northeast (39%)**, and **Midwest (35%)**.

Online purchasing of prescription medicines is more common among men, those with higher education, and those with higher household income.

- **46%** of males report having purchased prescription medicines online, compared to **30%** of females.
- **42%** of college-educated Americans report purchasing prescription medicines online, compared to **29%** of those with a high school degree or less.
- **61%** of those living in households earning **$100,000 or more** have purchased prescription medicines online, compared to **41%** of those earning **$50,000–$100,000** and **29%** of those earning **$50,000 or less.**

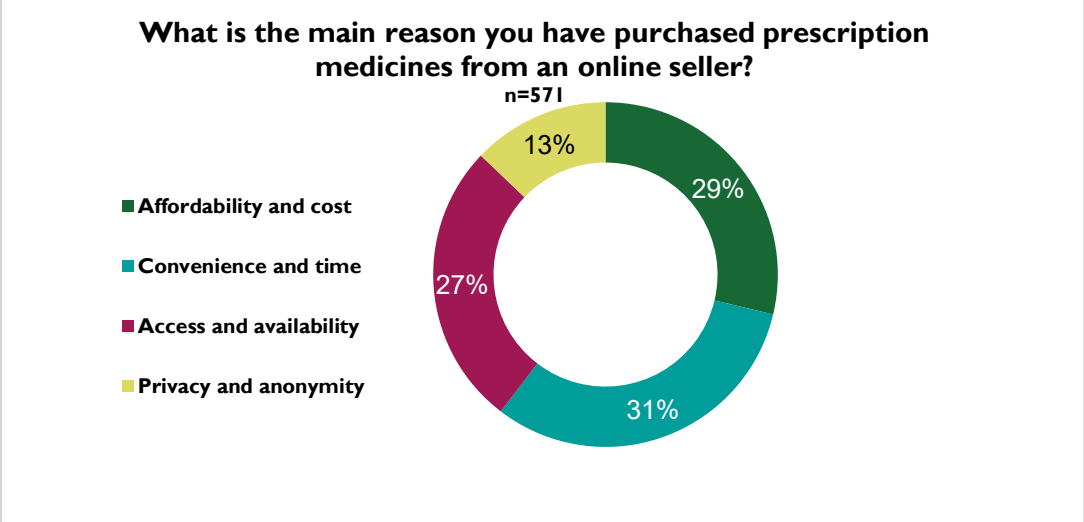
Many online purchasers still face challenges affording medications, though most have health insurance coverage.

- About **half (49%)** of those who have purchased prescription medicines online report they **struggle to afford** at least some of their prescription medications—significantly higher than the **25%** of Americans who have not purchased medicines online.
- The vast majority (**94%**) of online purchasers report having **health insurance that covers at least some prescription costs**, compared to **83%** of Americans who have not purchased prescription medicines online.

Why Americans Purchase Medicines Online

- Americans purchase prescription medicines online mainly for convenience and time savings (31%), affordability and cost (29%), and access and availability (27%).
    - The most common specific motivation (10%) is that it's easier to get refills when ordering online.
    - Other leading reasons include being able to get better prices through specific online sellers recommended by health insurers (9%) and saving more money overall (8%).

- Convenience also extends to having medications shipped directly to their door (7%).



AFFORDABILITY & COST (29%)	My health insurance offers a lower price if I use a specific online seller	9%
	I can save more money when I purchase my medications online	8%
	Buying medication online allows me to get medication when I cannot afford to see a healthcare provider for a prescription	5%
	Buying medication online helps me get medication my health insurance does not cover	5%
	Buying medication online allows me to afford medications I cannot afford at my local pharmacy	2%
CONVENIENCE & TIME (32%)	It is easier to get refills when I order online	10%
	It is more convenient to have online sellers ship the medication directly to my door	7%
	It is more convenient to order my medications online because I don't have to see a healthcare provider in person	5%
	The online ordering process is simpler and/or less time consuming than at my local pharmacy	5%
	Buying online allows me to buy larger quantities of the medication than at a local pharmacy	4%

ACCESS & AVAILABILITY (27%)	Buying medication online allows me to get my medication when I cannot get to my nearest pharmacy	6%
	I can get medications online that are often out of stock at my local pharmacy	5%
	Online pharmacies allow me to get medications not available in the U.S.	5%
	Buying medication online allows me to get medication when I cannot get an appointment with a local healthcare provider	5%
	I can get medications that I want or need that are only available online	3%
	I can get medications online without worrying that a local healthcare provider might not prescribe it	2%
PRIVACY & ANONYMITY (13%)	Buying medication online allows me to get medication without having to discuss it in person with a healthcare provider	6%
	Buying medication online helps me keep my medication private from my insurance company, healthcare provider, employer, etc.	4%
	Buying medication online helps me keep my medication private from family, roommates, acquaintances, etc.	3%

Knowledge Gaps and Misconceptions

What Americans Know

Most Americans, including those who purchase prescription medications online, are aware that all online sellers of prescription medicines need to be licensed as pharmacies. They are also aware of that FDA requires the manufacturers of brand and generic medicines to meet the same quality standards.

- **80% of Americans** are aware that websites and apps selling prescription medicines **must be licensed as pharmacies in every state they ship to.**
    - **82% of online prescription-medicine purchasers** answered this correctly.
    - **84% of online GLP-1 purchasers** answered this correctly.
- **83% of Americans** know that manufacturers of brand-name and generic drugs meet the same FDA quality standards.
    - **83% of online prescription-medicine purchasers** answered this correctly.

- **92% of online GLP-1 purchasers** answered this correctly.

What Americans DON'T Know - Online Protections and Prescription-Medicine Regulations

Despite being informed about the fundamental requirement that pharmacies be licensed, most Americans make dangerous, false assumptions about the extent to which this requirement is enforced online. Many Americans also seem uninformed or confused about the standards of practice required for pharmacies to acquire and maintain licensure. These misconceptions are significantly more prevalent among those who have previously purchased medicines online and those who have purchased GLP-1 medications online.

- **65% of Americans** falsely believe that all websites offering prescription medicines or health-care services online have been **reviewed and approved by FDA or state regulators** to ensure compliance with the law.
    - **75% of online prescription-medicine purchasers** hold this same false belief.
    - **76% of online GLP-1 purchasers** hold this same false belief.
- **51% of Americans** falsely believe that **only safe, verified online sellers** of prescription medicines appear on the **first page of search-engine results.**
    - **64% of online prescription-medicine purchasers** have this same false belief.
    - **68% of online GLP-1 purchasers** have this same false belief.
- **44% of Americans** falsely believe that **online pharmacies can sell prescription medicines without a valid prescription** if medical-history information is provided.
    - **58% of online prescription-medicine purchasers** hold this same false belief.
    - **62% of online GLP-1 purchasers** hold this same false belief.

What Americans DON'T Know – What are Compounded Medications

Most Americans are aware that there are fundamental standards that manufacturers of brand and generic medicines must meet, when it comes to compounded medications, misunderstanding is widespread and particularly acute amongst those who have previously purchased medicines, including GLP-1 drugs online.

Compounded medications are essentially copies of FDA-approved medications that the FDA permits certain facilities to prepare either when there is a shortage of medication, such as what occurred with many GLP-1 medications from March 2022 to February 2025, or when a patient requires a special formulation when the brand or generic version isn't suitable for them to take. However, many Americans appear to conflate compounded medications with generics and most assume that, like brand and generic medications, they are evaluated by the FDA for safety and quality. This is particularly concerning, given the prevalence of use of online compounding pharmacies (20%) and use of compounded medicines procured through online sources (39%).

- **43% of Americans** falsely believe that **compounded medications are the same as generics.**
    - **54% of online prescription-medicine purchasers** share this false belief.
    - **57% of online GLP-1 purchasers** share this false belief.
- **73% of Americans** falsely believe that **compounded medications are evaluated by FDA for safety and efficacy.**
    - **80% of online prescription-medicine purchasers** share this false belief.
    - **86% of online GLP-1 purchasers** share this false belief.

U.S. Pharmacy Licensure – Dissonance Between Perceived Importance and Practice

Most Americans who purchase prescription medicines online value U.S. pharmacy licensure and believe they verify—but fewer than half directly confirm licensure status using official sources.

- **82%** of those who have purchased prescription medicines online know that websites and apps selling prescription medicines must be licensed as pharmacies in every state they ship to.
- **71%** say it is *very important* that they purchase from a U.S.-licensed pharmacy, and **80%** view purchasing from a non-U.S.-licensed online pharmacy as risky.
- **90%** believe the source they purchase from is licensed in one or more U.S. states, and **91%** report verifying licensure either sometimes (35%) or always (56%).
- However, when asked *how* they verify licensure, only **39%** report using official sources such as NABP, state boards of pharmacy, LegitScript, or PCAB.

Despite high self-reported confidence in using licensed pharmacies, many consumers also appear to lack a clear understanding of how legitimate, licensed pharmacies operate—

potentially leading them to purchase from online sellers that fall outside accepted pharmacy standards.

- **Nearly half (46%)** of online prescription buyers report submitting their prescriptions by email, scan, or fax—methods that are inconsistent with NABP standards,[7] which require that electronically transmitted prescription drug orders be transmitted direct from prescriber to pharmacy and include a prescribing practitioner's electronic or digital signature.[8]
- An additional **5%** report that none of the online pharmacies they've used required a prescription at all, violating state laws which almost universally require that a valid prescription be obtained before any medicine is dispensed.

Despite expressing that pharmacy licensure is important and acknowledging the risks associated with unlicensed online sellers, many consumers who purchase their medicines online appear willing to forgo the protections and assurances offered by licensed pharmacies when presented with potential benefits, such as affordability, access, convenience, or privacy.

- While **39%** of online prescription medicine buyers said they would **stop purchasing medicines online** if they learned the sellers they use **weren't licensed anywhere, 33%** said they would **continue buying** from an **unlicensed source** if it significantly improved their **primary motivation for purchasing online**–be it cost savings, increased convenience, increased access, or increased privacy.
- When asked how specific benefits might affect their behavior, a substantial proportion of Americans who purchase prescription medicines online indicated a willingness to trade the safety associated with buying from a licensed and regulated pharmacy for each perceived benefit:
    - **45%** would buy from an unlicensed or unregulated source if it provided **greater privacy** when buying medicines.
    - **43%** would buy from an unlicensed or unregulated source if it made **ordering medicines more convenient.**
    - **41%** would buy from an unlicensed or unregulated source if it gave them **access to medicines they could not otherwise obtain.**

[7] National Association of Boards of Pharmacy. (2025, August). Model State Pharmacy Act and Model Rules of the National Association of Boards of Pharmacy. Mount Prospect, IL: National Association of Boards of Pharmacy. © 2025 NABP.

[8] ***Note****: Respondents could select multiple options; totals may exceed 100%.*

    - **41%** would buy from an unlicensed or unregulated source if it offered **lower prices.**

- When asked how changes in healthcare and prescription costs might affect their behavior, many Americans who purchase prescription medicines online indicated a willingness to trade the safety associated with buying from a licensed and regulated pharmacy for affordability:
    - **40%** said they would be more open to purchasing from an unlicensed or unregulated online source if their **overall healthcare costs rose sharply**.
    - **30%** said **any increase in healthcare costs** would make them more open to unlicensed sources.
    - **29%** said even a **modest increase in prescription costs** could push them toward unlicensed sources.
    - **28%** said a **large increase in prescription costs** would make them more open to unlicensed sources.

These findings suggest a disconnect between the perceived importance of the protections of pharmacy licensure and actual practice of those who purchase prescription medications online.

U.S. Sourcing - Dissonance Between Perceived Importance and Practice

Many consumers say they only trust U.S.-based sellers and acknowledge the risks of purchasing medicines that ship from entities located outside of the U.S.

- **73%** of online purchasers say they **only trust sellers located in the U.S.**, and **76%** say they **trust only medicines intended for the U.S. market.**
- **74%** say it is **risky** to take prescription medicines shipped from outside the U.S.—even if based solely on a **healthcare provider's recommendation.**

Despite these concerns, many online purchasers reported knowingly having purchased medicines they believed had a high likelihood of coming from international or foreign-market sources.

- **24% of online prescription medicine purchasers** have reportedly used an **international pharmacy**, and **59%** have purchased medicines they believed were **shipped from or intended for sale outside the U.S.**

- Among these purchasers, **91%** said they knew or suspected this prior to completing the purchase (**62% knew, 29% suspected**), suggesting deliberate risk-taking behavior.

Many consumers who purchase their medicines online are willing to purchase their prescription medicines from international sources when offered greater affordability, access, convenience, or privacy.

- While **39%** of online prescription medicine buyers said they would **stop purchasing medicines online** if they learned the medicine was **sold by someone in a foreign country, 52%** said they **would continue purchasing from a foreign source if it significantly improved their primary motivation for purchasing online**–whether cost savings, increased convenience, increased access, or increased privacy.

What Online Purchasers Value Most

Factors Prioritized When Choosing Online Sources

When asked what the top 3 most important factors are when purchasing prescription medication, those that have purchased medications online prioritize affordability, licensure status, and country of shipment over assurances of safety and quality.

- **48%** said knowing **what country the medicines are shipped from** was among their top three factors (34% top reason, 8% second, 7% third).
- **48%** said knowing the **seller is licensed as a pharmacy** was among their top three (24% top, 17% second, 7% third).
- **48%** also said **affordability** was among their top three factors (14% top, 16% second, 18% third).
- By comparison, fewer prioritized product quality and safety:
    - **40%** said being certain the **quality/safety matches their local pharmacy** was among their top three (7% top, 18% second, 15% third).
    - **33%** said being **confident in the quality/safety of medicines** was among their top three (5% top, 13% second, 15% third).

Risk Perceptions and Health Consequences

Confidence and Perceived Ability to Identify Risks

Perceived risk associated with purchasing prescription medicines online remains high and has risen sharply since 2023. Most Americans recognize that the health consequences of counterfeit or substandard medicines can be serious. Yet many continue to purchase medicines online despite limited confidence in the safety or effectiveness of the products they receive—leaving them vulnerable to harms that may be underreported due to the difficulty of detecting counterfeit or substandard products.

- **66%** of U.S. adults consider using medicines purchased online risky—a **22-percentage-point increase** from 2023.
- **87%** believe the health consequences of taking counterfeit or substandard medicines purchased online would be **serious**.

While most consumers acknowledge these risks, many who have purchased prescription medicines online nonetheless express confidence in their own ability to distinguish legitimate from illegitimate products.

- **72%** of those who have purchased prescription medicines online agree they can trust that the medicines they buy online are **just as effective** as those from a local pharmacy.
- **91%** of those who have purchased prescription medicines online say they are **at least somewhat confident** they can tell whether a medicine bought online is as safe and effective as one from a local pharmacy.

Despite this confidence, many admit to taking medicines without full assurance of safety or quality—often using personal experience after taking the drug to judge its legitimacy.

- **47%** of online prescription medicine purchasers report having taken a medicine bought online **without being fully confiden**t it was **just as safe** as what they'd receive at their local pharmacy.
- **46%** of online prescription medicine purchasers report having taken a medicine bought online **without being fully confident** it was **just as effective** as what they'd receive at their local pharmacy.

Medication Issues Encountered

A growing number of Americans who purchase medicines online report direct experience with products of questionable quality or safety. Nearly one in four have encountered at least one serious issue involving counterfeit, expired, or damaged medicines.

- **23%** of online purchasers report experiencing at least one **serious product-quality or safety concern**, including counterfeit, expired, or improperly stored medicines.[9]
    - **13%** said the medication they received was **counterfeit or fake**.
    - **10%** said they had received **expired medication**.
    - **7%** said they had received **damaged or improperly stored medication**.

Many also report receiving a medication different from what they ordered—discovering discrepancies through packaging, appearance, or performance.

- **17%** said they received a **different medication** than ordered.
    - **52%** said the **name** of the medication was not the same as what was ordered.
    - **51%** said the **packaging** looked different than expected.
    - **50%** said the **ingredients** were not the same as ordered.
    - **45%** said the **appearance** of the medication was different.
    - **32%** said the medication **did not work as it had before or as it should have**.
    - **32%** said the medication came from a **different manufacturer** than expected.
    - **14%** said the medication caused **unusual or unexpected side effects**.

Additional issues reported by online buyers include:

- **25%** said the **seller misused their payment information**.
- **24%** said their **medication was seized during shipping**.
- **23%** said the **seller misused their personal information**.
- **19%** said they were **charged but never received** the medication.

Reported Medication-Related Harms

More than one in four online purchasers report having received counterfeit or substandard medicines or being harmed by products purchased online—a figure that likely underestimates the true scope of harm, since cases involving insufficient or absent active ingredients often go undetected.

[9] ***Note**: Respondents could select multiple options; totals may exceed 100%*.

- **27%** of online purchasers report either having **received a counterfeit or substandard medicine** or **being harmed** by medicine they purchased online.
- **26%** have **reported** a medicine purchased online because they believed it was fake or harmful.

When problems occur, consumers most often turn to trusted health professionals and regulators for help.[10]

- **48%** said they would report an issue to their **healthcare provider**.
- **38%** said they would report it to their **pharmacist**.
- **38%** said they would report it to the **online seller**.
- **32%** said they would report it to the **FDA**.

That Americans who purchase prescription medicines online most often turn to healthcare providers and pharmacists—both when selecting an online seller and when facing product-quality concerns—suggests that these professionals are uniquely positioned to disrupt cycles of online harm. Yet the fact that more than a quarter of online purchasers report exposure to counterfeit, substandard, or otherwise harmful medicines indicates that while some providers help normalize online purchasing, not all are guiding patients to legitimate, verified sources.

Educating healthcare providers and pharmacists about their pivotal role in patient decision-making—and equipping them with practical tools and resources to identify legitimate online sellers—may be among the most effective strategies to reduce patient exposure to unsafe products and to strengthen confidence in lawful, verifiable online access to prescription medicines.

GLP-1 Medications Are Reshaping Online Demand

Prevalence of Online GLP-1 Purchasing and Demographics

GLP-1 receptor agonists (GLP-1 RAs) have rapidly become a popular medication used by Americans in the last few years and not surprisingly, this sharp rise has also been reflected in the online marketplace. GLP-1 medications have become a prominent and fast-growing category in the online prescription marketplace, drawing new consumers into online purchasing and exposing them to a wide range of online sources, both traditional and higher-risk channels.

[10] ***Note**: Respondents could select multiple options; totals may exceed 100%.*

- **14% of Americans report they are currently or have previously taken are** (7% currently, 7% previously), and another 14% say they are considering taking one.
- Among those with experience taking a GLP-1 medication, **25%** have purchased GLP-1 medications online.

Types of GLP-1 Medications Purchased Online

Americans who have purchased GLP-1 medications online report experience with a wide range of product types—including formulations that have not been approved by the FDA. While nearly all report purchasing brand-name products, many also report purchasing generic, compounded, "personalized/custom", "peptide," or "for research purposes-only" formulations, suggesting substantial variability in what consumers encounter and how these products are marketed online.[11]

- **95%** reported purchasing **brand-name** GLP-1 RAs online.
- **89%** reported purchasing **generic** GLP-1 RAs online.
- **74%** reported purchasing **compounded** GLP-1 RAs online.
- **72%** reported purchasing **personalized or custom** GLP-1 RAs online.
- **68%** reported purchasing **peptide** GLP-1 drugs online.
- **56%** reported purchasing GLP-1 drugs marketed **"for research purposes only."**

However, on average, Americans who have purchased GLP-1 medications online report experiencing purchasing **4.6 out of 6** listed GLP-1 product types from online sources and nearly half (**48%**) of GLP-1 online purchasers reported experience with **all six** categories of GLP-1 medications.

These results likely either significant confusion between several product types and or significant overlap in how these products are marketed rather than distinct purchases. Many respondents may have encountered overlapping or misleading claims (for example, compounded semaglutide marketed as "generic" or "personalized"), making it difficult to discern what kind of product they are taking.

Knowledge Gaps and Misunderstandings

Results from accompanying knowledge-assessment questions show widespread misunderstanding among online GLP-1 purchasers about how compounded and generic medications differ and the extent of FDA oversight.

[11] ***Note**: Respondents could select multiple options; totals may exceed 100%.*

- **86%** of online GLP-1 purchasers **incorrectly believe** that compounded medications are evaluated by the **FDA for safety and efficacy.**
- **57% incorrectly believe** that compounded medications are **the same as generics.**

These findings point to significant confusion among online GLP-1 purchasers regarding the regulatory status of the medicines they buy and help explain why many report experience with multiple product types.

Types of Online Sources and Referral Pathways

Americans who have purchased GLP-1 medications online report using a broader range of online sources than those who have purchased other prescription medicines online. **On average, 39% of GLP-1 online purchasers report prior experience with 2-3 online sources and 34% report experience with 4+ online sources compared to 38% and 8% of other online prescription purchasers respectively**. Additionally, certain non-traditional and higher-risk online sources are also more prevalent among those who purchase GLP-1 medications online. When asked directly whether they've used these resources to purchase GLP-1 medications, the prevalence confirms that they are using these online sources for GLP-1.

- **82%** of online GLP-1 purchasers have used an **online, home-delivery pharmacy** (compared to 59% of Americans who purchase other prescription medicines online).
- **50%** of online GLP-1 purchasers have used an **online telehealth prescription service** (compared to 21% of Americans who purchase other prescription medicines online).
- **32%** of online GLP-1 purchasers have used an **online international pharmacy** (compared to 21% of Americans who purchase other prescription medicines online).
- **27%** of online GLP-1 purchasers have used an **online compounding pharmacy** (compared to 18% of Americans who purchase other prescription medicines online).
- **28%** of online GLP-1 purchasers have used an **online wellness clinic or med-spa** (compared to 13% of Americans who purchase other prescription medicines online).
- **19%** of online GLP-1 purchasers have used **social media** (compared to 13% of Americans who purchase other prescription medicines online).
- **11%** of online GLP-1 purchasers have used a **messaging app** (compared to 3% of Americans who purchase other prescription medicines online).

Those who purchase GLP-1 medications online also report on average more external influences on their decision to order medications online or what online sources to order from. **On average, GLP-1 online purchasers report being influenced to order medications online or receiving referrals for specific sellers from 3.5 external sources compared to the average 2.4 external influences reported by their peers**. Additionally, certain external influences are more prevalent among those who purchase GLP-1 medications online.

- **67%** of online GLP-1 purchasers said they were influenced by a **healthcare provider** (compared to 42% of Americans who purchase other prescription medicines online).
- **44%** of online GLP-1 purchasers said they were influenced by a **pharmacist** (compared to 26% of Americans who purchase other prescription medicines online).
- **40%** of online GLP-1 purchasers said they were influenced by a **health-insurance recommendation or plan** (compared to 23% of Americans who purchase other prescription medicines online).
- **36%** of online GLP-1 purchasers said they were influenced by **family or friends**. (compared to 24% of Americans who purchase other prescription medicines online).
- **23%** of online GLP-1 purchasers said they were influenced by **ads on social media** (compared to 12% of Americans who purchase other prescription medicines online).
- **22%** of online GLP-1 purchasers said they were influenced by **celebrities or social-media influencers** (compared to 15% of Americans who purchase other prescription medicines online).
- **21%** of online GLP-1 purchasers said they were influenced by **online reviewers** (compared to 9% of Americans who purchase other prescription medicines online).
- **21%** of online GLP-1 purchasers said they were influenced by a **coach, trainer, or gym** (compared to 10% of Americans who purchase other prescription medicines online).

Risk Perceptions and Reported Harms

Reported harms are notably higher among those who have purchased GLP-1 medications online GLP-1 compared to Americans who have bought other medications online.

- **40%** of those who have purchased GLP-1 medications online report having personally **received substandard or counterfeit prescription medicines or been harmed by prescription medicine purchased online**, nearly double the prevalence (22%) reported by online purchasers of all other medications.

This could be because online GLP-1 purchasers report a higher tolerance for risk compared to their peers.

- **54%** of online GLP-1 purchasers have taken a medicine they bought online **without being fully confident it was just as safe** as what they would receive at their local pharmacy (compared to 44% of online purchasers of all other medication).
- **53%** of online GLP-1 purchasers have taken a medicine they bought online **without being fully confident it was just as effective** as what they would receive at their local pharmacy (compared to 43% of online purchasers of all other medication).

Also, while most online GLP-1 purchasers recognize the dangers associated with unverified or potentially unsafe online sellers:

- **84%** of online GLP-1 purchasers agree it is **risky to take a prescription medication obtained from an online seller that the FDA has warned** may provide incorrect doses or harmful formulations.

As noted above, many online GLP-1 purchasers use sources the FDA has cautioned against.[12]

- **36%** online GLP-1 purchasers have used **international online sellers** to purchase GLP-1 medications.
- **31%** online GLP-1 purchasers have used **online compounding pharmacy** to purchase GLP-1 medications.
- **21%** online GLP-1 purchasers have used **online med-spa or wellness clinic** to purchase GLP-1 medications.
- **22%** online GLP-1 purchasers have used **social media** to purchase GLP-1 medications.

Also as noted above, many online GLP-1 purchasers take GLP-1 formulations the FDA has cautioned against.[13]

---

[12] U.S. Food & Drug Administration. *FDA's Concerns with Unapproved GLP-1 Drugs Used for Weight Loss.* 25 Sept. 2025, www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/fdas-concerns-unapproved-glp-1-drugs-used-weight-loss.

[13] U.S. Food & Drug Administration. *FDA's Concerns with Unapproved GLP-1 Drugs Used for Weight Loss.* 25 Sept. 2025, www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/fdas-concerns-unapproved-glp-1-drugs-used-weight-loss.

- **74%** reported purchasing **compounded** GLP-1 RAs online.
- **72%** reported purchasing **personalized or custom** GLP-1 RAs online.
- **68%** reported purchasing **peptide** GLP-1 drugs online.
- **56%** reported purchasing GLP-1 drugs marketed **"for research purposes only."**

Impact of Social Media

Social media continues to evolve both as a marketing tool and a transactional sales channel for prescription medicines, particularly in the weight-loss and wellness space. While using social media to purchase prescription medicines online remains relatively uncommon compared with other online sources, social media platforms are playing a gradually more prominent role in how consumers—especially those who have purchased GLP-1 medications online—encounter, evaluate, and engage with online prescription medicine sellers.

Awareness and Use of Social Media as a Source of Prescription Medications

General awareness of social media being used to purchase prescription medicines remains modest, but use of social media for this purpose is somewhat higher among those who have purchased GLP-1 medications online. This trend suggests that increased algorithmic targeting and social-media marketing around weight-loss and wellness products may be exposing GLP-1 buyers to these platforms more frequently than other consumers.

- **24%** of Americans with experience ordering prescription medicines online have **heard of social media being used as a source for prescription medicines**, yet only **15%** report having personally used social media for this purpose.
- **Use of social media as a source for purchasing prescription medicines** is slightly higher among those who have purchased **GLP-1 medications online (19%)** compared to those who have purchased **other prescription medicines online (13%)**.

While online GLP-1 purchasers are only modestly more likely to use social media as a resource to purchase their medicines, they are more likely to have utilized certain sources that have relied heavily on social-media and influencer partnerships to gain visibility and promote GLP-1 products in the last few years.

- Compared to those who have purchased other prescription medicines online, online GLP-1 purchasers are more likely to use **online wellness-clinics or med-**

spas (**28% vs. 13%**), **online compounding pharmacies** (**27% vs. 18%**), and **online specialty pharmacies** (**33% vs. 16%**) to purchase their GLP-1 medicines.

Social Media as a Source of Promotion

Social media plays a greater role in shaping awareness of online sources among GLP-1 purchasers than it does for those who buy other medications online. They are more likely to have first encountered online medicine sellers through social media ads, influencers, or online discussion forums.

- **33%** of Americans who have purchased **GLP-1 medicines online** said they first learned about online sources of prescription medicines through **ads on social platforms**, compared with **21%** of other online purchasers.
- **25%** of GLP-1 online purchasers said they were **introduced to online sources by another social-media user**, compared with **11%** of other online purchasers.
- **16%** of GLP-1 online purchasers said **a celebrity or social-media influencer** first made them aware of online sellers, compared with **7%** of other online purchasers.
- **16%** of GLP-1 online purchasers said they first heard about an online source in **an online discussion group or forum**, compared with **5%** of other online purchasers.

Influence of Social Media on Decision-Making

Social media exerts a modestly stronger influence on purchasing decisions among GLP-1 buyers compared with other online purchasers. However, GLP-1 consumers also rely on a wider range of external sources when deciding whether and where to buy, suggesting that they are not dependent on social media alone but rather use it as one of multiple inputs guiding their decisions.

- **23%** of Americans who have purchased **GLP-1 medicines online** said **ads on social platforms** influenced their decision to order or helped them decide which seller to use, compared with **12%** of other online purchasers.
- **22%** of online GLP-1 purchasers said **celebrities or social-media influencers** influenced their decision, compared with **15%** of other online purchasers.
- **18%** of online GLP-1 purchasers said **others in online forums** influenced their decision, compared with **13%** of other online purchasers.
- However, on average, online GLP-1 purchasers rely on **3.5 sources** when deciding where to buy, compared with **2.4** among other online purchasers.

Perceptions of Influencer-Driven Promotion and Risk

Although social media plays an expanding role in how consumers discover and assess online sellers, Americans remain broadly skeptical of influencer-driven claims and advice.

Even among those who have purchased prescription medicines online—including GLP-1 buyers—most perceive influencer-based recommendations as risky.

- **87%** of U.S. adults report that **taking a prescription medicine based solely on a social-media influencer's recommendation** is risky.
- Among those who have **purchased prescription medicines online**, **84%** share this view.
- Among those who have **purchased GLP-1 medicines online**, **85%** consider it risky as well.

These findings indicate that while online GLP-1 purchasers are not necessarily more trusting of social-media sources, they are more immersed in digital ecosystems where social-media marketing amplifies exposure to a broader array of online sellers. When medications are in high demand, such as GLP-1 products, social media often serves as a gateway—connecting consumers not only to legitimate pharmacy services but also to potentially riskier online sources.

Impact of GLP-1 Advertising

Exposure to GLP-1 Advertising

Americans are heavily exposed to GLP-1 advertising, which increasingly shapes perceptions and decisions—particularly among those who purchase prescription medicines online.

- **56%** of Americans report seeing **GLP-1 RA ads frequently** (daily or weekly).
- **Among those who have prior or current experience using a GLP-1 medication, 81% report frequent exposure to GLP-1 ads**, compared with 42% of Americans who have not used a GLP-1 medication.
- Exposure is even higher among **online purchasers of prescription medicines (72%)** and especially among **online purchasers of GLP-1 medications (86%)**.

Advertising and Online Purchasing Behavior

Frequent exposure to GLP-1 advertising is linked with use of a wider range of online purchasing channels. Compared to those who rarely or never see such ads, those who see GLP-1 ads daily or weekly are more likely to engage with more types of online sellers and are more likely to use certain higher-risk online sellers compared to those who rarely or never see such ads.

- **70%** of all frequent GLP-1 ad viewers have used an **online or home-delivery pharmacy**, compared to 54% of those with limited or no exposure.

- **33%** of all frequent GLP-1 ad viewers have used **telehealth prescription services**, compared to 18% of those with limited or no exposure.
- **28%** of all frequent GLP-1 ad viewers have used **international pharmacies**, compared to 12% of those with limited or no exposure.

Advertising and Decision Influences

Frequent GLP-1 ad exposure also corresponds with a broader range of influences shaping purchasing decisions.

- Those who see GLP-1 ads daily or weekly are significantly more likely to cite **health insurers (31% vs. 11%)**, **celebrities or influencers (19% vs. 8%)**, **social-media ads (17% vs. 6%)**, and **online forums (13% vs. 2%)** as factors influencing where they purchase—roughly double the rates among those with little to no ad exposure.

Expectations of Advertising Credibility

At the same time, **the vast majority of Americans (86%)** say it is important that **ads for prescription medicines sold online make only clinically supported claims**—a view shared by **90%** of online purchasers and **96%** of online GLP-1 purchasers. This contrast highlights a clear gap between consumers stated expectations of advertising accuracy and the confusion that persists among those most frequently exposed to promotional content.

Demographic Profile of Respondents

[**Figure 1. Demographic Profile of 2025 Respondents** — Side-by-side comparison of All Respondents, Online Prescription-Medicine Purchasers, and Online GLP-1 Purchasers.]

		Total (n=1501)	Online prescription medicine purchasers (n=571)	Online GLP-1 Purchasers (n=156)*
		%	%	%
GENDER	Male	48%	59%	47%
	Female	52%	41%	53%
AGE GROUP	18 to 24	12%	12%	13%
	25 to 34	17%	24%	16%
	35 to 44	16%	22%	14%
	45 to 54	17%	19%	16%

	55 to 64	19%	13%	20%
	Over 65	19%	10%	21%
REGION USA	South	38%	39%	38%
	West	24%	24%	24%
	Northeast	17%	18%	17%
	Midwest	21%	19%	21%
Which best describes where you live?	Urban/metropolitan – Densely populated, city or large town	38%	46%	37%
	Suburban – Mainly residential, bordering a city or large town	41%	40%	41%
	Rural – Sparsely populated, small town or village	21%	14%	22%
EDUCATION	HS or less	30%	23%	32%
	PSE	70%	77%	68%
What is your race or ethnicity?	White (Non-Hispanic)	67%	63%	67%
	Hispanic or Latino	14%	15%	14%
	Black or African American	13%	15%	13%
	Asian	4%	5%	4%
	Native American or Alaska Native	1%	1%	1%
	Native Hawaiian or Other Pacific Islander	1%	0%	1%
	Other (please specify):	0%	0%	0%
	Prefer not to answer	0%	0%	0%
Which of the following religions do you most closely identify with?	Christian – Protestant	32%	32%	33%
	Christian – Catholic	23%	29%	22%
	Christian – Other (e.g., Orthodox, LDS, Evangelical)	9%	8%	10%
	Spiritual but not religious	8%	6%	9%
	Jewish	4%	5%	4%
	Muslim	4%	7%	3%

	Buddhist	1%	2%	1%
	Hindu	1%	1%	1%
	Atheist	4%	3%	4%
	Agnostic	4%	4%	4%
	Other (please specify)	4%	2%	4%
	Prefer not to answer	7%	3%	7%
Generally speaking, do you think of yourself as a Democrat, a Republican, an independent, or something else?	Democrat	30%	29%	31%
	Republican	37%	45%	36%
	Independent	27%	22%	27%
	Something else	6%	3%	6%
Including yourself, how many individuals live in your household?	1	25%	19%	26%
	2	28%	21%	29%
	3	19%	22%	19%
	4	18%	28%	16%
	5 or more	10%	10%	10%
INCOME	Low	61%	47%	64%
	Middle	31%	40%	29%
	High	9%	13%	7%

**The total unweighted number of GLP-1 online purchasers is n=156. For analyses, this was adjusted to account for oversampling of U.S. adults who reported currently or previously taking a GLP-1 receptor agonist (for diabetes or weight management).*

ASOP GLOBAL | ALLIANCE FOR SAFE ONLINE PHARMACIES

September 8, 2025

To Whom It May Concern:

Executive Summary: Foreign and domestic actors peddle poison for profit. They are taking advantage of America's overwhelming demand for medicines, opacity of the internet, the ability to hide in foreign jurisdictions, and porous U.S. borders. These bad actors are profiting from the online sale of mass quantities of counterfeit drugs, dangerous controlled substances, and illegal API used in compounded drugs offered online. Federal policymakers must commit to concrete, sustainable strategies to curb this public health and national security threat.

Foreign and domestic actors—including criminal elements—use websites, social media channels, and online marketplaces to peddle addictive controlled substances, counterfeit and unapproved prescription drugs, and illegal, mass-produced compounded drugs to Americans. This is a threat both to patient safety and our national security.

The Alliance for Safe Online Pharmacies (ASOP Global) urges you to take action against illegal online drug sellers to keep Americans safe. ASOP Global is a nonprofit 501(c)(4) organization whose members include pharmacists, pharmacies, academics, patient safety organizations, drug manufacturers, payment processors, and internet security organizations. Since 2009, ASOP Global has been working to protect patient safety globally and to ensure patient access to safe and legitimate online pharmacies in accordance with applicable laws.

The safety and security threats posed by illegal online drug sellers are pervasive and growing. Today online pharmacies, telemedicine, and direct-to-consumer healthcare are common and necessary, when done safely and legally. Indeed, more than half of American adults report having bought medicine online.[1] Unfortunately, illegal online pharmacies taint the legitimate market and threaten patient safety by operating illegally and selling illegitimate, potentially dangerous products:

- A 2023 research survey conducted by the ASOP Global Foundation found that more Americans are purchasing medication online than ever before: 52% of Americans aged 18 and older report having used an online pharmacy. This is a 10-percentage-point increase compared to 2021, and 17-percentage-point increase from 2020.[2]
- According to the National Association of Boards of Pharmacy (NABP), 96% of online drug sellers operate illegally. These sellers provide products from foreign or unlicensed sources, without valid prescriptions, or distribute counterfeit, substandard, or otherwise illegal medications.[3] [4]
- This rise in patients turning to online pharmacies comes at a cost to patient health and safety: 24% of Americans who had purchased medicine online report having received harmful, counterfeit, or substandard product.[5]
- Medicines sold by illegal online drug sellers have been found to be subpotent, super-potent, contaminated (such as with other drug ingredients, chemicals, or toxins), or to contain illegal active pharmaceutical ingredients (API), leading to adverse effects and even patient death. [6] [7] [8]

Preying on Unsuspecting Americans: Restrictions in access to prescription medications—whether due to policy barriers, coverage restrictions and limitations, provider access challenges, or drug shortages—drive unsuspecting consumers to seek alternative options on the internet. Unfortunately, less than 5% of Americans know how to find a safe, verified online pharmacy.[9] This environment has allowed for American patients to become test-subjects for unapproved drug combinations and modes of administration, including the sale of 'for research purposes only' chemicals, and do-it-yourself administration kits – putting Americans at risk of serious harm, including death. [10] [11] [12] [13] Bad actors like drug counterfeiters, digital drug dealers, illicit manufacturers, and illegal mass-production compounders take advantage of desperate patients.[14] [15]

Demand for Illegal GLP-1s Sold Online: Today, this problem is most evident in the illegal online market for GLP-1 agonists approved to treat diabetes and weight loss.[16] [17] Underregulated telehealth platforms and med spas have become increasingly common sources of GLP-1 medicines. A 2024 study found that 12% of American adults reported ever taking a GLP-1, with 21% of those purchasing the product through telehealth companies or med spas that typically sell medications not approved by the FDA.[18] A bipartisan coalition of 38 state and territory attorneys general said it best:

> "…online retailers are illegally selling the active ingredients of GLP-1 drugs directly to consumers, without a prescription. These retailers claim that the active ingredients they sell are "for research purposes only" or "not for human consumption". In reality, these companies advertise directly to consumers on social media, claiming that their products are an easier and more affordable way to obtain GLP-1 drugs. Much like with counterfeit versions, these active ingredients come from unregulated, undisclosed sources in countries like China and India and pose risks of contamination and inclusion of foreign substances."[19] [20]

All Classes of Medicines Are Illegally Sold Online: Beyond GLP-1 drugs, the risks posed by illegal online drug sellers extend to all classes of medicines. Illegal online sellers sell counterfeit and unapproved cancer treatments, HIV medicines, controlled substances, hormones, and more.[21] For more than 15 years, ASOP Global has tracked patient harms, revealing how people seeking everything from erectile dysfunction drugs to cancer treatments and even vitamins have fallen prey to global criminal schemes.[22]

National Security Implications: The threat from illegal prescription drugs often comes from foreign actors and American adversaries, reinforcing that this problem is a national security threat. Foreign actors in China, Russia, Mexico, Turkey and elsewhere prey on American patients. [23] [24] [25] [26] [27] [28]These foreign actors take advantage of Americans' overwhelming demand for medicines, opacity of the internet, the ability to hide in foreign jurisdictions, and porous U.S. borders to profit from the online sale of mass quantities of counterfeit drugs, dangerous controlled substances, and illegal API used in compounded drugs offered online.

As just one example, giant Chinese e-commerce platforms have a well-documented history of selling counterfeits into the U.S., including drugs.[29] Despite efforts by both the current and previous U.S. administrations, foreign governments either ignore or have not consistently prioritized this threat. Without global enforcement, illegal online drug sellers and illicit manufacturers persist, largely targeting Americans. [30] [31] [32] This puts United States' national security at risk.

Federal Policymakers Need to Act

ASOP Global urges you to use your time, resources, and authority to protect patients from illegal online drug sellers and related bad actors putting your constituents at risk. To begin, we ask that you support the following federal policies, current as of the date of this letter:

- Support the policy in FDA's FY2026 legislative proposals that would **allow mandatory destruction of imported products** that pose serious public health risks, eliminating the current option to export them.
- **Support report language included in the FY2026 Ag-FDA appropriations bills** in the Senate and House bills which address counterfeit medicines, illegal imports of unapproved new drugs, and enforcements of statutory limits on compounded copies when FDA-approved medicines are available.
- Support the proposal in FDA's FY2026 legislative proposals that provides FDA with **new authorities regarding certificates of analysis for APIs** used in drug manufacturing, including human drug compounding, that require identifying the name, address, and unique facility identifier of the API's original manufacturer.
- **Support the Protecting Patients from Deceptive Drug Ads Online Act** to address false and misleading prescription drug promotions by having FDA issue warning letters and fines to influencers and telehealth companies that engage in misleading advertising practices.
- **Cooper Davis and Devin Norring Act** which requires electronic communication service providers and remote computing service providers to report knowledge of various drug-related offenses (e.g., unlawful distribution of a counterfeit controlled substance, fentanyl, or methamphetamine) to the Drug Enforcement Administration.

Beyond these specific policies, we ask that you urge and support FDA, Customs and Border Protection, the Federal Trade Commission, the Department of Homeland Security, U.S. Patent & Trademark Office, and others to prioritize inspections and enforcement against all actors involved in this growing patient safety and national security threat. And where federal agencies lack either the authority or capacity to take action against actors engaging in dangerous medicine practices, Congress must act to focus resources to give agencies the tools they need. ASOP Global and our members have decades of experience and welcome the chance to work with you on specific, tangible actions to improve patient safety.

ASOP Global and our members have decades of experience and welcome the chance to work with you on specific, tangible actions to enhance patient safety in your state. Thank you for your attention on this serious matter. Please consider ASOP Global a resource going forward. We look forward to working with you to protect Americans.

Please do not hesitate to reach out to the ASOP Global by contacting Maya Bolter (maya.bolter@faegredrinker.com)

Carrie Harney

ASOP Global Board Chair
www.BuySafeOnlineRx.pharmacy

[1] *Consumer Behavior Survey Key Findings 2023*. [PDF] ASOP Global Foundation. Available at: https://asopfoundation.pharmacy/wp-content/uploads/2023/12/ASOP-Foundation-Consumer-Behavior-Survey-Key-Findings-2023.pdf

[2] *Consumer Behavior Survey Key Findings 2023*. [PDF] ASOP Global Foundation. Available at: https://asopfoundation.pharmacy/wp-content/uploads/2023/12/ASOP-Foundation-Consumer-Behavior-Survey-Key-Findings-2023.pdf

[3] *Consumer Behavior Survey Key Findings 2023*. [PDF] ASOP Global Foundation. Available at: https://asopfoundation.pharmacy/wp-content/uploads/2023/12/ASOP-Foundation-Consumer-Behavior-Survey-Key-Findings-2023.pdf

[4] National Association of Boards of Pharmacy (NABP), (2022). Rogue Rx Activity Report: Disrupting Illegal Online Pharmacies. National Association of Boards of Pharmacy. Available at: https://nabp.pharmacy/wp-content/uploads/2022/10/Rogue-Rx-Activity-Report-Disrupting-Illegal-Online-Pharmacies-2022.pdf

[5] *Supra* note 1.

[6] U.S. Food and Drug Administration (FDA), BeSafeRx: Frequently Asked Questions (FAQs), BeSafeRx: Your Source for Online Pharmacy Information (2020). Available at: https://www.fda.gov/drugs/besaferx-your-source-online-pharmacy-information/besaferx-frequently-asked-questions-faqs

[7] U.S. Drug Enforcement Administration (DEA)**,** *DEA Issues Warning About Illegal Online Pharmacies* (2024). Available at: https://www.dea.gov/alert/dea-issues-warning-about-illegal-online-pharmacies

[8] Centers for Disease Control and Prevention (CDC)**.** *Drug Overdose Deaths with Evidence of Counterfeit Pill Use — United States, July 2019–December 2021. Morbidity and Mortality Weekly Report*, Weekly / September 1 2023**;** 72(35): 949–956, Available at: https://www.cdc.gov/mmwr/volumes/72/wr/mm7235a3.htm

[9] Alliance for Safe Online Pharmacies (ASOP Global). (n.d.) *Online Pharmacy Consumer Behavior and Perception Survey*. Available at: https://buysaferx.pharmacy/public-awareness-campaigns/drug-importation/factsheets/online-pharmacy-consumer-behavior-and-perception-survey/

[10] Oregon Board of Pharmacy (2025). *Position Statements*. [online] Oregon.gov. Available at: https://www.oregon.gov/pharmacy/pages/position-statements.aspx

[11] Office of the Attorney General William Tong (2025)**.** *Attorney General Tong Sues GLP-1 Weight Loss Drug Distributor Triggered Brand, Announces Investigation Into Made In China Over Sale of Untested, Unsafe "Research-Grade" Drugs to Connecticut Consumers*. Available at: https://portal.ct.gov/ag/press-releases/2025-press-releases/attorney-general-tong-sues-glp-1-weight-loss-drug-distributor-triggered-brand#:~:text=Letter%20to%20Connecticut%20Weight%20Loss,GLP-1%20weight%20loss%20drugs

[12] Office of the Attorney General of Maryland (2025). *Attorney General Brown Calls for Action Against Counterfeit Weight Loss Drug Makers*. [online]. Available at: https://www.marylandattorneygeneral.gov/press/2025/021925.pdf

[13] U.S. Food and Drug Administration (2025). *FDA's Concerns with Unapproved GLP-1 Drugs Used for Weight Loss*. [online]. Available at: https://www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/fdas-concerns-unapproved-glp-1-drugs-used-weight-loss

[14] American Society of Health-System Pharmacists (2025) *Drug Shortages Statistics*. ASHP. Available at: https://www.ashp.org/drug-shortages/shortage-resources/drug-shortages-statistics?loginreturnUrl=SSOCheckOnly#:~:text=SUMMARY,for%20the%20past%2018%20months.

[15] Mackey, T. K. and Nayyar, G., (2016). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety*, 15(5), pp.681–694. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC3374535/

[16] U.S. Food and Drug Administration (2024) *FDA approves first treatment to reduce risk of serious heart problems specifically in adults with obesity or overweight*. FDA. Available at: https://www.fda.gov/news-events/press-announcements/fda-approves-first-treatment-reduce-risk-serious-heart-problems-specifically-adults-obesity-or-overweight

[17] U**.**S. Food and Drug Administration (2023) *FDA approves new medication for chronic weight management*. FDA. Available at: https://www.fda.gov/news-events/press-announcements/fda-approves-new-medication-chronic-weight-management

[18] Montero, A., Sparks, G., Presiado, M. and Hamel, L.(2024). *KFF Health Tracking Poll May 2024: The Public's Use and Views of GLP-1 Drugs*. [online] Kaiser Family Foundation. Available at: https://www.kff.org/health-costs/kff-health-tracking-poll-may-2024-the-publics-use-and-views-of-glp-1-drugs/

[19] National Association of Attorneys General (2025) *State and Territory Attorneys General Urge FDA to Take Action Against Counterfeit and Illegally Sold GLP-1 Drugs*, NAAG. Washington, D.C., 19 February. Available at: https://www.naag.org/policy-letter/state-and-territory-attorneys-general-urge-fda-to-take-action-against-counterfeit-and-illegally-sold-glp-1-drugs/

[20] The New York Times, 2024. *Ozempic Fake Counterfeit Drugs*, The New York Times (Well blog), (2025). Available at: https://www.nytimes.com/2024/07/12/well/ozempic-fake-counterfeit-drugs.html?searchResultPosition=1

[21] Partnership for Safe Medicines (2017) *Bipartisan Safety Issues: How Many Different Kinds of Black Market Medicines Have Been Sold in Your State?*. Available at: https://www.safemedicines.org/2017/01/bipartisan-safety-issues.html

[22] ASOP Global. (2020). *Patient Harms Tracker*. Available at: https://buysaferx.pharmacy/wp-content/uploads/2020/06/Patient-Harms-Tracker-6-4-2020.pdf

[23] IQVIA Institute for Human Data Science (2023) *Assessing the impact of illegal online pharmacies in the U.S.: Sales, volume and adverse events*. IQVIA Institute for Human Data Science, in collaboration with Translucent Datalab and IE University. Available at: https://www.iqviainstitute.org

[24] *Gilead Sciences, Inc. et al v. Meritain Health, Inc. et al*, No. 1:24-cv-03566-JRR (D. Md. June 24, 2025). Memorandum Opinion signed by Judge Julie Rebecca Rubin.

[25] Eban, K. (2024) Why Counterfeit Ozempic Is a Global-Growth Industry. Vanity Fair, 4 June. Available at: https://www.vanityfair.com/news/story/counterfeit-ozempic-global-growth-industry

[26] U.S. Attorney's Office, Southern District of New York. (2024) *U.S. Attorney announces charges against 18 defendants in scheme to manufacture and distribute millions of deadly counterfeit pharmaceuticals through fake online pharmacies*. Available at: https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-18-defendants-scheme-manufacture-and-distribute

[27] U.S. Attorney's Office, Western District of Washington, 2025. *Two brothers from India arraigned on indictment for selling counterfeit cancer drugs and adulterated medications*, U.S. Department of Justice [online]. Available at: https://www.justice.gov/usao-wdwa/pr/two-brothers-india-arraigned-indictment-selling-counterfeit-cancer-drugs-and

[28] U.S. Department of Justice, 2024. *Foreign national charged for selling counterfeit cancer drugs* [online] 25 July. Available at: https://www.justice.gov/archives/opa/pr/foreign-national-charged-selling-counterfeit-cancer-drugs

[29] Information Technology & Innovation Foundation (2025). *How Chinese Online Marketplaces Fuel Counterfeits*. Available at: https://itif.org/publications/2025/08/20/how-chinese-online-marketplaces-fuel-counterfeits/.

[30] The White House. (2023). *FACT SHEET: Biden-Harris Administration Continues Progress on Fight Against Global Illicit Drug Trafficking*. Available at: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/16/fact-sheet-biden-harris-administration-continues-progress-on-fight-against-global-illicit-drug-trafficking/

[31] The White House. (2025). *Fact Sheet: President Donald J. Trump Imposes Tariffs on Imports from Canada, Mexico, and China*. Available at: https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-imposes-tariffs-on-imports-from-canada-mexico-and-china/

[32] Clemens, E. (2025). *How Chinese Online Marketplaces Fuel Counterfeits*. Information Technology and Innovation Foundation. Available at: https://itif.org/publications/2025/08/20/how-chinese-online-marketplaces-fuel-counterfeits/

December 10, 2025

The Honorable Brett Guthrie
Chairman
The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

RE: H.R. 6292 – "Don't Sell Kids' Data Act"

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky,

We are writing on behalf of the Major County Sheriffs of America (MCSA) and the Association of State Criminal Investigative Agencies (ASCIA) to express concerns about the challenges H.R. 6292, the "Don't Sell Kids' Data Act," would potentially create for criminal investigations and child safety as currently written.

MCSA and ASCIA strongly support strengthening minors' data privacy. We appreciate the Committee's leadership on this issue, and we share your commitment to protecting children from online child exploitation, trafficking, abuse, and other harms. But as introduced, certain provisions in H.R. 6292 could inadvertently eliminate critical evidence, shield offenders, and impede urgent efforts to identify and rescue victimized children.

Our goal is not to oppose the bill, but to work with you to refine it so that it advances privacy protections while preserving the tools necessary to safeguard vulnerable children.

The types of investigations that could be impacted include Internet Crimes Against Children (ICAC) child exploitation cases, trafficking investigations, missing and abducted child response, cybercrime attribution involving juvenile victims or offenders, and homicides or other violent crimes where minors are victims, witnesses, or suspects.

Below are specific language concerns.

- **§2(a)(1)(A): Prohibition on maintaining minors' data**
  This could prevent detection of identity theft victimization of minors, which currently relies on data maintained by credit reporting companies and other data brokers.
- **§2(b)(2): Mandatory deletion within 10 days**
  Without an explicit requirement to preserve records when served with lawful process, a data broker could be forced to destroy evidence needed to identify child victims or offenders.
- **§2(b)(1)(B)(iii): Deletion request by an "agent"**
  The bill allows anyone claiming to be an agent of a minor to demand deletion – without verification. Individuals grooming, exploiting, or abducting a child could compel the destruction of evidence.
- **§2(g)(3): Potential reclassification of common platforms as data brokers**
  The current language could – in an unintended manner – classify platforms providing direct-to-consumer services (e.g., Facebook, Instagram, MeetMe) as data brokers, especially if the platform obtains data from other sources including when done so in a good faith effort to comply with existing federal law. This could potentially create conflicts with COPPA and other existing federal laws and disrupt the ability of platforms to assist in child safety investigations.
- **Broad prohibitions on collection, use, and transfer of minors' data**
  As written, the bill would block legitimate, life-saving uses - such as missing child recovery analytics, suicide-risk detection, and threat assessment research used by law enforcement and child protection specialists.

Below are some real-world investigative and minor victimization risk examples under the current bill language:

- **Identity theft victims could go undetected for years.**
  Credit reporting companies routinely maintain files that help parents and law enforcement identify when a minor's Social Security Number is being used fraudulently. This bill could prevent that entirely.
- **Law enforcement could lose the ability to identify children in child sexual abuse material (CSAM) or ongoing exploitation.**

Investigators regularly use facial recognition and other commercial data to identify "unknown minor" victims and stop active abuse. The bill would eliminate these tools, directly reducing the ability to rescue children in real time.

We respectfully request the opportunity to work with you to refine the legislative text so that privacy protections are strengthened without compromising child safety or criminal investigations. Our organizations stand ready to provide technical assistance and proposed language to achieve these shared goals.

We are also reviewing other bills on the December 11 markup agenda and would value the opportunity to discuss the law enforcement perspective with you.

Thank you for considering our views and we look forward to working with you.

Sincerely,

Louis Grever
Executive Director
Association of State Criminal Investigative Agencies (ASCIA)

Megan Noland
Executive Director
Major County Sheriffs of America (MCSA)

December 10, 2025

RE: Vote "No" on The Kids Online Safety Act, The App Store Accountability Act, the SCREEN Act, Sammy's Law, COPPA 2.0 and Other Bills That Threaten Free Speech, Privacy and/or Preemption

Dear Members of House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade,

The American Civil Liberties Union would like to thank the Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade for working to protect children online – this effort has never been more important. However, that protection cannot come at the expense of the First Amendment rights promised in our nation's constitution, at the risk of user privacy or at the expense of allowing states to protect consumers.

We advise subcommittee members to vote "No" on any bill that requires users to verify their ages before accessing online content. The ACLU has long been vocal about its opposition to age verification mechanisms because of their imposition on the First Amendment rights and privacy of internet users. Most methods of age verification require data collection (usually government identification or biometrics) that is vulnerable to indefinite storage and misuse by companies. Moreover, any form of age verification runs the risk of shutting individuals who are unable or unwilling to verify their ages out of First Amendment protected online spaces.

We also advise Members to closely evaluate the constitutionality of any bill that would allow the government to censor material that it deems harmful for children – as most content (with narrow exceptions) is protected by the First Amendment regardless of a users' age. Finally, we urge members to vote "No" on any legislation that would preempt states from protecting consumers. Specifically, we urge "No" votes on the following bills:

Vote No on HR 1623, the SCREEN Act, introduced by Rep. Miller

The SCREEN Act would require covered platforms who "make available" information deemed inappropriate or minors to verify the ages of users. As noted above, when any entity verifies a users' age they must collect data like government identification or biometrics. Once collected, this data may not only be misused by the company collecting it, but, it could also be the subject of a data breach – allowing any number of bad actors to access the personal information of users.

Moreover, if adults cannot successful verify their ages, these requirements will prevent adults from accessing First Amendment protected online spaces. This is particularly likely if the verification mechanism requires users to submit valid government identification to verify their age. About 21 million adult U.S. citizens lack a drivers' license, and another 28.6 million lack identification with their current name or address.[1] Additionally, facial identification systems are

[1] Jillian Andres Rothschild, etc al. *Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers and Knowledge*, University of Maryland Center for Democracy and Engagement (January 2024),

not universally reliable – often struggling to verify the ages of disabled individuals (particularly those whose faces are impacted by their disability), those with "young faces," or individuals from communities of color.[2] Age verification also would prevent adults who lose their IDs or who face a technological issue from accessing online spaces.

Requiring age verification also impermissibly burdens the First Amendment right to anonymity online. Many individuals will forgo accessing sensitive, personal, or stigmatized content (even when it is First Amendment protected) if they need to hand over identifying information before accessing it. For many, the risk that an unwanted party learn their browsing history is simply too large a risk. And under the First Amendment – it doesn't matter whether the use of anonymity is "motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible" – the ability to be anonymous is still protected.[3]

Vote NO on HR 3149, the App Store Accountability Act

The App Store Accountability Act would require app stores to verify the ages of all users before that user can download or use apps. Age verification through app stores poses the same risks to privacy and speech as detailed above. Moreover, it is a particularly ineffective solution because it's so easy to get around. Youth could use their parents' devices or a web browser to access prohibited apps.

Vote NO on The Kids Online Safety Act

The Kids Online Safety Act (KOSA) would not only implicitly require age verification because it sets different rules for how apps and websites need to treat children and adults – but it also would lead platforms to take down First Amendment protected information – including information which is actually helpful to children.

While we appreciate attempts to resolve our concerns that previous versions of this bill would lead to censorship, the revised version of this legislation will nonetheless lead to many of the same harms as previous versions. Whereas previous versions required platforms to regulate design features leading to certain harms, this new version simply requires platforms to implement "reasonable policies" that would prevent harms to minors. However, absent any guidance, we believe that platforms will do what they would have done under previous versions of the bill – remove any content that could conceivably cause a harm regardless of its constitutional protection.

Because content moderation tools are unable to differentiate between different types of content using similar keywords, platforms are also likely to inadvertently remove a significant amount of content that is actually helpful to youths. For example, in attempting to prevent

---

https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%202023%20survey%20Key%20Results%20Jan%202024%20%281%29.pdf.

[2] Rindala Alajaji, *10 (not so) Hidden Dangers of Age Verification,* Electronic Frontier Foundation (December 8, 2020), https://www.eff.org/deeplinks/2025/12/10-not-so-hidden-dangers-age-verification.

[3] *McIntyre v. Ohio Elections Commission,* 514 U.S. 334, 341–42 (1995).

physical harm, platforms would likely try remove content advocating for suicide. But, because content moderation tools may simply look for keywords, they could also remove content allowing youths to find life-saving mental health resources.

Vote "No" on HR 2657, Sammy's Law

Sammy's Law would help parents monitor kids' online activity on social media through third party software. This legislation opens children and teens' online lives to monitoring by their parents and guardians, without consideration of the privacy rights of the child or (especially) teen. This is particularly concerning for teens in unsafe situations at home or LGBGTQ+ youth who have not yet shared their sexuality/gender identity with their family. It would also lead to increased data collection about youths.

Vote NO on HR 6291, the Children and Teens' Online Privacy Protection Act

The Children and Teens' Online Privacy Protection Act ("COPPA 2.0") makes important improvements to the existing COPPA statute, including limiting platforms' use of children's data and giving teens robust privacy rights. COPPA 2.0 also seeks to avoid burdening families with repeated collection of children's data for age verification. Unfortunately, COPPA 2.0 vastly expands preemption of state laws, attacking "any law, rule, regulation, requirement, standard, or other provision . . . that relates to the provisions" of the bill. This language is sweeping preempting not only children's privacy laws, but also state laws regarding consumer privacy, consumer protection and tort claims. Instead, COPPA's existing "conflict" preemption should be maintained, and COPPA 2.0 should not advance to the House floor with its current approach to preemption.

It is imperative that free speech, privacy and states' ability to protect consumers are not jeopardized by efforts to protect youths online. We look forward to working with you on other ways to protect kids' online safety. If you have any questions about these bills, please do not hesitate to reach out to jleventoff@aclu.org.

Sincerely,

Christopher Anders
Director, Democracy & Technology
American Civil Liberties Union

Jenna Leventoff
Senior Policy Counsel
American Civil Liberties Union

CENTER FOR DEMOCRACY & TECHNOLOGY

Hon. Brett Guthrie
Chair
House Committee on Energy and Commerce
2161 Rayburn House Office Building
Washington, DC 20515

Hon. Frank Pallone
Ranking Member
House Energy & Commerce Committee
2107 Rayburn House Office Building
Washington, DC 20515

Hon. Gus Bilirakis
Chair
House Committee on Energy and Commerce,
Subcommittee on Commerce,
Manufacturing and Trade
2306 Rayburn House Office Building
Washington, DC 20515

Hon. Jan Schakowsky
Ranking Member
House Energy and Commerce Committee,
Subcommittee on Commerce,
Manufacturing, and Trade
2408 Rayburn House Office Building
Washington, DC 20515

Dear Chair Guthrie, Chair Bilirakis, Ranking Member Pallone, and Ranking Member Schakowsky,

Thank you for convening the hearing entitled "Legislative Solutions to Protect Children and Teens Online." Focusing on empowering children as they navigate their online lives is a critical topic. The Center for Democracy & Technology writes to reinforce the testimony offered at the hearing and provide additional details related to our concerns with some of the legislation the subcommittee is considering.[1]

State Law Preemption

States have long played a critical role in protecting against harms to children. State level protections specifically applicable to children online run the gamut from restrictions on access to social media platforms or constitutional content (laws that raise significant constitutional concerns), to the creation of educational programs to help children learn to navigate the online world, to meaningful privacy protections that mitigate the monetization of children's online activities. Generally applicable laws also provide significant protections for children. These laws might include state unfair and deceptive trade practices statutes, tort and common law claims, civil rights statutes, educational protections, criminal laws, and comprehensive privacy statutes that contain heightened standards for children's data. Congress should be very careful when seeking to displace that authority and these existing laws.

In their current forms, H.R. 6291, Children and Teens' Online Privacy Protection Act, ("COPPA 2.0"), H.R. 6484, Kids Online Safety Act ("KOSA"), and many of the other bills scheduled for markup would preempt "any law, rule, regulation, requirement, standard, or other provision having the force and

[1] These issues are not fully representative of CDT's position on all of the bills being marked up, but represent some of CDT's most immediate concerns. CDT supports some of the other bills under consideration. We look forward to working with you to share more detailed feedback in the coming weeks.

effect of law that relates to the provisions of this Act." We are concerned that the "relates to" standard will sweep too broadly and preempt much of the state-level legislation that either specifically protects children or provides significant protections to children online, even where COPPA 2.0 or KOSA do not specifically cover the activities addressed by the state law or the state law provides better protections for children. In general, in legislation that provides protections to children, Congress has chosen to narrowly preempt state level efforts, if it chose to preempt them at all. The preemption standard contained in many of the bills before the Committee represents a problematic break with that precedent that could undermine protections in place for children across the country. At the very least, with such broad preemption language, every state-level child-related enforcement will be met with a preemption claim, causing significant wasteful and abusive litigation that we should not hoist onto states.

Children should not wind up with fewer protections after Congress acts. We urge the Committee not to preempt state laws related to children other than where there is an actual conflict between federal and state law.

Sammy's Law

Sammy's Law, H.R. 2657, is a well-intentioned effort to provide parents and children with access to tools intended to help keep children safe, a goal that we support. However, as currently written, the bill threatens to do more harm than good by exposing children's sensitive data to third-party actors with insufficient privacy safeguards and enabling extensive 24/7 monitoring of children's private online activity.

The bill requires large social media platforms to share vast amounts of their young users' data, including the contents of their communications, with third-party providers designated by either parents or their children. It also permits third-party providers once designated to manage the online interactions, content, and account settings of children on large social media platforms on the same terms as the child. Monitoring content and conduct through these third-party tools is likely to result in a chilling effect, where teens change what they say and do because they know they are being surveilled. Indeed CDT research has shown that monitoring technologies often lead to children changing their behaviors online.[2] A national survey commissioned by CDT in 2021 on the experiences of students being monitored on school devices found that almost 60% of students reported that they held back from saying what they truly meant online because they were being monitored.[3]

[2] Dhanaraj Thakur, Hugh Grant-Chapman, & Elizabeth Laird, *Beyond the Screen: Parents' Experiences with Student Activity Monitoring in K-12 Schools*, Ctr. for Democracy & Tech. (Jul. 2023), https://cdt.org/wp-content/uploads/2023/07/2023-07-28-CDT-Civic-Tech-impacts-of-student-surveillance-report-final.pdf.
[3] Hugh Grant-Chapman, Elizabeth Laird, & Cody Venzke, *Student Activity Monitoring Software: Research Insights and Recommendations*, Ctr. for Democracy & Tech. (Sept. 2021), https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/.

Additionally, Sammy's Law would allow these third-party monitoring services to share data about teenagers' online behaviors in a number of circumstances. For example, they may share data proactively with parents or with the child whose data is at issue when there is "foreseeable risk" to them experiencing a set of harms, ranging from anxiety to eating disorders to academic dishonesty. To monitor for this list of harms, many of which are ambiguous and raise significant privacy concerns, monitoring services are likely to use automated monitoring and detection tools to parse conversations, all of which are error-prone, potentially leading to erroneous flagging of innocent interactions. Moreover, third-party monitoring services will be required to keep data related to disclosure made to parents or children potentially indefinitely, at least until the parent or child request its deletion, creating risky "honeypots" of children's data that may be exploited by bad actors.

In all, Sammy's Law, as currently drafted, risks chilling children's speech on essential online services and contains insufficient privacy and data minimization protections for the particularly sensitive and large amounts of data at issue. We urge the Committee to consider more tailored ways to encourage and enable the use of tools to help keep kids safe.

Safe Messaging for Kids Act

The Safe Messaging for Kids Act, H.R. 6257, is also a well-intentioned effort to provide tools to parents and kids, but also presents significant privacy and speech-related concerns. The bill would ban ephemeral messaging for minors. It would prohibit minors under 13 from accessing direct message features without parental consent. It would further allow parents to control direct messaging with verifiable parental consent, notify parents about unapproved contacts, allow the parents to approve or deny the requests, view and manage contacts, and disable direct messaging features.

In addition to raising concerns related to incentivizing the use of age verification technologies without sufficient safeguards and to limiting access to constitutionally protected speech,[4] the bill also would create privacy, safety, and practical concerns. Ephemeral messaging, or disappearing messages, is a feature some services offer that may have concerning uses, but may also serve a privacy-protective function that children should be able to access. For example, if young people choose to engage in intimate messaging with one another, ephemeral messaging could reduce the risk of misuse of those messages for purposes that one of the parties did not consent to. Banning ephemeral messaging for teens would in fact likely exacerbate the threats of nonconsensual intimate images, sextortion and distribution of child sexual abuse material. Research has shown that ephemeral messages and content allows young people to explore and test out aspects of their identity, which is a healthy and typical

[4] Aliya Bhatia & Nick Doty, *Mitigating Risk to Rights with Age Verification: Privacy-Preserving Guardrails that Should Accompany Deployments of Age Verification Approaches*, Ctr. for Democracy & Tech. (Oct. 10, 2025), https://cdt.org/insights/mitigating-risk-to-rights-with-age-verification-privacy-preserving-guardrails-that-should-accompany-deployments-of-age-verification-approaches/.

behavior.[5] Ephemeral messaging can also be a helpful tool for domestic violence victims to maintain privacy and safety. Banning the use of ephemeral messaging for kids may, therefore, unintentionally expose vulnerable users to additional privacy and safety risks in the service of protecting them from harmful or abusive interactions.

Additionally, when CDT spoke with parents and teens about the use of parental tools to manage their safety, both parents and teens expressed skepticism of parents approving direct message contacts.[6] Parents viewed the need to review each potential contact within services as burdensome, preferring higher level approvals and involvement; while their teens viewed control over who they could message as too invasive, and impractical given the active social lives youth navigate. A more effective approach would be to incentivize the creation of tools that help both parents and teens manage their data and ensure that teens and children have effective mechanisms to report problematic behavior and block unwanted contacts.[7]

App Store Accountability Act

The App Store Accountability Act, H.R. 3149, also raises significant privacy, free expression, and practical concerns. The bill would require app stores to verify the age categories of their users, using commercially available methods. It would then require parental consent for minors to download any app and parental consent for any significant changes app developers made to their terms of services.

Because the App Store Accountability Act requires age assurance for everyone to access constitutionally protected speech, it is likely to face significant constitutional challenges. It further insufficiently protects the privacy of users who will now need to provide additional data to verify their age categories to app stores. At a minimum, the App Store Accountability Act should require that any age assurance method used to comply with the bill be proportional and narrowly tailored; reliant on high quality sources of data to ensure context-dependent accurate verification; nondiscriminatory and uniformly accessible to all; private and secure, meaning unlinkable, data-minimized, retention-limited, purpose-restricted, securely-implemented, and not shared or distributed; transparent; and accountable and remediable.[8]

---

[5] Michal Luria & Nate Foulds *Hashtag-forget: using social media ephemerality to support evolving identities,* In Extended abstracts of the 2021 CHI conference on human factors in computing systems, at 1-5 (May 2021), https://dl.acm.org/doi/abs/10.1145/3411763.3451734

[6] Michal Luria & Aliya Bhatia, *What Kids and Parents Want: Policy Insights for Social Media Safety Features*, Ctr. for Democracy & Tech. (2025), https://cdt.org/insights/what-kids-and-parents-want-policy-insights-for-social-media-safety-features/.

[7] https://cdt.org/insights/more-tools-more-control-lessons-from-young-users-on-handling-unwanted-messages-online/

[8] Aliya Bhatia & Nick Doty, *Mitigating Risk to Rights with Age Verification: Privacy-Preserving Guardrails that Should Accompany Deployments of Age Verification Approaches*, Ctr. for Democracy & Tech. (Oct. 10, 2025), https://cdt.org/insights/mitigating-risk-to-rights-with-age-verification-privacy-preserving-guardrails-that-should-accompany-deployments-of-age-verification-approaches/.

Congress should also consider which app developers should be permitted to have access to age category data and include clear restrictions preventing them from using that data for any other purpose other than assigning the correct age category to a user. Not all apps on a phone need to know a user's age or age category. For instance, a compass application or flashlight function does not need to know a user's age. Some apps are also appropriate for all ages and do not need age category data. Minimizing the number of actors with access to personal information would mitigate privacy risks. The App Store Accountability Act also requires app developers to obtain and re-obtain verifiable parental consent too often and in ways that may be duplicative of other regulatory requirements, risking fatigue on the part of parents.

The Parents Over Platforms Act, H.R. 6333, represents a preferable approach, basing its structure mainly on voluntary age signaling. Age signaling is a more privacy-preserving approach and will create less invasive data collection and consent requirements. We urge the Committee to focus on improving the Parents Over Platforms Act.

Conclusion

Thank you for considering CDT's perspective. We look forward to working with the Committee as it further considers legislation to protect children online.

Kids Online Safety Act (KOSA)
House Bill (H.R. 6484) and AINS Memo

Bill Summary: The strong Senate version of KOSA (S.1748), reintroduced this year with support from 70 bipartisan co-sponsors, requires tech companies to design their platforms in ways that put children's and teens' health and well-being ahead of engagement metrics and profits. However, the newly introduced House version (H.R. 6484 and its AINS) would be comparatively weaker and tailored to the wishes of tech companies, exposing kids and teens to online harms. Several key changes are needed to strengthen the House bill and better protect young people.

Common Sense Media Calls for 3 Urgent Changes to the House KOSA Bill:

- **Restore the duty of care in the House Version of KOSA.** The robust duty of care in the Senate bill would finally hold tech companies accountable for the harms they knew—or reasonably should have known—their design choices would cause. This standard only targets dangerous product design, not the content on their platforms.
- **Reinstate the Senate's stronger knowledge standard**—"actual knowledge or knowledge fairly implied on the basis of objective circumstances." The House's current approach represents a step backward, even compared with the already weak standard this committee approved in the 118th Congress.
- **Remove or significantly revise the preemption language**. As written, the House bill risks wiping out existing child-protection laws in red and blue states alike. Preemption may be appropriate when it creates a protective floor for all children, but the House bill instead establishes a restrictive ceiling that prevents states from enacting stronger measures. As currently drafted, it prioritizes the interests of the tech industry over the safety of children.

Even with the changes outlined above, the House version of KOSA would still require several critical additional changes, including:

- **Restore the broader, more comprehensive list of harms from the Senate version**, which offers far stronger protections than the limited harms identified in the House bill.
- **Broaden the definition of "design feature,"** which is drawn too narrowly in the House bill and undermines its effectiveness in the future by using "any" rather than "such as."
- **Reinstate the Senate bill's data-privacy and protections from "personalized design features,"** including ensuring that "personalized design features" are turned off by default for young users, with the ability to opt in.
- **Close the substantial loophole in Section 3(b) of the House bill**, which allows companies to evade responsibility by claiming that addressing harms was not "technically feasible."
- **Remove the limitation on state action, Section 5(3)(B),** while federal action is pending. There absolutely is no reason to handicap a state's power and role in protecting their residents.

For further recommended revisions, please reach out to Holly Grosshans, Senior Counsel for Tech Policy, at hgrosshans@commonsense.org.

Why should the Committee strengthen H.R. 6484: Our youth are facing a mental health crisis, and evidence shows that social media platforms contribute to it. We need Congress to force companies to change design features that maximize engagement, often at the cost of children' s well-being. The strong Senate version of KOSA shifts the responsibility to platforms while also giving minors and parents more meaningful controls and continued access to the internet.

It is unsurprising that NetChoice, the leading trade association for major technology companies, publicly supported the package of "kids' safety bills" unveiled at last week's subcommittee hearing. The House's diluted version of KOSA removes the duty of care entirely—the very mechanism that would meaningfully hold platforms accountable and require them to prioritize minors' well-being over profit incentives.

Only weeks ago, newly unsealed documents from litigation involving Meta, TikTok, Snap, and YouTube offered an unprecedented look into how these companies both recognized and intentionally designed features that are addictive and harmful to young users. **These documents demonstrate that none of this was accidental.**

Key revelations from the documents include:

- Meta's own internal planning documents labeled child safety as a "non-goal." Employees went even further, describing the company's products as "digital cocaine," admitting they were "creating a world of addicted monsters," and acknowledging that the platforms were "making people's health deteriorate slowly over time."
- TikTok documents show differences between the Chinese version of TikTok (Douyin) and the U.S. version, stating: "We give spinach to kids in China and opium to kids in America."
- The CEO of Snap internally referred to Streaks as "toxic behavior" that the company shouldn't reinforce. Yet, in 2023, Snap launched a paid feature to "restore" lost streaks for a fee, monetizing the very anxiety they created.
- YouTube research had shown that teens were more susceptible to online harms because "changes in brain development predisposes young teens to act more impulsively, show a greater tendency towards risk taking, and lead to an increased interest in riskier content."

The disclosures in these documents build on years of whistleblower evidence that first exposed the gap between companies' public assurances and internal reality, painting a deeply troubling picture where platforms knowingly prioritize profits over child safety.

These companies were not only aware of the harms but documented them and engineered addictive systems, all while misleading parents, lawmakers, and the public at large.

The evidence is clear - **we need accountability and meaningful action to protect children online now.**

Dec 8, 2025

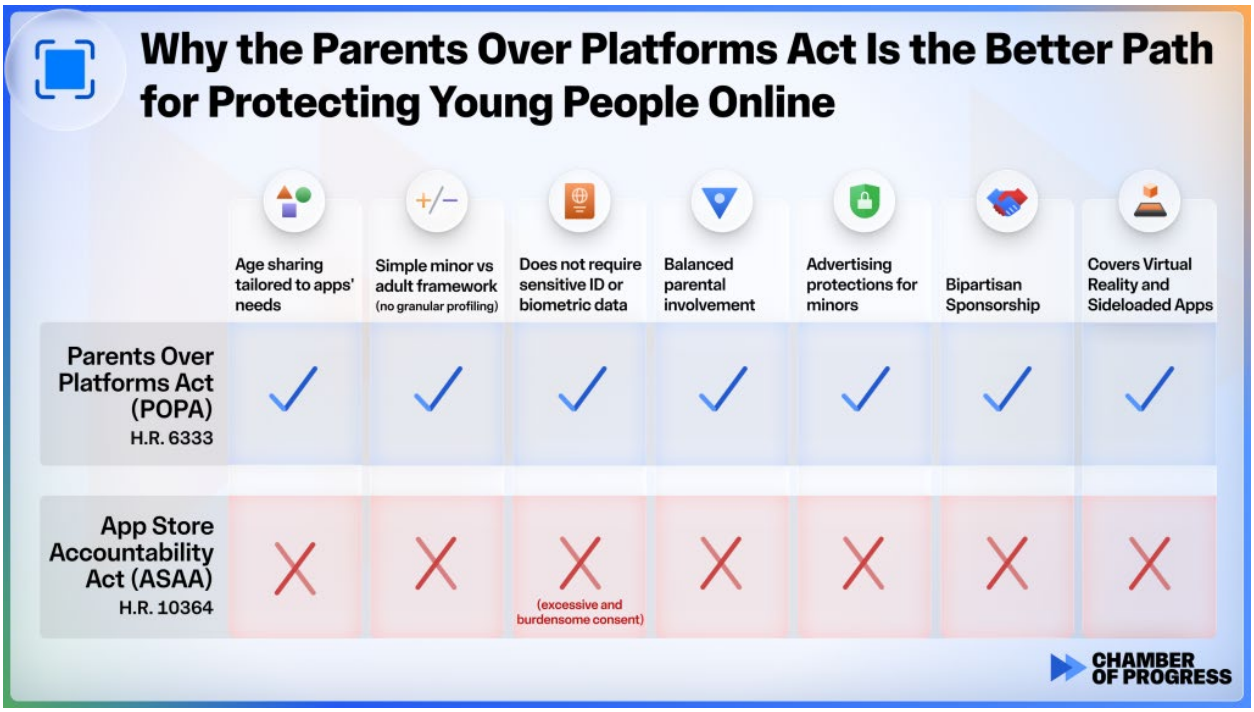
Why the Parents Over Platforms Act Is the Better Path for Protecting Young People Online


Aden Hizkias

As lawmakers consider new ways to protect young people online, **two proposals have emerged that tackle a similar challenge from very different angles: the bipartisan-sponsored Parents Over Platforms Act (POPA) and the App Store Accountability Act (ASAA)**.

Both bills aim to ensure that minors have safer experiences with mobile apps, but they differ sharply in how they approach age assurance, parental involvement, and data privacy.

A close look at both bills shows that POPA offers a more balanced, privacy-protective, and practical framework for families and developers alike. The chart below highlights the core distinctions.



POPA Lets Safety and Privacy Coexist

POPA creates a straightforward system that gives app stores the ability to send developers a simple signal about whether a user is a minor or an adult. This allows apps to turn on

safety features, limit adult-only content, and block personalized ads to minors without collecting extra personal information or requiring intrusive age checks.

In this framework, when a thirteen-year-old sets up an account in the app store, the store asks for age during setup and records that the user is a minor. Later, if that child wants to download Instagram, the app store sends Instagram a minor signal so the app can immediately apply youth protections. If the child downloads an app that does not offer different experiences for minors and adults, POPA does not require any age signal at all.

POPA's design delivers:

- Minimal data collection and strict limits on how age information is used.
- Practical, easy-to-understand tools for parents.
- Protections that prevent large platforms from using compliance data to their advantage.

In practice, POPA means safer, simpler, and more privacy-respecting online experiences for youth while avoiding unnecessary burdens for families, users, and developers.

ASAA Creates a Complex System That Adds Burdens for Families

In contrast, the App Store Accountability Act creates a far more expansive regulatory structure. It requires app stores to determine a user's exact age category and to obtain verifiable parental consent before a minor downloads an app, makes an in-app purchase, or uses an app after certain updates.

Meeting ASAA's accuracy and verification standards would likely **require far more intrusive methods of confirming identity and age, potentially including government ID checks, facial matching tools, or other biometric or third-party verification systems,** since app stores must be able to prove both a user's precise age group and that the consenting adult is the legitimate parent or guardian.

In this framework, if a thirteen-year-old wants to download a social media app, the app store must first verify that the user fits into the teenager category using a method designed to ensure accuracy. The download cannot proceed until the parent receives a notice, reviews a required parental consent disclosure, and provides verifiable parental consent through a formal process tied to a parental account.

If the teen later tries to buy an in-app add-on, the app store must stop the purchase and seek parental approval again. If the app issues a significant update that changes its data practices or features, the app store must notify the parent and obtain a new round of consent before the teen can resume using the app. Each of these steps creates additional

pauses, notifications, and verification loops for families who may be trying to complete otherwise simple interactions.

ASAA's structure introduces:

- Extensive age verification requirements that increase data collection.
- Significant parental burden due to repeated consent requirements.
- Exposure to state-by-state enforcement actions, increasing compliance risk.

ASAA aims to improve parental oversight but may unintentionally encourage overcollection of children's data, overwhelm families, and impose heavy operational burdens that do little to enhance safety.

ASAA Leaves Major Gaps That Put Kids at Risk

ASAA is so narrowly drawn that it leaves major gaps that could leave young people vulnerable. ASAA only applies to app stores serving phones and tablets, and only when a minor downloads an app through those stores.

This means that whole categories fall outside of the bill's coverage: game consoles and VR headsets aren't covered, preloaded system apps don't trigger obligations, and sideloaded apps evade the law entirely. ASAA also ignores the url-accessible or web versions of covered applications, potentially allowing users to circumvent the law by accessing platforms and services via a browser.

POPA takes a broader approach that closes these loopholes. It covers connected devices including phones, tablets, consoles, and VR headsets, and puts age-assurance duties on both app stores and developers, and includes web versions of covered apps.

Those responsibilities follow the product wherever a teen uses it. While ASAA's narrow scope and carveouts make it possible for companies to route around its protections, POPA regulates the real ecosystem comprehensively.

Why POPA Offers the Stronger, More Sustainable Path Forward

POPA succeeds because it focuses on what truly matters: **protecting young people while keeping privacy, usability, and innovation intact.** It creates a system that works for families and does not burden developers or app stores with unnecessary complexity.

POPA delivers a better approach because:

- It protects minors without relying on intrusive identity checks or sensitive data collection.

- It ensures age information stays minimal, controlled, and purpose-limited.
- It gives parents meaningful oversight without constant approval prompts.
- It offers developers clear, practical requirements that enhance safety.

As lawmakers explore new ways to make digital spaces safer for young people, it is essential to prioritize solutions that increase protection without creating new privacy risks or daily obstacles for families. POPA meets that need by strengthening safeguards while keeping the app ecosystem open, functional, and privacy-respecting. It offers a balanced, modern framework that supports parents and gives children safer online experiences without the high costs or complexity of alternative proposals.

December 11, 2025

The Honorable Gus Bilirakis
United State House of Representatives
Washington, DC 20510

The Honorable Jan Schakowsky
United State House of Representatives
Washington, DC 20510

The Honorable Brett Guthrie
United State House of Representatives
Washington, DC 20510

The Honorable Frank Pallone
United State House of Representatives
Washington, DC 20510

Re: House Package of 18 Bills to Protect Children and Teens Online

Dear Representative Bilirakis, Representative Schakowsky, Representative Guthrie, Representative Pallone, and Members of the Subcommittee on Commerce, Manufacturing, and Trade:

The undersigned education and parent associations write today to provide feedback on the package of 18 bills to protect children and teens online that was introduced on November 25, 2025. We appreciate your continued leadership on the important work of increasing online privacy and data security protections for our nation's children and teens, and we look forward to continuing to work with you as the package progresses.

Our organizations prioritize the privacy and safety of student data, and we strongly support updates and revisions to child privacy protections. Minors are uniquely vulnerable to harms online and deserve heightened protections to keep them safe. While we commend the Committee's goals to pass legislation modernizing protections for children online, we are deeply concerned that the package may unintentionally limit schools' ability to effectively establish privacy-protective safeguards for education technology (edtech).

We are particularly concerned that the broad preemption language added to the Children and Teens' Online Privacy Protection Act (COPPA 2.0) will invalidate state laws regulating edtech vendors who receive student data when providing services for schools, such as California's Student Online Personal Information Protection Act (SOPIPA) and similar laws passed in twenty-three other states. SOPIPA-style laws establish comprehensive requirements for edtech vendors that supplement the responsibilities of educational agencies or institutions under the Family Educational Rights and Privacy Act (FERPA). These protections are critical to ensuring student privacy is safeguarded when it is shared externally with third party technology companies.

The Kids Online Safety Act (KOSA) also has similarly broad preemption language. We are concerned that this language would significantly limit state child privacy laws that benefit students. These state laws are crucial to ensuring that young people retain strong online privacy protections.

We are also concerned that several of these bills may have unintended consequences for schools utilizing collaborative and gamified edtech platforms to personalize and enhance learning. For example:

- The Algorithmic Choice and Transparency Act requires online platforms to give users an option to easily switch between personalized recommendation systems and input-transparent algorithms, potentially requiring edtech providers to offer students non-adaptive versions of adaptive learning products. The bill should not allow students to unilaterally decide to circumvent using an adaptive learning product that their school has carefully vetted for privacy and security safeguards and contracted to use to improve learning.
- The Safer Guarding of Adolescents from Malicious Interactions on Network Games (GAMING) Act requires online video game providers to limit minors' ability to communicate with other users (including adults) by default, and says that parents are the only one who can disable the safeguards. This may unintentionally restrict students' ability to communicate with teachers and their classmates on gamified edtech platforms used in class.

Thank you for considering our views and it is our hope that we can address these issues of great importance to education stakeholders. We look forward to continuing to work with you to fine-tune the provisions in these bills to ensure that enhanced privacy protections for children online do not have unintended consequences for our nation's schools.

Sincerely,

AASA, The School Superintendents Association

Association of Educational Service Agencies

Association of School Business Officials International (ASBO)

Council of the Great City Schools

National Association for Pupil Transportation

National Association of Elementary School Principals

National Association of Secondary School Principals

Public Interest Privacy Center