1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

September 30, 2024

Via Electronic Submission

Office of the New York State Attorney General
The Capitol
Albany, NY 12224-0341
ChildDataProtection@ag.ny.gov

RE: Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 899-ee *et seq*.

Dear Office of the Attorney General,

Thank you for your ongoing work and the opportunity to comment regarding the implementation of the New York Child Data Protection Act. The Future of Privacy Forum ("FPF") is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.[1]

The New York Child Data Protection Act ("NYCDPA" or "the Act") creates heightened protections for youth online, going beyond the existing federal protections under the Children's Online Privacy Protection Act. We note that New York does not currently have a broad, baseline privacy law that applies to *all* consumers. Therefore, the forthcoming Office of the Attorney General ("OAG") regulations should engage with certain core privacy issues such as which types of data processing are necessary, what is or is not included in the definition of "personal data", and whether data sharing for research is permitted under the Act. Furthermore, given that as of this comment 20 states have passed some form of baseline consumer privacy law,[2] the OAG should consider emerging trends in U.S. privacy law in developing regulations to support robust, interoperable privacy rights and protections for young people and lay a foundation for the development for subsequent, generally applicable privacy frameworks in New York. Finally, we recommend taking steps to ensure that the NYCDPA can interact with existing laws such as New York's Education Law 2-d in order to ensure that students and schools can continue to utilize data-enabled educational tools. **FPF's comments detail several areas for consideration in aligning with existing privacy laws in New York, other states, and the federal Children's Online Privacy Protection Act.**

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.
[2] See Keir Lamont, *Effective Dates of State Privacy Laws*, Future of Privacy Forum (last updated: July 25, 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Key-Dates-Chart-2024-Update.pdf.

Additionally, the Act calls for developing a new class of browser or device signals to convey messages about whether an individual is a covered minor and invoke affirmative consent rights. Enabling individuals to exercise privacy rights at scale on a default basis can ease the burdens of privacy self-management. However, the NYCDPA contemplates new technologies that pose outstanding development, standardization, and use challenges. **FPF's comments provide technical and policy considerations for the OAG to promote the privacy and utility of device signals.**

A. The OAG should look to existing sources of law, including the COPPA Rule's internal operations exception, state privacy laws, and the GDPR to provide guidance on the scope of "permissible processing" activities.

The NYCDPA prohibits an operator from processing, allowing a processor to process, or allowing a third-party operator to collect the personal data of a minor 13-17 years of age unless the minor has given ***informed consent*** or such processing or collection is ***strictly necessary*** for one of the following activities:

> (a) providing or maintaining a specific product or service requested by the covered user;
>
> (b) conducting the operator's internal business operations. For purposes of this paragraph, such internal business operations shall not include any activities related to marketing, advertising, research and development, providing products or services to third parties, or prompting covered users to use the website, online service, online application, mobile application, or connected device when it is not in use;
>
> (c) identifying and repairing technical errors that impair existing or intended functionality;
>
> (d) protecting against malicious, fraudulent, or illegal activity;
>
> (e) investigating, establishing, exercising, preparing for, or defending legal claims;
>
> (f) complying with federal, state, or local laws, rules, or regulations;
>
> (g) complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
>
> (h) detecting, responding to, or preventing security incidents or threats; or
>
> (i) protecting the vital interests of a natural person.[3]

The advanced notice of proposed rulemaking (ANPRM) asks three questions concerning permissible processing under the NYCDPA: (1) "What factors should OAG consider in defining what processing is 'strictly necessary' to be permissible without requiring specific consent?" (2) "What factors should OAG consider in determining whether bundled products or services are incorporated into the 'product or service requested by the covered user'?" and (3) "Are there examples of permissible processing pursuant to internal business operations that should be explicitly noted in OAG's regulations?"

[3] N.Y. Gen. Bus. Law § 899-ff (Consol. 2024).

The permissible processing framework in NYCDPA § 899-ff—requiring either informed consent or necessity of a specific purpose—is representative of an emerging transition in American privacy law. Historically, personal data uses were permitted unless explicitly prohibited by law, and requirements to obtain opt-in consent were more limited, such as for collecting and using sensitive data or under sectoral approaches, such as the federal Children's Online Privacy Protection Act (COPPA). The NYCDPA is one of several recently enacted U.S. state laws that embrace more substantive data minimization rules that enumerate discrete permissible processing purposes and limit the collection and use of personal data based on the purpose(s) for which data is collected and used.[4]

The NYCDPA provides that as an alternative to processing data for a "permissible purpose", an operator may collect and use personal data if they receive "informed consent" from a covered minor.[5] The OAG's rules should seek to ensure that operators do not overly rely on obtaining "informed consent" as the basis for their data collection and processing activities. Frequent or repeated requests for consent have the potential to produce "consent fatigue" for users.[6] In short, informed consent will be most effective if requests are reserved to higher-risk use cases or for secondary processing purposes unrelated to providing a service. Preserving the integrity of a meaningful informed consent standard requires guidance that is permissive enough to allow operators to confidently engage in commonplace, low- to minimal-risk business activities that are consistent with covered users' reasonable expectations. Thus, the overall success of this framework depends on how narrowly or broadly the NYCDPA's "strictly necessary" standard for using personal data for a permitted purpose is set.

FPF writes to identify several potential ambiguities and tensions in the "strictly necessary" standard and highlight relevant sources of law and guidance to which the OAG should refer in crafting rules and guidance related to factors for "strictly necessary," bundling of products or services, and internal business operations. These recommendations are intended to provide clarity that can foster consistent implementation of the NYCDPA's "permissible processing" standard across covered operators and to promote harmonization with other legal regimes, including state privacy laws and the federal COPPA Rule, where appropriate.

---

[4] *See* Jordan Francis, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, IAPP (May 22, 2024), https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation.

[5] N.Y. Gen. Bus. Law § 899-ff(3)(a) (Consol. 2024). When required in the correct circumstances, informed consent is an important source of friction that *deters* unnecessary, risky, and harmful processing or data collection. Conversely, when paired with a strong, default rule regarding the permissible purposes for processing personal data, informed consent can act as a vital release valve to *enable* processing of personal data consistent with individuals' subjective preferences.

[6] Consent fatigue is a phenomenon in which individuals are unduly burdened by constant requests for consent in the form of banners, notices, and other interfaces, resulting in diminished capacity to understand and meaningfully engage with those requests for consent. Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, Thorsten Holz, *(Un)informed Consent: Studying GDPR Consent Notices in the Field* (Oct. 2019), available at https://arxiv.org/abs/1909.02638 (describing how the "high prevalence [of consent notices] has led website visitors to become fatigued with consent mechanism").

1. *The OAG should develop high-level factors for determining whether data processing is "strictly necessary" for a permissible purpose.*

On a conceptual level, to say that a data processing activity is "strictly necessary" for any of the purposes under § 899-ff(2) implies two things—causality and limited discretion. For processing of personal data to be "necessary" for a given purpose, there must be a cause-and-effect relationship such that the processing enables, advances, or precipitates an outcome. The strength of the nexus between the processing and the desired outcome, however, turns on how much discretion is given to an operator in determining whether their data processing activities satisfy this standard. That processing must be "strictly" necessary implies a highly direct relationship between the processing and the outcome, leaving operators with a narrow ambit.

Given the novelty of this "necessity" approach, it is possible that different operators could interpret the scope of the § 899-ff(2) permissible purposes very differently, resulting in inconsistent interpretation of the law and protection of teens under the law. Building robust guidance on "strictly necessary" is necessary to minimize discrepancies across operators. OAG should consider developing high-level factors for "strictly necessary" processing that reflect the discussion of causality and limited discretion above.

2. *The OAG should develop more detailed guidance for open-ended permissible processing activities such as providing or maintaining a requested product or service, conducting internal business operations, identifying and repairing technical errors, and protecting the vital interests of a natural person.*

In addition to developing high-level factors for "strictly necessary" processing, FPF recommends that the OAG develop guidance on the meaning of "strictly necessary"—alongside illustrative examples—with respect to data collection and processing for the permissible purposes of (1) providing or maintaining a requested product or service; (2) conducting internal business operations; (3) identifying and repairing technical errors; and (4) protecting the vital interests of a natural person.[7] Because of their expansive and open-ended nature, these permissible purposes may warrant additional guidance. For example, assessing whether collection or processing is strictly necessary for complying with federal law (permissible purpose (f)) will typically be a narrower, simpler question than whether collection or processing is necessary for providing a requested product or service or protecting the vital interests of a natural person (permissible purposes (a) and (i)). Similarly, operators are likely to question whether the collection and processing of personal data for things such as internal research and product improvement are permissible under a combination of purposes (a), (b) and (c) (notwithstanding (b)'s language against relying on internal business operations to conduct research).

[7] N.Y. Gen. Bus. Law § 899-ff(2)(a), (b), (c), & (i) (Consol. 2024).

Another ambiguity with the NYCDPA's permissible processing framework is that the "internal business operations" permissible purpose explicitly precludes operators from relying on that purpose for "prompting covered users to use the website, online service, online application, mobile application, or connected device when it is not in use."[8] While the principle of limiting manipulative and intrusive design practices and overly "nagging" prompts is an important design protection for young users, there are circumstances where this principle may curtail beneficial nudges and notifications to covered teens. For example, reminders to complete homework, a language learning app reminding individuals to complete scheduled lessons, alerting a user of a potential security incident, or a service providing notice that they have received a message from a friend or family member could all be forbidden under a strict reading of the internal business operations purpose (b). Operators would benefit from guidance that lays out clear permissions for such beneficial nudges and notifications, whether that means additional guidance on the internal business operations permissible purpose or separately permitting such notifications as "providing or maintaining a specific product or service requested by the covered user" under permissible purpose (a). The OAG can proactively address these concerns through guidance to increase the likelihood of consistent practices (and protections for young users) across operators.

Another issue that the OAG should explicitly address in rulemaking is advertising. Many websites, including those directed to minors, rely on advertising for their primary business model and source of revenue to support the availability and development of accessible and age-appropriate services. Under the COPPA Rule, the internal operations exception allows operators to collect a persistent identifier (and no other personal information) to be used for the sole purpose of "serv[ing] contextual advertising on the Web site or online service or cap[ping] the frequency of advertising."[9] Many state privacy laws also restrict cross-context behavioral advertising based on third-party data to minors and teens (subject to opt-in consent) but permit less data-intensive and privacy-implicating contextual advertising or advertising based on first-party data. State privacy laws also typically explicitly permit related practices necessary for measuring the performance, attribution, and reach of an advertisement.[10] In contrast, the NYCDPA's "internal business operations" permissible purpose explicitly prohibits reliance on that exception for "any activities related to marketing[or] advertising."[11] The Act's approach could lead operators to justify advertising activities like attribution and frequency capping as being strictly necessary to provide or maintain a product or service, or it could act as a broad prohibition on a wide swath of advertising practices regardless of their impact on privacy interests. The OAG should specify whether and under what circumstances (permitted purposes or informed consent) various advertising activities shall be permitted under the NYCDPA.

[8] *Id.* (b).
[9] 16 C.F.R. § 312.5(c)(7) (2023).
[10] *E.g.*, Colo. Rev. Stat. § 6-1-1303(25)(b)(IV) (2023).
[11] N.Y. Gen. Bus. Law § 899-ff(2)(b) (Consol. 2024).

3. *Where appropriate, the OAG should look to similar "necessity" provisions in other jurisdictions.*

In crafting guidance on the NYCDPA's "strictly necessary" standard and the scope of the Act's permissible purposes bases for data processing, there are many potential sources of inspiration in emerging U.S. privacy laws. Similar language on necessity and permissible purposes appears in other U.S. state laws concerning comprehensive consumer privacy,[12] health data privacy,[13] and youth privacy.[14] On the international scale, the European Union's General Data Protection Regulation (GDPR) includes "necessary for the performance of a contract" as one of its lawful bases for processing personal data.[15] Thus there are many peer regulators in the U.S. and abroad with whom OAG could consult in developing strictly necessary standards. In particular, the OAG should consider the four laws, regulations, and regulatory guidance in developing factors for assessing when collection and processing is "strictly necessary" and when bundling of products, services, or features is impermissible:

- The Washington My Health My Data Act (WMHMDA),[16] enacted in 2023 and currently in effect, includes a similar consent-necessity framework whereby regulated entities and small businesses may not "collect any consumer health data except" (i) with individual consent for a specified purpose, or (ii) "[t]o the extent necessary to provide a product or service" requested by the consumer. The Washington State OAG has not yet provided guidance about this standard in its FAQs concerning the law.[17] Given the conceptual similarity between WMHMDA and the NYCDA's consent and necessity requirements, it could be beneficial for your office to consider any future enforcement of WMHMDA's necessity standard. In doing so, it would be important to note differences between the standards, such as "necessary" versus "strictly necessary" and the NYCDPA's specifically enumerated permissible purposes.

---

[12] Jordan Francis, *The Old Line State Does Something New on Privacy*, FPF (Apr. 23, 2024), https://fpf.org/blog/the-old-line-state-does-something-new-on-privacy (discussing Maryland's novel data minimization rules tied to "reasonably necessary" and "strictly necessary" standards).
[13] Kate Black, Felicity Slater, Jordan Wrigley & Niharika Vattikonda, *Assessing 'Necessity' under State Health Privacy Laws* (Apr. 1, 2024), https://iapp.org/news/a/assessing-necessity-under-state-health-privacy-laws (discussing "necessity" under the Washington My Health My Data Act).
[14] Bailey Sanchez, Felicity Slater & Chloe Altieri, *Connecticut Shows You Can Have It All*, FPF (June 9, 2023), https://fpf.org/blog/connecticut-shows-you-can-have-it-all (discussing youth privacy amendments to the Connecticut Data Privacy Act, which "[a]bsent consent, [prohibits] controllers . . . from processing data not reasonably necessary to provide a service").
[15] General Data Protection Regulation (GDPR), Art. 6(1)(b).
[16] H.B. 1155, 68th Leg., 2023 Reg. Sess. (Wash. 2023), https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf#page=1.
[17] Wash. State Off. Att'y Gen., Protecting Washingtonians' Personal Health Data and Privacy, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy (last visited Sept. 17, 2024) (noting that the FAQs "may be periodically updated").

- The recently enacted, but not yet effective, Maryland Online Data Privacy Act (MODPA)[18] includes data minimization and permissible purpose rules that (1) limit the collection of personal data to what is "reasonably necessary" to provide or maintain a requested product or service, and (2) limit the collection, processing, and sharing of sensitive data to what is "strictly necessary" to provide or maintain a requested product or service (subject to various Act-wide exceptions). Like with WHMDMA, there are open questions about how MODPA's necessity requirements will ultimately be interpreted and enforced, but these emerging standards could inform the OAG's understanding of when processing activities are "strictly necessary."
- The California Privacy Protection Agency, in its implementing regulations for the California Consumer Privacy Act, included a data minimization rule that ties permissible purposes to "reasonable expectations of the consumer(s) whose personal information is collected or processed."[19] The factors for determining reasonable expectations, such as the nature of the product or service being offered and the disclosures made in marketing and other materials, could be relevant for both establishing the bounds of "strictly necessary" processing and determining whether bundled products or services are incorporated into the "product or service requested by the covered user."
- Under the GDPR, controllers are prohibited from processing personal data unless they have a lawful basis for doing so. One lawful basis is where processing "is necessary for compliance with a legal obligation to which the controller is subject."[20] Determining the scope of this lawful basis has proven challenging for European regulators. For example, European data protection authorities have clashed on the question of whether a social media company may rely on that lawful basis to process personal data for the delivery of behavioral advertising, with the European Data Protection Board (EDPB) concluding that it was not appropriate in one case.[21] The EDPB's prior guidance on this lawful basis offers detailed analysis of necessity in the context of GDPR and practical advice, such as four lines of inquiry to ask in determining whether that lawful basis is appropriate:
    - What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
    - What is the exact rationale of the contract (i.e. its substance and fundamental object)?
    - What are the essential elements of the contract?
    - What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the

[18] S.B. 541, 2024 Reg. Sess., (Md. 2024), https://mgaleg.maryland.gov/2024RS/chapters_noln/Ch_455_sb0541E.pdf.
[19] Cal. Civ. Code § 1798.100 *et seq.;* Cal. Code Reg. tit. 11, § 7002.
[20] General Data Protection Regulation (GDPR), Art. 6(1)(b).
[21] *E.g.*, European Data Protection Board, Binding Decision 4/2022 on the Dispute submitted by the Irish SA on Meta Platforms Ireland Limited and Its Instagram Service (Art. 65 GDPR) (Dec. 5, 2022), https://www.edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf.

service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?[22]

The EDPB's guidance can be helpful in promulgating factors for when processing is "strictly necessary" as well as when bundled products or services are incorporated into the "product or service requested by the covered user."

- Another EU law to consider is the ePrivacy Directive, which regulates "the confidentiality of communications and the rules regarding tracking and monitoring,"[23] such as through cookies. The ePrivacy Directive requires consent for "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user," unless such storage or access is "*strictly necessary* in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."[24] The UK's Information Commissioner's Office (ICO) has provided guidance on that exception which focuses on whether the storage of, or access to, information is *essential* to provide a requested service.[25]

These laws are not one-to-one copies of the NYCDPA's consent-necessity framework, but they provide an opportunity either for the OAG to pull relevant factors and guidance to inform its own bespoke standards or to engage with the laws' relevant enforcers to benefit from their experience and to encourage harmonization across frameworks.

On the specific question of what factors the OAG should consider "in determining whether bundled products or services are incorporated into the 'product or service requested by the covered user,'" it may be helpful to consider related privacy law principles regarding the concept of "consent bundling." In order for consent for data collection and processing activities to be "specific," which is a common statutory requirement stemming from GDPR, it is important to "ensure that consent requests for significantly divergent collection and processing purposes are not inappropriately grouped into 'take-it or leave-it' offers" while also balancing the need to avoid consent fatigue.[26] The concerns underlying bundled consent are similar to those underlying bundled products or services under the NYCDPA's consent-necessity framework. Thus, factors

---

[22] European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, version 2.0 (Oct. 8, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[23] European Data Protection Supervisor, ePrivacy Directive, https://www.edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en (last visited Sept. 23, 2024).

[24] ePrivacy Directive, Art. 5(3) (emphasis added).

[25] Information Commissioner's Office, *What Are the Rules on Cookies and Similar Technologies?*, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies (last visited Sept. 23, 2024).

[26] Keir Lamont & Daniel Sturkie, Future of Privacy Forum, FPF Colorado Privacy Act pre-rulemaking comments at 8–9 (July 12, 2022), https://fpf.org/wp-content/uploads/2022/07/FPF-Colorado-Privacy-Act-Pre-Rulemaking-Comments-1.pdf.

relevant to determining when consent bundling is inappropriate—such as when a processing purpose is unrelated, unexpected, or incompatible with the core function of a product or service—could be analogized to help answer the question of when bundled products or services are incorporated into the product or service.

4. *Where appropriate, align the definition of "internal business operations" with the COPPA Rule's internal operations exception.*

The ANPRM asks for "examples of permissible processing pursuant to internal business operations that should be explicitly noted in OAG's regulations" pursuant to permissible purpose (b). Under the federal COPPA Rule, operators are not required to obtain verifiable parental consent where they are collecting "a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service."[27] Currently, the COPPA Rule defines internal operations as:

> (1) Those activities necessary to:
>
> (i) Maintain or analyze the functioning of the Web site or online service;
>
> (ii) Perform network communications;
>
> (iii) Authenticate users of, or personalize the content on, the Web site or online service;
>
> (iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;
>
> (v) Protect the security or integrity of the user, Web site, or online service;
>
> (vi) Ensure legal or regulatory compliance; or
>
> (vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4);
>
> (2) So long as The information collected for the activities listed in paragraphs (1)(i)-(vii) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.[28]

The OAG should also consider harmonizing with federal regulations on this issue, to the extent that the COPPA Rule's definition is not inconsistent with the NYCDPA's statutory text. This harmonization would support the NYCDPA's overall cohesion because COPPA and the COPPA Rule are the controlling law for covered users under the age of twelve.[29] It may be confusing for parents or disruptive to the availability of services if there are restrictions on using teenagers' data under state law that do not apply to using young childrens' data under federal law.

Beyond harmonization, the COPPA Rule's internal operations exception provides helpful policy guidance on the types of processing that allow operators to effectively offer their services to children. For example, while targeted advertising to children is a key concern of lawmakers,

---

[27] 16 C.F.R. § 312.5(c)(7) (2024).
[28] 16 C.F.R. § 312.2 (2024).
[29] N.Y. Gen. Bus. Law § 899-ff(1)(a) (Consol. 2024).

contextual advertising can be an alternative to help support a website while still limiting data collection. Another example is maintaining a website's functionality and accessibility, even if this was not specifically requested by the user. Providing examples of such business activities and guidance on when an activity falls within one of those internal business operations could make New York a leader on this issue, as it is a longstanding challenge with the COPPA Rule that there is scant guidance on interpreting the internal operations exception from the Federal Trade Commission.[30]

Overreliance on the federal internal operations exception may be complicated, however, because the Federal Trade Commission is currently considering an update to the COPPA Rule, which proposes to modify the substance of the internal operations exception.[31] Many laws and regulations, including the statutory text of the NYCDPA, future-proof their reliance on the COPPA Rule by incorporating reference to "15 U.S.C. § 6502 and its implementing regulations." Whether that approach is desirable depends on whether the OAG would prefer to prioritize harmonizing with the COPPA Rule regardless of how the rule changes, or whether the OAG would prefer to incorporate specifics from the rule.

Finally, the COPPA Rule contains a mechanism by which interested parties may file a written request for FTC approval of certain activities to be included within the scope of internal operations.[32] The OAG could consider adopting a similar process (either through formal or informal procedures) for interested parties to petition for additional clarity and guidance around the definition of internal business operations so as to account for changed circumstances, such as new business needs and changes in technology.

B. Where appropriate, align core privacy concepts with the developing state comprehensive privacy landscape.

The New York Child Data Protection Act and the SAFE For Kids Act were passed before an underlying baseline consumer privacy framework was established in New York. Without an

---

[30] For guidance on the internal operations exception, see Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* at J(5), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Sept. 23, 2024); Fed. Trade Comm'n, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business (providing detailed information on the COPPA Rule's exceptions to requiring VPC). FPF has previously recommended that the FTC issue additional guidance on the internal operations exception. Bailey Sanchez, Jim Siegl & Daniel Hales, Future of Privacy Forum, FPF Comments Re: COPPA Rule Review at 8–9, 16, 20–21 (Mar. 11, 2024), https://fpf.org/wp-content/uploads/2024/03/Final-Future-of-Privacy-Forum-COPPA-NPRM-03.11.24.pdf.

[31] Bailey Sanchez, Jim Siegl & Daniel Hales, Future of Privacy Forum, FPF Comments Re: COPPA Rule Review at 8–9, 16, 20–21 (Mar. 11, 2024), https://fpf.org/wp-content/uploads/2024/03/Final-Future-of-Privacy-Forum-COPPA-NPRM-03.11.24.pdf (providing recommendations on proposed changes to the internal operations exception).

[32] 16 C.F.R. § 312.12(b) (2024).

existing consumer privacy framework establishing generally applicable guardrails for the collection and use of personal data, these statutes must address in the first instance core privacy concepts such as the scope of "personal data". While children, teens, and other vulnerable groups experience heightened risks online as compared to adults, FPF encourages the OAG to consider instances where regulatory alignment with other state laws may be appropriate to harmonize important protections, enable socially beneficial data processing, and reduce unnecessary cross-jurisdictional regulatory divergences for companies.

1. *Consider excluding publicly available information and aggregate or deidentified information from the definition of "personal data."*

The Act defines "personal data" as "any data that identifies or could be reasonably linked, directly or indirectly, with a specific natural person or device."[33] This is a strong, broad definition that aligns with emerging global standards by focusing on identifiability rather than listing specific types of categories of information. However, given the breadth of this standard, many jurisdictions have included particular carve outs or limitations in order to meet other legal requirements, reflect technical realities, or advance other public policy priorities. For example, the comprehensive U.S. state privacy laws include common exclusions to the scope of "personal data," including "publicly available information" and "deidentified data," neither of which are explicitly recognized under the NYCDPA.[34]

[33] N.Y. Gen. Bus. Laws § 899-ee(4) (Consol. 2024).
[34] *See, e.g.* Conn. Gen. Stat. § 42-515(18); Colo. Rev. Stat. § 6-1-1303(17)(b) *see also* David A. Zetoony, *What is 'publicly available information' under state privacy laws?* GreenbergTraurig (Sept. 13, 2023), https://www.gtlaw-dataprivacydish.com/2023/09/what-is-publicly-available-information-under-the-state-privacy-laws/.

Publicly available information has historically almost always been excluded from U.S. privacy laws due to protecting the interest of accessing information of public importance, such as government records and court documents. Publicly available information is also often excluded to alleviate any perceived concerns about the government restricting access to information. These carveouts within state comprehensive privacy laws are not uniform but typically include information that has been lawfully made available through public government records and data that has been made available through "widely distributed" media or information that a consumer has made "widely available" to the general public.[35] At the same time, some information made publicly available can also carry significant privacy implications.[36] For example, persistent collection and tracking of individuals appearing in public can reveal highly sensitive personal activities and choices, and raises additional equity and fairness concerns.[37] One way California privacy law has sought to balance these equities is by exempting from its definition of public information "biometric information collected by a business about a consumer without the consumer's knowledge."[38]

The ANPRM further asks how regulations should account for "anonymized or deidentified data that could still potentially be re-linked to a specific individual." U.S. privacy laws typically exclude appropriately de-identified data from some or all coverage. When subject to appropriate technical controls, data that has been deidentified does not carry the same level of risk as personal information.[39] The main policy rationales for excluding deidentified data are to enable statistical or aggregate socially beneficial research, and incentivize companies to store data in less identifiable forms. Furthermore, as a technical matter, organizations will not be able to apply user-specific privacy rights to deidentified data as such information cannot be linked with any particular individual – for example, if data has been deidentified, it is not clear how a business could respond to a user request to revoke consent for the use of the that data.

Appropriately deidentified data may already outside the scope of the definition of "personal information" under the NYCDPA. However, an explicit exclusion, along with a definition of what is considered deidentified data can be helpful to provide clarity for both individuals and companies while encouraging companies to store data in more privacy-preserving formats. State privacy laws typically require "deidentified" data to meet a three part standard rooted in guidance from the Federal Trade Commission[40] requiring that organizations (1) take reasonable measures to

---

[35] *See, e.g.* Conn. Gen. Stat. § 42-515(25); Colo. Rev. Stat. § 6-1-1303(17)(b).
[36] *See e.g.,* Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, California Law Review, (forthcoming 2025) *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884485.
[37] *See* Will Knight, *Clearview AI has New Tools to Identify You in Photos*, Wired (Oct. 4, 2021), https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos.
[38] Cal. Civ. Code § 1798.140, subd. (v)(2).
[39] *See* Kelsey Finch, *A Visual Guide to Practical Data De-identification*, FPF (Apr. 25, 2016), https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification (exploring the spectrum of data deidentification).
[40] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

ensure that the data cannot be associated with an individual, (2) publicly commit to maintaining and using deidentified data without attempting reidentification, and (3) contractually obligating any recipient of that data to comply with the provisions of the law.[41]

2. Consider recognizing research as a permissible purpose for data collection and processing

State privacy laws often include some form of exclusion in order to enable public interest research activities, meaning that personal data otherwise covered under state privacy laws may still be shared with researchers. Typical language provides that:

> "Nothing in this [section] shall be construed to restrict a controller's or processor's ability to: Engage in public or peer-reviewed scientific, [historical] or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities."[42]

Given that the NYCDPA and SAFE For Kids were passed to create additional protections for minors online, developing guidance on whether and how data sharing for research may still take place will further the statute's intentions. For example, researchers at one of New York's universities may want to study the mental health effects of social media on teens, including usage patterns and the content that is directed to or accessed by child and teen users. Data sharing for research is an important tool in which to evaluate and inform better business practices and public policy on important topics such as children's wellbeing online.[43] Privacy risks from data sharing can be mitigated by covered operators implementing reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

C. Consult with the New York State Education Department to ensure alignment with New York's existing student privacy laws and implementing regulations.

Although student data is often excluded from consumer privacy laws[44], student data is not explicitly excluded from the NYCDPA's scope. This may have been an intentional policy choice by the New York Legislature, but is likely to have consequences that would prevent or limit the ability of students to use educational devices and services. As the OAG develops regulations, understanding how this law will interact with New York's existing student privacy laws and

---

[41] *See* David A. Zetony, *What is de-identified data?* GreenbergTraurig (Nov. 22, 2021), https://www.gtlaw-dataprivacydish.com/2021/11/what-is-de-identified-data/.
[42] *E.g.*, Conn. Gen. Stat. § 42-524(a)(10); Va. Code Ann. § 59.1-582(A)(8); Utah Code Ann. § 13-61-304(1)(j); *see also* Cal. Civ. Code § 1795.105, subd. (d)(6) (providing an exception to an individual's right to delete their personal information).
[43] *See* Sara Jordan, *Data Sharing for Research*, Future of Privacy Forum https://fpf.org/wp-content/uploads/2022/12/FPF-Playbook-singles.pdf.
[44] Randy Cantz, *Demystifying the Consumer Privacy Patchwork*, Student Privacy Compass (Jan. 18, 2024), https://studentprivacycompass.org/demystifying-the-consumer-privacy-patchwork.

implementing regulations is critical. In particular, the OAG should carefully consider the unique dynamic in schools when it comes to Federal Education Rights and Privacy Act (FERPA), COPPA and New York Education Law 2-d's exceptions to requiring consent for edtech products.

Under COPPA, a school may act as an agent for a parent and provide consent for edtech companies to collect data from students on behalf of parents when there is a valid vendor contract in place and data is used only for educational purposes.[45] New York Education Law 2-d and its implementing regulations create additional obligations for schools regarding student data and directly regulate third-party contractors of schools, including edtech.[46] Under Education Law 2-d, personally identifiable information of students may not be sold or used for marketing purposes, and a parental bill of rights for data privacy and security must be included in contracts with third-party contractors, which outlines a number of obligations that edtech companies contracting with schools must abide by, such as not redisclosing data beyond what is authorized by the school.[47]

Each school may use several thousand edtech services, so each parent providing consent for each student for each service would place a disproportionate burden on parents.[48] Both Education Law 2-d and FERPA, through the school official exception,[49] acknowledge that the school is better positioned to vet vendors and enter into contracts with edtech companies on behalf of individual parents. Resources like the Student Data Privacy Consortium's National Data Privacy Agreement provide model terms addressing student privacy concerns and data governance.[50] We encourage the OAG to consider the NYCDPA's consent provisions in the context of this dynamic and consult with the New York State Education Department Chief Privacy Officer.

---

[45] COPPA FAQ N.1 Can an educational institution consent to a website or app's collection, use or disclosure of personal information from students?, (Federal Trade Commission), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS.

[46] Future of Privacy Forum & Playwell, LLC, *Third Party Contractor Requirements at a Glance: NY Education Law §2-d*, Student Privacy Compass (Jan. 29, 2020), https://studentprivacycompass.org/wp-content/uploads/2020/01/NYS-Education-Law-2-d-at-a-Glance_FPF.Playwell.pdf.

[47] *Id.*, *See also* N.Y. Comp. Codes R. & Regs. tit. 8, § 121.9.

[48] Instructure, *EdTech Top 40: A Look at K-12 EdTech Engagement During the 2023-24 School Year* (June, 2024), https://www.instructure.com/edtech-top40.

[49] Privacy Assistance Technical Center, *FERPA Exceptions-Summary,* Student Privacy Compass (April 2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_portrait_0.pdf.

[50] Student Data Privacy Consortium, *National Data Privacy Agreement,* Access 4 Learning Community (April 24, 2024), https://privacy.a4l.org/national-dpa/.

D. Mitigate privacy, technical, and practical implementation concerns with "age flags" by further consulting with stakeholders and establishing baseline criteria. FPF offers technical and policy considerations the OAG must consider in furthering this emerging technology.

The NYCDPA requires that companies treat an individual as a covered minor if "a user's device communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism that complies with regulations promulgated by the attorney general."[51] The Act also contemplates similar, potentially distinct mechanisms that will convey information regarding "processing that the covered user consents to or declines to consent to."[52] Given that these are novel requirements in privacy law, and refer to technologies that are not currently in operation, FPF writes with technical and policy considerations for the development of age flag and consent signals. We note that in 2024 California considered a similar proposal for signaling age information with AB 1949 but the proposal was vetoed by Governor Newsom, expressing concern that the bill could have "unanticipated and potentially adverse effects on how businesses and consumers interact with each other, with unclear effects on children's privacy."[53]

While "age flags" and "consent flags" as contemplated in the Act are tools still in their early stages of development, a comparison can be drawn between these flags and universal opt-out mechanisms provided for and currently utilized in state comprehensive privacy laws that were developed over many years of standardization efforts. Universal opt-out mechanisms (UOOMs) refer to a range of desktop and mobile tools designed to provide consumers with the ability to configure their devices to automatically opt out of the sale or sharing of their personal information with internet-based entities with whom they interact.[54] These tools transmit opt-out preferences using technical specifications, such as the Global Privacy Control.[55] UOOMs were developed over many years of standardization efforts, yet are still an expanding technology.[56]

In states that provide for UOOMs, there are typically statutory criteria and, in some cases, implementing regulations detailing technical requirements and disclosures necessary for valid UOOMs. For example, the Colorado Privacy Act and implementing regulations require that a UOOM must be an opt-out choice; must clearly communicate the consumer's unambiguous choice to opt-out of specific processing; must be consumer-friendly, clearly described, and easy

[51] N.Y. Gen. Bus. Law § 899-ii (Consol. 2024).
[52] *Id.*
[53] *See* A.B. 1949, 2024 Reg. Sess., (Ca. 2024) *and* Governor Newsom, *AB1949 Veto Message*, Office of the Governor (Sept. 28, 2024), https://www.gov.ca.gov/wp-content/uploads/2024/09/AB-1949-Veto-Message.pd .
[54] Samuel Adams and Stacey Gray, *Survey of Current Universal Opt-Out Mechanisms,* Future of Privacy Forum (October 12, 2023), https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms/.
[55] Global Privacy Control, *Take Control of Your Privacy*, https://globalprivacycontrol.org/ (last visited September 25, 2024).
[56] *Id.*; 4 Colo. Code Regs. § 904-3, part 5. (Co. 2023).

to use; consistent as possible with any other similar mechanism required by law or regulation in the United States; and must allow the controller to accurately authenticate the consumer as a resident of Colorado and as a legitimate request.[57] The OAG should adopt baseline principles for developing valid age and consent flags that support usability and predictability on behalf of users and operators. **To help the OAG develop baseline criteria for age flags, FPF details a set of technical and policy considerations.**

1. Technical considerations for the development of "age flags"

- *Should "age flags" be the one source of truth on age for a covered operator?* The NYCDA conceives of "age flags" as a proactive signal to a covered service rather than a resource that businesses may query. While age assurance strategies vary widely across services, sometimes a service might ask individuals to self-declare their age or undergo a verification process. Therefore, a covered operator may already have adequate age information in some instances. We encourage the OAG to consider whether a signal about age should be preferenced over other age assurance methods. We further encourage the OAG to consider the discretion a covered operator should have in resolving conflicting age information, especially noting the potential for families to share devices without adjusting age flag settings for each usage session.
- *What is the process for verifying age with the age flag provider?* The OAG should consider whether to affirmatively approve technical specifications, methods, or providers of age flags based on specific criteria. Additionally, if an age flag provider verifies the age of its users, the OAG should consider whether that provider should share the assurance level with the covered operator. Given that no technical specifications currently exist for age flags, a potential scenario could exist where an individual simply self-declares their age with an age flag mechanism that is not subject to any validation process. Self-declaration provides a lower level of assurance than a method like providing digital identification, so without approval criteria, the covered operator may need accompanying information on the assurance level.
- *What role does residency authentication play?* In the NYCDPA, a covered user must be someone in the state of New York. However, an operator receiving an age flag may not always have an available means to determine whether a visitor is accessing a website from New York. Under the Act, it is unclear if the age flags are queryable or proactively offered to a service regardless of the user's location. The OAG can consider alleviating this point by opting for signals to be queryable upon request of the covered operator only after determining the user is in New York. Alternatively, the OAG can clarify that the obligations under the law do not apply where the age flag is sent and a user is not "in" New York.

[57] 4 Colo. Code Regs. § 904-3, part 5.

2. Policy considerations for the development of "age flags"

- *When should age flags be communicated—proactively, on a default basis, or only when queried?* The NYCDPA is ambiguous on when an "age flag" signal will be communicated, but under a strict reading of the statutory requirements, the signal is automatically offered to all websites. The Act's scope is limited to a certain segment of services that are primarily directed to minors. However, an "age flag" signal could potentially be broadcast to *every* website online and app, even those outside of the Act's scope. A key difference between New York's age signals and UOOM is that UOOM signals an individual's preference with respect to opting out of certain types of data practices. In the case of New York, the signal reveals a level of personal information – whether a particular individual is or is not a minor. Some online services, like news organizations, might be agnostic to visitor ages and do not seek to collect any age information, and it may be counterintuitive to data privacy best practices to offer age information proactively. The OAG should explore how an age flag could be queried, such as only delivering it upon the request of a covered operator or at the user's discretion. Each approach may have tradeoffs, such as bad actors improperly requesting to receive signals, or users needing to take extra steps to use the mechanism. Ultimately, deciding when to share the age flag is key to the technology's effectiveness.
- *Is there potential for bad actors to misuse the age flags?* If the implementation of an age flag is an under-18 signal that is proactively broadcast as a user browses the internet, there is the potential for a bad actor to build a profile of devices associated with minors. There is also a potential for age flag providers to over-collect or misuse information in the verification or authentication process. The OAG should consider what if any policy or technical approaches could mitigate these risks.
- *What role does the age flag play in other obligations under the statute?* Under the Act, the age flag communicates whether an individual is a *minor*—under 18 years old or 18 and over. However, the Act's protections differ between those under 13s and 13 - 17-year-olds. What additional steps should the service take to determine where a minor fits between these two age delineations, or alternatively, should the age signal provide more granular age information? FPF's SAFE for Kids comments address methods for parental consent and age age assurance, but we note the privacy risks highlighted above would be exacerbated by sharing more granular age information of minors with every website.[58]
- *Will the OAG approve or reject certain implementations of the age flag, and will this be communicated to the public?* The OAG should consider mitigating the prevalence of malicious actors in this emerging technology. The intention of the age flags is to communicate online who is or is not a minor, so parents and minors seeking to avail

[58] FPF's comments on the OAG's SAFE for Kids Act ANPRM were submitted contemporaneously to these comments and therefore cannot be linked here. To view those comments, please contact Bailey Sanchez or find them on fpf.org if available. *See also* Bailey Sanchez & Jim Siegl, *New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs*, FPF (June 26, 2023), https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs.

themselves of this tool may be targeted by deceptive marketing tactics. For example, while filing for federal student aid is free, there is now a studentaid.gov resource page on avoiding student aid scams due to malicious actors in the space.[59] Colorado opted to affirmatively approve or reject implementations of the UOOM, though currently, only one implementation is approved. To support standardization, predictability for operators, and mitigate the potential for bad actors, the OAG should consider a process to review and approve qualifying "age flag" signals, this could be carried out for both providers of signals and the technical specifications for individual signals.

- *Should the OAG consider incentivizing innovation in this emerging technology?* Given that age flags are not commonplace in the market, at either the vendor or company level, the OAG can consider whether any "good faith" compliance defense is appropriate. For example, a "good faith" compliance defense could alleviate issues with conflicting age information or conflicting age flags, if there is an influx of new signals in the market. Additionally, as the methods, vendors, and implementations of age flags develop, businesses may have difficulty determining signals that are valid expressions of user age status and establishing configurations to detect valid signals. The OAG can consider what reasonable efforts should be made to respect valid signals.

E. Separately consider opt-in flags from age flags, as opt-in flags are not currently in the market.

Affirmatively invoking privacy choices on an individual website-by-website basis can create burdensome friction and may be impracticable for ordinary consumers. In response to this issue, many comprehensive state privacy laws allow consumers to exercise **opt-out** rights through device signals such as browser plug-ins. UOOMs typically give consumers the ability to restrict the use of personal data for targeted advertising and data sales.[60] UOOMs have been a pro-consumer innovation in U.S. privacy law because such tools allow individuals to exercise their privacy preferences on a default basis, instead of requiring individuals to navigate the privacy settings of each website or app they visit.

In contrast to UOOMs common under state privacy laws, the NYCDPA appears to contemplate minors **opting-in** to the collection and processing of their personal data on a default basis through device settings consistent with the Act's informed consent requirements.[61] It is important to note upfront that "opt-in" consent is different in-kind from "opt-out" consent. Under opt-in consent, a company must provide notice and an individual must take an affirmative consent action to allow data collection and processing. Under an opt-out consent model, the default is that data collection and processing may take place absent separate action from a user. Both U.S.

---

[59] VSAC Staff, *Student Loan Scams Are on the Rise - Two Scams to Avoid and Ten Red Flags to Notice*, VSAC (Aug. 28 2024), https://www.vsac.org/blog/Avoid-Student-Loan-Scams; *Avoiding Student Aid Scams*, Student Aid, https://studentaid.gov/resources/scams (last visited Sept. 24, 2024).
[60] E.g., Cal. Civ. Code § 1798.135, subd. (b); Colo. Rev. Stat. § 6-1-1306.
[61] N.Y. Gen. Bus. Law § 899-ii (Consol. 2024).

state and global consumer privacy regimes typically set a high bar for opt-in consent, specifically that such consent must be "freely given, specific, informed, and unambiguous."[62] It is therefore unclear how a minor could give "informed consent" under the NYCDPA on a default basis through a device setting. Opting into data collection and processing by default appears inherently contradictory to requirements that consent be "specific" and "informed."

The NYCDPA anticipates the use of such signals to "decline to consent" to processing but this would also be extremely difficult to operationalize across industry without further standardization. Businesses collect different data sets for different purposes, so opt-in consent is often inherently contextual to a specific interaction between a user and business. In contrast, under existing law, the exercise of rights on a default basis is tied to specific business activities so that consumers know what to expect when they install and use device signals. In the context of the NYCDPA, providing for opt-out consent signals appears unnecessary because the law is already an opt-in consent framework, meaning that processing cannot take place unless informed consent is affirmative provided (or a permissible purpose is satisfied).

Critically, to FPF's knowledge, mechanisms to provide affirmative consent to processing are **not *currently in the market*** and opting individuals into data collection and processing by default through device or browser settings may actually result in more data collection and processing, weaken transparency and consumer choice, and undermine the purposes of the NYCDPA. Given the unique technical and policy challenges posed by developing novel device signals that communicate opt-in consent, FPF recommends that the forthcoming rulemaking, the OAG explicitly treat opt-in signals contemplated under the NYCDPA separately from age flag signals as the two signal mechanisms present unique risks and opportunities that would be best resolved separately and communicated through separate mechanisms.

Thank you for this opportunity to provide comment on these proposed regulations. We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Bailey Sanchez at bsanchez@fpf.org.

Sincerely,

Bailey Sanchez	Jordan Francis,	Keir Lamont
Senior Counsel	Policy Counsel	Senior Director
Future of Privacy Forum	Future of Privacy Forum	Future of Privacy Forum

[62] General Data Protection Regulation (GDPR), Art. 4(11).