



Data Minimization's Substantive Turn

Key Questions & Operational Challenges Posed by New State Privacy Legislation

FPF U.S. Legislation White Paper

June 2025

Jordan Francis, Policy Counsel, U.S. Legislation

Executive Summary

Data minimization is a bedrock principle of privacy and data protection law, with origins in the Fair Information Practice Principles (FIPPs) and the Privacy Act of 1974. At a high level, data minimization prohibits a covered entity from collecting, using, or retaining more personal data than is necessary to accomplish an identified, lawful purpose. In recent years, data minimization has emerged as a contested and priority issue in privacy legislation. Under longstanding notice-and-choice legal regimes, companies have been subject to “procedural” data minimization requirements whereby collection and use of personal data is permitted so long as it is adequately disclosed or consent is obtained. As privacy advocates have pushed to shift away from notice-and-choice, some policymakers have begun to embrace new “substantive” data minimization rules that aim to place default restrictions on the purposes for which personal data can be collected, used, or shared, typically requiring some connection between the personal data and the provision or maintenance of a requested product or service. For its proponents, this substantive turn promises to better align companies’ collection and use of personal data with consumers’ reasonable expectations. For its detractors, however, this trend threatens to upend longstanding business practices, introduce legal uncertainty, and threaten socially beneficial uses of data. The core of this debate is really the societal value of different uses of data, and whether certain data uses should be allowed, encouraged, discouraged, or prohibited by default, which itself is a proxy for major economic and political decisions with vast societal implications.

This white paper explores state lawmakers’ turn towards substantive data minimization. In Part I, this paper identifies the relevant standards: procedural data minimization (the majority rule); substantive data minimization (the rule that is currently law in Maryland and several sectoral laws); and reasonable expectations (the approach taken by California). These substantive data minimization rules raise a number of challenges and unresolved questions, which are explored in Part II. The questions raised by substantive data minimization include: (1) The role of consent; (2) How to determine what is “necessary” to provide a requested product or service; (3) The role of default protections versus individual control; (4) Whether substantive data minimization is too uncertain; (5) Whether procedural and substantive data minimization can be characterized as “objective” and “subjective”; and (6) The interplay between substantive data minimization and a law’s exceptions. How these questions are resolved will have significant implications for economic activity and data-intensive business practices, including advertising, artificial intelligence, and product improvement generally. The paper concludes by briefly outlining several options for how policymakers could approach constructing a forward-looking, flexible substantive data minimization rule.

Acknowledgements

The author thanks Keir Lamont for his contributions to this white paper. This white paper is based in part on a prior article written by the author that was first published by the IAPP in May 2024.¹

Table of Contents

- I. The Legislative Shift from Procedural to Substantive Data Minimization.....3
 - A. Terminology..... 4
 - B. The Majority Rule: Procedural Data Minimization..... 5
 - C. An Emerging Paradigm: Substantive Data Minimization..... 8
 - 1. The Maryland Online Data Privacy Act is the First State Comprehensive Law to Include Substantive Data Minimization..... 9
 - 2. Alternative Formulations of “Substantive Data Minimization” 11
 - D. The Third Stream: California’s “Reasonable Expectations” Standard..... 12
- II. Interpretive Questions and Considerations for Covered Entities and Policymakers.....15
 - A. Interpretive Questions..... 16
 - 1. What Role Does Consent Play?..... 16
 - 2. What is “Necessary” to Provide or Maintain a Product or Service?..... 17
 - B. Policy Considerations and Possible Rule Constructions..... 22
 - 1. Default Protections versus Individual Control..... 23
 - 2. Reasonable Certainty and Socially-beneficial Secondary Uses..... 25
 - 3. Subjectivity versus Objectivity..... 26
 - 4. Interplay with the Law’s Exemptions..... 27
 - 5. Options for Constructing a Substantive Data Minimization Rule..... 27
- Conclusion..... 30
- Appendix..... 31

¹ 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>.

I. The Legislative Shift from Procedural to Substantive Data Minimization

Data minimization—which prohibits a covered entity from collecting, using, or retaining more personal data than is necessary to accomplish an identified, lawful purpose—has become a priority issue in privacy legislation. Lawmakers in recent years have experimented with moving away from notice-and-choice regimes that focus on disclosures made to the consumer towards substantive rules that delineate specific “permissible processing” activities. This shift is motivated by the perception from privacy advocates that procedural data minimization rules allow covered entities² to collect and use personal data for any reason so long as that use is disclosed in a privacy notice, whereas a substantive data minimization rule limits the collection and use of personal data to what is necessary to provide or maintain a requested product or service, which could be better-aligned with individuals’ reasonable expectations.³

Others have argued, however, that this shift towards data minimization will inhibit desirable data practices due to its vagueness and restrictiveness—especially the development of AI models and products, longstanding advertising practices, internal operations such as product improvement, and research.⁴ The core of this debate is really the societal value of different uses of data, and whether certain data uses should be allowed, encouraged, discouraged, or prohibited by default, which itself is a proxy for major economic and political decisions with vast societal implications.⁵

² Given that various consumer privacy laws and bills have varying, unique terminology for the entities to which they apply (e.g., controller, business, regulated entity, covered entity), this white paper uses the term “covered entity” to refer in the abstract to the entities subject to consumer privacy legislation.

³ Eric Null, *States Are Letting Us Down on Privacy*, CDT (Jan. 28, 2024), <https://cdt.org/insights/states-are-letting-us-down-on-privacy> (“Data minimization requirements place the privacy-protecting burden primarily on companies that collect and exploit the data, rather than on the already overburdened consumer. . . . For years, however, most people have agreed that notice-and-consent has failed, in large part because we know that people do not read or understand laborious, labyrinthian privacy policies.”). For counterarguments, see *infra* Part II.B.

⁴ See Paul Lekas & Anton van Seventer, *The American Privacy Rights Act’s Hidden AI Ban*, Tech Dirt (Oct. 29, 2024), <https://www.techdirt.com/2024/10/29/the-american-privacy-rights-acts-hidden-ai-ban> (“[A] framework built around permitting only predetermined uses of data would have unintended, unforeseen and potentially disastrous consequences both for domestic technological development and U.S. competitiveness on the world stage.”); see also Jules Polonetsky, Omer Tene & Joseph Jerome, *Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Settings*, 13 Colo. Tech. L. J. 333 (2015) (describing the “increase in research taking place outside of universities and traditional academic institutions” utilizing commercial data). State comprehensive consumer privacy laws typically include research exemptions. *E.g.*, Conn. Gen. Stat. § 42-524(a)(10) (2025) (providing that nothing in the Connecticut Data Privacy Act shall be constructed to restrict a controller’s ability to “engage in public or peer-reviewed scientific 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 that determines, or similar independent oversight entities that determine,” whether the public benefits of the research outweigh privacy risks as offset by reasonable safeguards).

⁵ Omer Tene & Jules Polonetsky, *To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J. L. & Tech. 281, 332–57 (arguing that debates over default practices (e.g., targeted advertising) are more about the social value of the underlying activity rather than a legal or technical question).

In deemphasizing consent requirements, substantive data minimization could also disempower individuals by placing decisions over how data may be used in the judgement of either companies or regulators, regardless of whether or not an individual consents to their use of their information for a particular purpose. This policy debate around data minimization has in recent years led to the emergence of three distinct types of data minimization rules in state comprehensive privacy laws: procedural data minimization (the majority rule); substantive data minimization (the rule that is currently law in Maryland); and reasonable expectations (the approach taken by California). This white paper provides background on these distinct rules and the policy tensions to consider with each.

A. Terminology

As a decades-old concept that has been implemented and interpreted in a variety of legal frameworks across industries and jurisdictions, discussions about data minimization can be hampered by inconsistent terminology. For clarity, consider these common terminological pitfalls—

- **Data Minimization as an Umbrella Term:** This white paper refers to a set of related principles—data minimization and purpose limitation—under the umbrella term “data minimization” for simplicity and to reflect the increasingly broad use of this term in policy discussions. There are nuanced differences between what these terms mean under various legal frameworks, but at a high level: Data minimization means that a covered entity should not collect, use, or retain more personal data than is necessary to accomplish an identified, lawful purpose;⁶ and purpose limitation typically means that a covered entity must obtain an individual’s consent if it plans to use that individual’s personal data for a purpose other than the purpose for which it was collected (i.e., “secondary use” restrictions).⁷
- **Collection v. Processing:** In common parlance, processing personal data is often treated synonymously with using personal data in some way. In privacy laws, however, processing is generally defined broadly to include any set of operations on data, including collection, retention, maintenance, and deletion. For example, under Maryland’s comprehensive privacy law, “process” means “an operation or set of operations performed by manual or automated means on personal data,” and it includes “collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.”⁸ That law does not define “collecting,”

⁶ Info. Comm’rs Off., *Principle (c): Data Minimisation*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation> (last visited Mar. 24, 2025).

⁷ Info. Comm’rs Off., *Principle (b): Purpose Limitation*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/purpose-limitation> (last visited Mar. 24, 2025).

⁸ Maryland Online Data Privacy Act, S.B. 541, § 14-4601(y), 2024 Reg. Sess. (Md. 2024) (emphasis added).

but the term is clearly different (and narrower) than “processing.”⁹ This distinction matters because some data minimization rules have different limits for collection than processing more generally, and data minimization at collection (i.e., intake or creation of personal data) is inherently narrower than data minimization at processing. If a law has different data minimization requirements for “collecting” personal data and “processing” personal data, but if “processing” is defined to include “collecting,” then such rules may be internally inconsistent.

- **Personal Data v. Sensitive Data:** Another key distinction in state privacy laws is between personal data and sensitive data. Personal data is typically defined as any information linked or reasonably linkable to an identified or identifiable individual (“consumer”). Sensitive data is a subset of personal data subject to heightened protections. Typical categories of sensitive data include personal data that reveal certain sensitive characteristics (e.g., race), precise geolocation data, personal data of a known child, and biometric or genetic data. Like the collection versus processing distinction, statutes may have one data minimization rule applicable to personal data generally and another, overriding data minimization rule specific to sensitive data.
- **Exemptions:** Another important qualifier is that each of the laws discussed in this white paper includes its own exemptions and exceptions that limit the law’s impact on various sectors and common practices. These may include entity-level exemptions (e.g., non-applicability to government bodies and agencies, small businesses, nonprofits, or entities already subject to privacy laws such as GLBA or HIPAA), data-level exemptions (e.g., exclusions for employee data, publicly available information, or data subject to laws such as GLBA or HIPAA), or exceptions for specific activities (e.g., collecting and processing personal data for security purposes, solely internal uses, and compliance with other laws). None of the laws discussed in this white paper are truly “comprehensive” in the sense of affecting every possible entity and use of personal data. When evaluating the impact of the data minimization requirements of a specific law or bill, refer to that law’s various exemptions and exceptions.

B. The Majority Rule: Procedural Data Minimization

There has been a flurry of privacy legislative activity at the state level in recent years. Between 2018 and 2024, nineteen U.S. states enacted comprehensive consumer privacy laws. These laws are “comprehensive” in the sense that they are technology neutral, broadly applicable, and non-sectoral regulations of the collection, use, and disclosure of non-public “personal data.”¹⁰ Of

⁹ Of the state comprehensive privacy laws, the California Consumer Privacy Act (CCPA) is the only one to define “collection”: “‘Collects,’ ‘collected,’ or ‘collection’ means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.” Cal. Civ. Code § 1798.140, subd. (f).

¹⁰ See generally Jordan Francis, *Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends* (Nov. 2024), <https://fpf.org/wp-content/uploads/2024/11/REPORT-Anatomy-of-State-Comprehensive-Privacy-Law.pdf>.

those nineteen laws, all but California's are based in large part on the Washington Privacy Act (WPA) framework, a privacy bill from Washington State that was introduced several years in a row and, despite not being enacted, nevertheless became a model bill for other states.¹¹ Fourteen of the nineteen state comprehensive privacy laws include procedural data minimization, secondary use, and sensitive data consent requirements.¹² Under this framework, a controller is required to:

1. Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer ["data minimization"];
2. Not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent ["secondary use"]; and
3. Not process sensitive data concerning a consumer without obtaining the consumer's consent ["opt-in consent"].¹³

These three rules—data minimization, the consent requirement for secondary uses, and the consent requirement for processing sensitive data—establish the purposes for which controllers can process personal data. To put it simply: Collecting personal data is permitted as long as the purpose for collection is adequately disclosed; obtain consent to process personal data for new, unrelated purposes; and obtain consent to process sensitive data. As for the other five state laws, Utah, Iowa, and Rhode Island currently do not have explicit data minimization requirements whereas Maryland and California each have unique data minimization rules (see Parts C & D, respectively, below).

This framework can be labeled as “procedural data minimization” because these three rules are all procedural in nature. The data minimization and secondary use restrictions turn on procedural steps—what disclosures were made—rather than on the substance of the processing activity.¹⁴ The opt-in consent requirement for processing sensitive data, likewise, is procedural because whether the activity is legal depends upon whether the procedural requirements for consent (namely, that consent be “freely given, specific, informed and unambiguous”¹⁵) are met.

¹¹ *Id.* at 4–16 (explaining the history and common elements of the WPA framework).

¹² Colo. Rev. Stat. § 6-1-1308(3) (2024). See also Conn. Gen. Stat. § 42-520(a) (2024); Del. Code Ann. tit. 6, § 12D-106(a) (2024); Ind. Code § 24-15-4-1(f) (2024); Ky. Rev. Stat. Ann. § 367.3617(1) (2024); Minn. Stat. § 325M.16, subd. (2) (2024); Mont. Code Ann. § 30-14-2812(1) (2024); Neb. Rev. Stat. § 87-1112(1) (2024); N.H. Rev. Stat. Ann. § 507-H:6(l) (2024); N.J. Stat. Ann. § 56:8-166.12(a) (2024); Or. Rev. Stat. § 646A.578 (2024); Tenn. Code Ann. § 47-18-3305(a) (2024); Tex. Bus. & Com. Code Ann. § 541.101(a) (2024); Va. Code Ann. § 59.1-578(A) (2024).

¹³ *E.g.*, Conn. Gen. Stat. § 42-520(a) (2024). For similar language in other laws, see *supra* note 11.

¹⁴ 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>.

¹⁵ Conn. Gen. Stat. § 42-515(7).

Procedural data minimization has engendered considerable debate in recent years. Starting with the skeptical view, privacy advocates have accused this rule of being little more than a codification of notice-and-choice.¹⁶ Under that view, entities are free to collect whatever personal data they want, regardless of whether that data is in any way necessary for a legitimate business need, so long as the entity discloses the purpose for which it collects and uses the data in its privacy notice. When individuals therefore go out into the world and interact with an entity, they unwittingly agree to whatever data collection and use is specified in the privacy notice, which the individual likely did not read and is not in a position to bargain against. Proponents of procedural data minimization, however, often observe that procedural minimization rules can be more practical in light of the multiplicity of business models and data practices across the different business sectors that privacy laws regulate. Further, they may argue that procedural language is a meaningful check on unconstrained data collection while still providing reasonable certainty as to what needs to be done to be compliant with the law and continue legitimate business operations.¹⁷ Procedural data minimization's requirement to identify data practices upfront arguably is a meaningful limit on unconstrained data collection for the sake of speculative, undefined use further in time. Furthermore, requiring that covered entities get opt-in consent—under the meaningful “freely given, specific, informed, and unambiguous” standard—is a significant limit on data covered entities can collect and what they can do with that data.¹⁸

Where does this language come from? Like many aspects of the WPA framework, which is the basis of the majority of state comprehensive privacy laws, the procedural data minimization rule was adapted from the European Union's General Data Protection Regulation (GDPR), which itself is based on decades-old practices such as the Fair Information Practice Principles.¹⁹ Article 5, which establishes “Principles relating to processing of personal data,” provides,

¹⁶ E.g., *Data Minimization*, EPIC <https://epic.org/issues/consumer-privacy/data-minimization> (“The key words ‘as disclosed to the consumer’ mean that businesses are not really limited at all—they may collect and use data for any purposes they disclose in their privacy policies that no one ever reads.”) (last visited Mar. 30, 2025).

¹⁷ See Mike Hintze, *In Defense of the Long Privacy Statement*, Md. L. Rev., 76 Md. L. Rev. 1044, 1078–81 (2017) (arguing that lengthy privacy notices can create external accountability, create a culture of internal discipline and compliance, and be subject to meaningful enforcement from regulators while avoiding broader challenges from free speech advocates or industry that stricter privacy reforms would engender).

¹⁸ That limit, however, only functions to protect consumers if it is meaningfully enforced, including with prohibitions on employing manipulative design practices (i.e., “dark patterns”).

¹⁹ See Pollyanna Sanderson, Katelyn Ringrose & Stacey Gray, *It's Raining Privacy Bills: An Overview of the Washington State Privacy Act and other Introduced Bills*, FPF (Jan. 13, 2020), <https://fpf.org/blog/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills> (discussing how the Washington Privacy Act adapted some of the GDPR's key terms, definitions, and concepts, while still maintaining significant differences from GDPR in terms of scope and obligations). The collection limitation principle pre-dates GDPR by several decades. See Cheryl Saniuk-Heinig, *50 Years and Still Kicking: An Examination of FIPPs in Modern Regulation*, IAPP (May 25, 2021), <https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation> (identifying different instantiations of the collection limitation principle in laws around the globe).

“Personal data shall be collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with those purposes,” and that the data collected shall be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).”²⁰

⚠ Do not use this language’s origin as a proxy for its effect. Despite the superficial similarity in language, GDPR’s “data minimisation” principle operates very differently in practice than procedural data minimization requirements in U.S. state privacy laws. The critical distinction is that GDPR has other core principles which limit the collection and processing of personal data. Arguably the most important principle is “lawfulness”: Processing personal data (which includes collection) is prohibited unless the controller relies on one of the six lawful bases identified in the Regulation, such as if the data subject has provided valid consent for the processing, or if the processing is necessary for the performance of a contract between the data subject and the controller.²¹ Thus, under GDPR, processing personal data is additionally constrained by the lawfulness requirement which operates in tandem with the “purpose limitation” and “data minimization” requirements described above. Once a lawful basis is established and a purpose for processing provided, then data minimization provides an additional limit on the collection of personal data. In contrast, U.S. state privacy laws do not have a comparable requirement to lawful bases. In the absence of such a requirement, procedural data minimization creates an implicit lawfulness requirement: Processing purposes are generally permitted so long as they are disclosed.

C. An Emerging Paradigm: Substantive Data Minimization

Despite an emerging consensus forming around the WPA framework as the model for comprehensive privacy legislation in the states,²² lawmakers continue to iterate on that model and explore novel protections and obligations. This section looks at the rise of an alternative model of data minimization—substantive data minimization—that gained traction in recent years, culminating in the enactment of the Maryland Online Data Privacy Act in 2024.

²⁰ General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119), Art. 5(1)(b), (c) [GDPR].

²¹ GDPR Arts. 5(1)(a) & 6. There are six lawful bases enumerated in GDPR. The three most relevant are when “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”; “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”; and “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.” GDPR Art. 6(a), (b) & (f).

²² Jordan Francis, *Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends* (Nov. 2024), <https://fpf.org/wp-content/uploads/2024/11/REPORT-Anatomy-of-State-Comprehensive-Privacy-Law.pdf>.

1. The Maryland Online Data Privacy Act is the First State Comprehensive Law to Include Substantive Data Minimization

Prior to 2024, every state comprehensive privacy law based on the WPA framework either included procedural data minimization or lacked a general data minimization requirement. Maryland became the first state to break from this trend in May 2024 when it enacted the Maryland Online Data Privacy Act (MODPA), a comprehensive consumer privacy law that included substantive data minimization requirements.²³ Maryland's substantive data minimization rule is currently set to become effective in October 2025.²⁴ Under the MODPA:

A controller may not:

(1) Except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains, collect, process, or share sensitive data concerning a consumer ['data minimization' and 'secondary use' for sensitive data];

(2) Sell sensitive data;

...

(8) Unless the controller obtains the consumer's consent, process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer ['secondary use' for personal data].

...

A controller shall:

(l) Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains; ['data minimization' for personal data]²⁵

The MODPA's data minimization framework takes a bifurcated approach, setting different standards for personal data and sensitive data (a subcategory of personal data). For personal data, a controller may not collect a consumer's personal data unless it is limited to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. This is a departure from the procedural data minimization rule used

²³ In 2024, Maine and Vermont both came close to enacting comprehensive privacy legislation that included substantive data minimization requirements similar to Maryland's. See H.121, 2023–24 Reg. Sess. (Vt. 2024), <https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0121/H-0121%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf> (vetoed June 13, 2024); L.D. 1977, 131st Leg., (Me. 2024), <https://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1270&item=2&snum=131> (rejected by the Maine Senate Apr. 17, 2024).

²⁴ In the 2025 legislative session, lawmakers introduced a bill that would have amended the MODPA to align its data minimization rule with the majority of state comprehensive privacy laws. This bill did not pass. H.B. 1365, 2025 Reg. Sess. (Md. 2025), <https://mgaleg.maryland.gov/2025RS/bills/hb/hb1365F.pdf>.

²⁵ S.B. 541, § 14-4607, 2024 Reg. Sess. (Md. 2024). This excerpt excludes additional, narrower rules, such as the prohibitions on targeted advertising to individuals whom the controllers knows or should know to be under the age of 18.

in most states, where collection is simply tied to the purposes that a controller discloses to a consumer.²⁶ For secondary use, the MODPA includes the same procedural rule as the majority of states—a controller must get consent for any processing that is not reasonably necessary to nor compatible with the purposes it disclosed to the consumer. This means that, for personal data, the turn to substantive data minimization only acts as a gate on collection, but once data is validly collected, that data can be processed for any purpose as long as it was adequately disclosed. The turn to substantive data minimization is more impactful for sensitive data, however, as collection, processing, and sharing are limited to what is “strictly necessary” to provide a specific product or service requested by the consumer, and selling sensitive data is outright prohibited.

These data minimization rules are “substantive” in that whether the collection, processing, or disclosure of personal data or sensitive data is allowed turns on the nature of the processing activity and the relationship between the consumer and controller.²⁷ Determining whether the data practice is permitted requires assessing what data are either “reasonably necessary and proportionate” or “strictly necessary” to “provide” or “maintain” the “specific” product or service that is “requested” by the consumer. Thus, compliance entails a meaningful examination of the commercial relationship with the consumer, their expectations, what is ultimately being delivered to the consumer, and how each act of data collection, use, and disclosure benefits the consumer.

There is nothing new under the sun. While substantive data minimization requirements appear to be increasing in prevalence and scope, they are not wholly new, even with respect to comprehensive state privacy laws. Many of the existing state privacy laws that have procedural data minimization requirements also include narrower data minimization requirements for specified activities that use “reasonably necessary and proportionate” language. State comprehensive privacy laws typically provide that nothing in the law shall be interpreted to restrict a controller’s or processor’s ability to engage in certain listed activities, such as complying with state and federal law, protecting against security incidents, preserving the integrity or security of systems, and more. While these activities are nominally excepted from the law, some restrictions still apply. For example, Connecticut’s law provides that:

Personal data processed by a controller or consumer health data controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this

²⁶ It is important to note that Maryland’s rule does not abandon transparency and notice entirely. Although whether or not a controller can collect personal data does not turn on the disclosures made by the controller, the controller is nevertheless required by the law to disclose the purposes for which it processes personal data in a privacy notice. S.B. 541, § 14-4607(d), 2024 Reg. Sess. (Md. 2024).

²⁷ This white paper does not use the term “substantive data minimization” to indicate that this rule is stronger or more consumer protective than procedural data minimization; as Part II explores, there are serious questions as to whether that will be true in practice, despite whatever claims supporters or opponents of the rule have made thus far.

section [certain internal uses] shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention.²⁸

This is similar to a substantive data minimization obligation, only applied narrowly to the activities that are otherwise preserved by the law. Similar “necessity” provisions exist in some youth privacy protections in existing state comprehensive privacy laws.²⁹

2. Alternative Formulations of “Substantive Data Minimization”

The Maryland Online Data Privacy Act did not form in a vacuum. Rather, a wave of proposed bills and enacted laws in recent years have included variants of substantive data minimization. These bills and laws reveal different potential subtypes of substantive data minimization, each of which has its own strengths and weaknesses, which will be explored in Part II of this white paper. This section briefly summarizes a few alternative approaches seen in recent years.

- Necessity or Permitted Purposes:** The American Data Privacy Protection Act of 2022, a federal bill that passed committee but failed to receive a floor vote in the U.S. House, included a substantive data minimization requirement that followed a necessity-or-permitted-purposes approach. Under the ADPPA, covered entities would have been prohibited from collecting, processing or transferring covered data “unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to—(1) provide or maintain a specific product or service requested by the individual to whom the data pertains; or (2) effect a purpose permitted under subsection (b).”³⁰ The ADPPA included 17 permitted purposes, such as authenticating users of a product or service or preventing, detecting, protecting against, or responding to a security incident.³¹ For sensitive covered data, the standard was raised to “strictly necessary” and the list of permitted purposes was narrowed.³²
- Necessity or Consent:** Washington’s broad health privacy law, the My Health My Data Act (MHMD), provides yet another framework for substantive data minimization—necessity or consent. Under MHMD, a regulated entity may not collect any consumer health data except: (i) with a consumer’s consent or (ii) “[t]o the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.”³³

²⁸ Conn. Gen. Stat. § 42-524(f) (2024).

²⁹ E.g., Conn. Gen. Stat. § 42-529a(b) (2024).

³⁰ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 101–102 (2022) (version Dec. 30, 2022).

³¹ *Id.* § 101(b).

³² *Id.* § 102(2). There are further limits on transferring sensitive covered data to third parties. *Id.* § 102(3).

³³ Wash. Rev. Code § 19.373.030 (2024). Note that MHMD defines “collect” broadly to include “buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.” *Id.* § 19.373.010(5). For more on MHMD’s “necessary” requirement, see 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>.

- **Necessity or Consent or Permitted Purposes:** Other laws and bills have blended these approaches. Under the New York Child Data Protection Act (NYCDPA), an operator of a website, online service, online application, mobile application, or connected device cannot collect the personal data of a covered user aged 13 through 18 unless the collection is strictly necessary for one of nine permitted purposes listed in the act (one of which is providing a specific product or service requested by the covered user) or if the operator obtains informed consent for the collection.³⁴ This framework is similar to the ADPPA in that it allows for collection with doing so is necessary for the provision of a requested product or service or for one of several other enumerated permitted purposes. Like MHMD, however, it also allows for covered users to consent to processing activities that are otherwise not explicitly permitted.

For a table of non-exhaustive examples of substantive data minimization requirements in privacy legislation—covering legislation that is federal and state, proposed and enacted, and sectoral and comprehensive—see Table 1 in the Appendix to this paper.³⁵

D. The Third Stream: California’s “Reasonable Expectations” Standard

California has charted its own path with respect to data minimization. Under the California Consumer Privacy Act (CCPA), a business’s “collection, use, retention, and sharing” of personal information must be “reasonably necessary and proportionate” to achieve either (1) “the purposes for which the personal information was collected or processed,” or (2) “for another disclosed purpose that is compatible with the context in which the personal information was collected.”³⁶ Additionally, after a business provides notice at collection of the categories of personal information to be collected and the purposes for that information’s collection and use, a business cannot (1) collect additional categories of personal information or sensitive personal information, nor (2) use previously collected personal information for additional purposes incompatible with the disclosed purpose at collection, without providing new notice to the consumer.³⁷ California does not require opt-in consent for the use of sensitive personal information and instead creates a narrow, but substantive, opt-out right by which a consumer can direct a business to “to limit its use of the consumer’s sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services” or to perform a select number of “business purposes” under the law or as authorized in the CCPA regulations.³⁸

³⁴ N.Y. Gen. Bus. Code § 899-ff(1)–(2) (2024).

³⁵ Substantive data minimization continues to appear in various proposed bills and regulations. For example, the Consumer Financial Protection Bureau’s proposed implementing regulations for Section 1033 of the Dodd-Frank Act would require that third parties limit their “collection, use, and retention of covered data to what is reasonably necessary to provide the consumer’s requested product or service.” Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838, 90,996 (Nov. 18, 2024).

³⁶ Cal. Civ. Code § 1798.100, subd. (c).

³⁷ *Id.* (a).

³⁸ Cal. Civ. Code § 1798.121, subd. (a).

The law's implementing regulations, however, go further. Under the regulations, a business's collection, use, retention, and sharing of personal information must be limited to what is "reasonably necessary and proportionate" to achieve either: a disclosed purpose that is consistent with an individual's reasonable expectations, another disclosed purpose that is compatible with the context in which the personal information was collected, or another disclosed purpose for which the business obtained the individual's consent.³⁹ The regulations' introduction of a "reasonable expectations" standard for the collection and use of personal information adds (or enlarges) a substantive component to the CCPA's data minimization requirements.⁴⁰

"Reasonable expectations" is a longstanding concept under American privacy law. In the consumer protection context, the Federal Trade Commission's (FTC) enforcement authority against deceptive trade practices, which the FTC has long utilized to police deceptive privacy statements, considers whether statements or omissions are misleading from the perspective of a reasonable consumer.⁴¹ In the criminal law context, the *Katz* test for Fourth Amendment protection asks whether an individual has an (1) "actual (subjective) expectation of privacy" and (2) whether that "expectation be one that society is prepared to recognize as 'reasonable.'"⁴² This test has been criticized for shrinking Fourth Amendment protections over time as novel technologies become commonplace and individuals adjust their expectations.⁴³ The test has also been criticized as being "remarkably opaque" as courts continue to struggle to determine which privacy interests are "reasonable."⁴⁴

California's "reasonable expectations" test differs from the *Katz* test in a few ways. Most notably, it does not include a subjective element, which should allay some of the concerns about the erosion of privacy expectations over time. Second, the CCPA regulations do not leave businesses entirely on their own to assess what is within a consumer's reasonable expectations. Rather, the

³⁹ Cal. Code Reg. tit. 11, § 7002. Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is "reasonably necessary and proportionate" to achieve a given purpose depends upon: (1) "The minimum personal information that is necessary to achieve the purpose identified"; (2) "[t]he possible negative impacts on consumers posed by the business's collection or processing of the personal information"; and (3) "[t]he existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in [factor (2)]."

⁴⁰ According to the California Privacy Protection Agency, this requirement is a "clarification" of the statutory requirements. See *infra* note 46 and accompanying text.

⁴¹ See Chris Jay Hoofnagle, Federal Trade Commission: Privacy Law and Policy 123–130 (2016) (describing the FTC's 1983 Policy Statement on Deception, which considers "the perspective of a consumer acting reasonably in the circumstances") (citing FTC Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

⁴² *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

⁴³ Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139 (2016); see also Woodrow Hartzot, Evan Selinger & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 Wash. U. L. Rev. 717 (2024) (discussing how tying privacy rights to people's norms and expectations results in a gradual erosion of privacy).

⁴⁴ Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 505 (2007).

regulations provide the following factors for whether collection or processing is consistent with an individual's reasonable expectations:

- “The relationship between the consumer(s) and the business”;
- “The type, nature, and amount of personal information that the business seeks to collect or process”;
- “The source of the personal information and the business’s method for collecting or processing it;”
- “The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business’s good or service”; and
- “The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s).”⁴⁵

Some of these factors—as well as other factors in § 7002 relevant to when a new purpose is compatible with the context in which personal information was first collected and whether a practice is “necessary and proportionate” to achieve a disclosed purpose—are similar to the GDPR’s factors for determining whether a secondary use is “compatible” with the purpose for which the data were originally collected.⁴⁶

Categorizing this in the substantive-procedural framework, California’s rule is a “hybrid” approach because it relies on both procedural and substantive factors. For example, the disclosures made to a consumer, both in a privacy notice and in broader disclosures such as marketing material, are a relative but not dispositive fact as to whether processing of personal information can occur under the CCPA regulations. Other factors that examine the relationship between the parties and the nature of the data in question remain relevant.

According to the Final Statement of Reasons (FSOR) that accompanied the final rule, the reasonable expectations standard is a “clarification” of the statutory text that “further[s] the explicit purposes of Proposition 24” by “providing consumers with the ability to control their personal information.”⁴⁷ According to the FSOR:

When a business’s purpose for collecting or processing personal information is inconsistent with the consumer’s reasonable expectations, consumers lose control over their personal information and are not in an informed position where they can exercise their rights or knowingly and freely negotiate with a business over the business’s use of their personal information.⁴⁸

⁴⁵ Cal. Code Reg. tit. 11, § 7002, subd. (b).

⁴⁶ Compare *id.* subds. (b)–(d), with GDPR art. 6(4).

⁴⁷ Cal. Priv. Prot. Agency, California Consumer Privacy Act Regulations Final Statement of Reasons, at 4, (Mar. 29, 2023), https://coppa.ca.gov/regulations/pdf/20230329_final_sor.pdf.

⁴⁸ *Id.*

The FSOR also explains how to apply the factors. At a high level, the factors are (1) “objective,” in that they should be assessed from the perspective of a “reasonable consumer” rather than the subjective expectations of a specific consumer, and (2) they “must be assessed together.”⁴⁹

Notably, the first factor—the relationship between the consumer and the business—aligns with Maryland-style substantive data minimization. According to the FSOR, “If a business’s relationship with a consumer is based on the provision of a specific good or service, it is more likely under this factor that the consumer would reasonably expect the purpose of collection or processing to be the provision of that good or service.”⁵⁰ Rather than focusing on whether data is “necessary” for providing a product or service, the FSOR describes this assessment in terms of whether data is “related” to the product or service: “[W]hen the consumer’s relationship with a business is to obtain a specific service (e.g., provision of a mobile flashlight), the consumer is unlikely to expect that the business will collect personal information *unrelated* to the provision of that service.”⁵¹

II. Interpretive Questions and Considerations for Covered Entities and Policymakers

Substantive data minimization is moving from theory to reality. Washington’s My Health My Data Act has been in effect since March 31, 2024.⁵² The Maryland Online Data Privacy Act and the New York Child Data Protection Act are both scheduled to go into effect in 2025.⁵³ For privacy professionals and covered entities preparing for or building out compliance strategies, it is imperative to understand the bounds of this new regulatory framework. Until regulatory guidance or public enforcement comes, many will be left wondering what substantive data minimization’s effects are. Substantive data minimization could lead to the outcomes its advocates clamor for—a reworked information economy where businesses’ data practices align with consumer expectations and individuals are free to make choices without being subject to excessive and unnecessary data collection. Alternatively, this new framework could prove to be vague and unduly burdensome for covered entities, leading to uncertainty or overcompliance that restricts and impedes beneficial data uses and deprives consumers of access to desired products and services.

The remainder of this paper explores unresolved questions and operational challenges posed by this legislative shift, some arguments for and against substantive data minimization, and some alternative ways policymakers could construct such a rule.

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.* at 4–5 (emphasis added).

⁵² Keir Lamont, Bailey Sanchez & Jordan Francis, *Effective Dates for State Privacy Laws*, FPF (July 25, 2024), <https://fpf.org/wp-content/uploads/2024/07/FPF-Key-Dates-Chart-2024-Update.pdf>.

⁵³ *Id.*

A. Interpretive Questions

For privacy professionals working in compliance, the Maryland Online Data Privacy Act and other substantive data minimization requirements create uncertainty as to how to build or adapt compliance programs that meet these nebulous new standards. This section explores some of the immediate interpretive questions posed by novel substantive data minimization requirements.⁵⁴

1. What Role Does Consent Play?

The interplay between consent and a data minimization requirement is critical because consent can convert an otherwise inflexible, restrictive rule to one that is adaptable and accommodating of novel data uses (setting aside, *arguendo*, concerns about the friction and operational challenges introduced by consent requirements). Consent can affect a data minimization obligation either explicitly or implicitly.

Starting with the explicit relationship between consent and data minimization, it is possible to write a substantive data minimization rule whereby consent explicitly overrides any other limits on the collection or processing of personal data. For example, under Washington’s My Health My Data Act, a regulated entity cannot collect personal data unless either (a) doing so is necessary to provide a requested product or service, or (b) the regulated entity obtains consent for the data use.⁵⁵ Under that framework, consent can act as a release valve in that it provides an alternative legal basis for desirable activities, from the perspective of both a consumer and a covered entity, that might not otherwise be allowed or might be too risky to engage in without legal certainty. Thus, the added flexibility from including consent—as either an alternative permissible purpose or as an exception to a necessity requirement—lowers the stakes of how to interpret a substantive data minimization requirement because it reduces the pressure to read a data minimization permissively so as to allow a desired activity. The MODPA takes a less clear approach to consent than the My Health My Data Act. Specifically, the MODPA’s secondary use restriction for processing personal data provides that consent can legitimize an otherwise unnecessary or incompatible use of personal data. Because “process” is defined to include “collect,” then arguably a controller can collect any personal data so long as it obtains the consumer’s consent in a way that meets statutory requirements.⁵⁶

⁵⁴ The following are not an exhaustive list of considerations for compliance with substantive data minimization requirements. Rather, they are a handful of the most pressing and high-level questions that must be addressed.

⁵⁵ Wash. Rev. Code § 19.373.030 (2024). Note that “collect” is defined broadly under that law to include “process.” This necessity-or-consent structure is conceptually similar to how “performance of a contract” and “consent” are two alternative lawful bases for processing personal data under the GDPR. GDPR art. 6.

⁵⁶ An alternative reading of the statute would be that the specific rule (do not collect personal data unless it is reasonably necessary to provide the product or service) overrides the more general rule (do not process personal data for reasons that are not necessary to or compatible with the disclosed purposes).

The implicit role of consent raises another interpretive question. Substantive data minimization rules ask what collection or processing of personal data is necessary to provide a specific product or service “requested” by the individual to whom the personal data relates. When is a product or service “requested”? From a consumer’s perspective, the question arguably does not make sense. For a broad range of products and services, the onus is on a business, in the first instance, to offer the product or service. Consumers then select from available offerings, and may make additional customizations, setting changes, and other potential modifications to an order or ongoing service.

This ambiguity around what it means for a product or service to be “requested” by a consumer creates an ironic possibility: The turn from procedural to substantive data minimization was likely intended to reduce reliance on consent, yet it may exacerbate the problem in practice. This is because a broad reading of “requested” could incentivize the proliferation of consent pop-ups. If collection of personal data is tied to what is necessary to provide or maintain a specific product or service “requested” by a consumer, then arguably any processing activity can be justified under this rule if opt-in consent is obtained, because signifying consent makes the activity “requested” by the individual. Notably, because the language is “requested” and not “consented to,” then such consent prompts may not need to satisfy a law’s heightened consent requirements (e.g., that consent be “freely given, specific, informed, and unambiguous”). This creates the incentive for entities to spread ever-increasing, sub-standard consent prompts. Relying on such an interpretation may prove risky, however. If a reasonable consumer would not perceive a benefit from the collection or use of that data—meaning that, all else held constant, the nonexistence of that data would not alter the product or service they receive or improve their experience, even subtly—then an enforcer may not agree that merely clicking a consent pop-up is enough to make a use of personal data “necessary” for a requested product or service.


2. What is “Necessary” to Provide or Maintain a Product or Service?

The core limitation of a substantive data minimization requirement is the “necessity” standard—the collection and/or processing of personal data must be “necessary” to provide a specific product or service requested by the person to whom the data relates. This raises two questions: (1) How does one assess what is “necessary,” and (2) how does that change depending on what modifiers are used (e.g., reasonably necessary v. necessary v. strictly necessary)? These questions have significant real world implications, particularly with respect to secondary uses of personal data, the role of ad monetization in providing otherwise “free” access to content or services, and reliance on the law’s various exceptions. Consider the following:

Ad Monetization: If a news website were subscription based, rather than freely accessible, few would argue that the collection of a persistent identifier and payment information is not reasonably or strictly necessary for providing the requested service. But many websites opt to remain free-to-access and rely on monetization from advertising. In that case, what categories of personal data are reasonably necessary for it to collect and under what circumstances is such data strictly necessary for offering the specific product or service requested? What about

personal data used for ad measurement and attribution? Must the website rely on contextual advertising, or can it engage in retargeting and/or cross-context behavioral advertising? If advertising is within the bounds of “necessary,” does that change if the standard is raised to “strictly necessary,” as MODPA does for processing and disclosing sensitive data? This critique—the unclear status of advertising—was raised recently by FTC Commissioner Melissa Holyoak in prepared remarks at the 2024 National Advertising Division keynote.⁵⁷ Outside of advertising, there are similar examples of activities that are expected by consumers but which may not be allowed under an overly narrow interpretation of what is “necessary” to provide a requested product or service. For example, content moderation requires processing personal data but may not be “strictly necessary” for providing a social media service.

Bundling: Tying permissible personal data collection and processing to providing or maintaining a “requested” product or service creates a risk to individuals in that businesses are free to define the product or service in question and potentially bundle products or services. If the business can define the requested product or service to include ancillary and potentially unwanted features or data flows, then substantive data minimization could end up being functionally the same as procedural data minimization.

 **New York is considering this question.** The recently enacted New York Child Data Protection Act (NYCDPA) includes a substantive data minimization rule that 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 nine enumerated activities under the statute.⁵⁸ One of those permissible purposes is “providing or maintaining a specific product or service requested by the covered user.”⁵⁹ Shortly after the law was enacted, the Office of the Attorney General (NY OAG) released an Advanced Notice of Proposed Rulemaking that requested input about how it should address this bundling question:

Many modern online services bundle products or services together, or include ancillary products or services in response to a user request: for example, a cooking app might automatically display nearby groceries with relevant ingredients when a user looks up a recipe, which would require processing the user’s geolocation information. What factors should OAG consider in determining whether bundled products or services are incorporated into the ‘product or service requested by the covered user’?⁶⁰

⁵⁷ Melissa Holyoak, *A Path Forward on Privacy, Advertising, and AI: Remarks at National Advertising Division Keynote 2024* (Sept. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-NAD-Speech-09-17-2024.pdf.

⁵⁸ N.Y. Gen. Bus. Law § 899-ff(1)(b) (2024). For minors aged 12 and under, the processing is permitted if allowed under 15 U.S.C. § 6502 and relevant regulations.

⁵⁹ *Id.* § 899-ff(2)(a).

⁶⁰ Off. of the N.Y. Att’y Gen., *Child Data Protection Act: Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 899-ee et seq.* (Aug. 1, 2024), <https://ag.ny.gov/sites/default/files/2024-08/child-data-protection-act.pdf>.

In May 2025, the NY OAG released guidance that clarified the “strictly necessary” processing standard. The guidance emphasized that a product or service must be “specific” and “requested by the covered user,” which the guidance equates to being **“within the expectations of a reasonable covered user.”**⁶¹ Per the guidance, user consent is not necessary to track users’ online activities if the operator “clearly and conspicuously markets its core service as one that tracks specific user activities to provide a record of activities (e.g., a budgeting platform tracking spending activities in order to offer a monthly spending statement),”⁶² as that is sufficient to bring the activity within a reasonable user’s expectations. However, the guidance further provides that operators may not “circumvent” the law “simply by marketing its core service as one that includes tracking a covered user’s personal data to support personalization such as behavioral advertising or creating a profile on a specific individual to display or prioritize certain media.”⁶³ Any personal data collected as being “strictly necessary” to provide a requested product or service “may not be used by the operator . . . for any other purpose.”⁶⁴ This guidance from the NY OAG is a helpful framing of the problem and could provide a useful framework for approaching this problem under other substantive data minimization standards such as those in Maryland or Washington.

Another noteworthy aspect of the NYCDPA is that it provides other permitted purposes in conjunction with providing a requested product or service. Notably, the NYCDPA does not require consent to process a teenager’s personal data if doing so is strictly necessary for “conducting the operator’s internal business operations.”⁶⁵ Unlike the federal COPPA Rule’s internal operations exception, however, the NYCDPA states that internal business operations does not include **any activities** related to “marketing, advertising, [or] research and development.”⁶⁶ Excluding those activities from internal business operations exacerbates the ambiguity as to the meaning of providing a requested product or service.

⁶¹ Off. of the N.Y. Att’y Gen., *New York Child Data Protection Act Implementation Guidance*, (May 19, 2025), <https://ag.ny.gov/sites/default/files/2025-05/nycdpa-guidance.pdf> [hereinafter NYCDPA Guidance].

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ N.Y. Gen. Bus. Law § 899ff(2)(b).

⁶⁶ *Compare id.* (excluding marketing, advertising, and research and development from “internal business operations”), with 16 C.F.R. §§ 312.2 & 312.5(c)(7) (not requiring parental consent for collecting “a persistent identifier and no other personal information” if used for the “sole purpose of providing support for the internal operations of the Web site or online service,” which includes activities “necessary” to “[m]aintain or analyze the functioning of the Web site or online service” and “[s]erve contextual advertising on the Web site or online service or cap the frequency of advertising,” amongst other things). The updated COPPA Rule, set to go into effect on June 23, 2025, will have stricter limits on ed tech providers’ ability to use children’s personal information for product improvement. 89 Fed. Reg. 2,034, 2,074 (Jan. 11, 2024) (defining “School-authorized education purpose”).

The NY OAG's May 2025 guidance reiterated that the NYCDPA's "internal business operations" permitted purpose differs in scope from the COPPA Rule's "internal operations" exception in that it does not include "any activities related to marketing, advertising, research and development, [or] providing products or services to third parties."⁶⁷ However, the guidance provides that the "protecting against malicious, fraudulent, or illegal activity" permitted purpose allows processing personal data for "frequency capping of advertising."⁶⁸ Similarly, the "vital interests of a natural person" allows for processing personal data for "user trust, health, and safety policies."⁶⁹

Artificial Intelligence Development: By narrowing a controller's ability to collect and/or process personal data, substantive data minimization will undoubtedly have an impact on product improvement, development, and internal research. This problem is especially acute for the development of artificial intelligence, which relies on vast troves of data for training. Here the distinction between narrower restrictions on "collecting" personal data and broader restrictions on "processing" personal data matters, at least for developers that are using first-party data for training AI models. This problem also raises whether using *personal* data is necessary for training models, as model developers could rely in some circumstances on publicly available information, deidentified data, or synthetic data, all of which may be outside of privacy law.

Can a Controller Collect Personal Data Without a First-party Relationship? Substantive data minimization rules are grounded in the first-party context; restrictions on collection (or processing) of personal data turn on what is necessary to provide or maintain a specific product or service requested by the individual to whom the data relates. This framing poses a challenge to entities who do not have a direct-to-consumer relationship. For example, consider providers of third party SDKs. While these entities may act as service providers or processors insofar as they are processing personal data at the instructions of a business or controller, they may not be able to independently act as a controller by retaining, processing, or disclosing collected data for their own purposes. This could be an intentional policy decision—SDK providers are under increasing public scrutiny over perceived privacy violations.⁷⁰ More broadly, this could impact any purchaser of personal data. Depending on how it is interpreted, if "collection" includes purchasing, leasing, or otherwise acquiring personal data from another entity, then MODPA could foreclose the purchase of personal data, because such an act of "collection" is not in service of providing a requested product or service to the consumer to whom the data relates. Depending on how consent affects a substantive data minimization

⁶⁷ NYCDPA Guidance, *supra* note 61 (citing N.Y. Gen. Bus. Law § 899-ff(2)).

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ See Press Release, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, Tex. Att'y Gen., (Jan. 13, 2025), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45>.

rule, it is possible that such sales of personal data could proceed pursuant to consumers' consent.

A statutory rule tied to “necessity” requires additional detail or factors on how to determine what is necessary. This issue is especially pressing for Maryland’s law because it contains two different necessity standards: collecting, processing, and sharing sensitive data is tied to what is “strictly” necessary for providing or maintaining a requested product or service, whereas collecting personal data is limited to what is “reasonably necessary and proportionate” for providing a requested product or service. Distinguishing between these two standards requires establishing a baseline guiding principle as to what “necessary” means in the first place.

As practitioners wait for potential guidance on what is “necessary”—whether that comes in amendments to statutory text, through rulemaking, or in interpretive guidance by the law’s enforcers—there are other sources of law that could prove useful in the short term. For example, California’s privacy regulations provide factors as to when collection or processing aligns with individuals’ reasonable expectations. One advantage of California’s rule is that “reasonable expectations” have been a cornerstone of American privacy law for decades in the Fourth Amendment context, predating modern data privacy and data protection regimes. Such a standard therefore has an established body of law from which someone can analogize and draw useful principles, even if the criminal privacy context is not directly relevant. Similarly, the European Data Protection Board (EDPB)—an independent EU body empowered to support consistent application of the GDPR throughout the Union, promote cooperation and resolve disputes between Member State Data Protection Authorities, and issue interpretive guidance on the application of the GDPR—has issued guidance on the scope of when processing personal data is “necessary for the performance of a contract to which the data subject is party” under the GDPR.⁷¹ Some of the suggested questions from the guidance include:

- “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 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?”⁷²

⁷¹ EDPB, 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, ¶¶ 23–39 (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 (discussing how to determine what is “necessary” under GDPR Art. 6(1)(b)).

⁷² *Id.* 33.

This paper does not suggest that Maryland-style substantive data minimization requirements should be read as a 1:1 analog of the EDPB's interpretation of Article 6(1)(b), which has been described as “the narrowest possible interpretation” of contractual necessity and which does not support product improvement.⁷³ Looking to the EDPB guidance on Art. 6(1)(b) to color one's interpretation of Maryland's data minimization requirements would be a conservative, low-risk approach to compliance. An alternative option is to interpret providing or maintaining a requested product or service broadly to include activities such as advertising, the development of new products and features, and similar activities that are arguably within consumers' expectations but are not “essential” to offer a product or service. There is some textual support for this broader understanding in Maryland's law. For example, the existence of a right to opt-out of targeted advertising implies the ability to collect and process personal data for targeted advertising.

This paper highlights these EDPB factors only insofar as they can provide a useful framework for approaching compliance, even if the Maryland-style requirements ultimately are more permissive than Article 6(1)(b). Despite the conceptual similarities between Art. 6(1)(b) and Maryland's data minimization requirements, these are distinct legal regimes with different language. Thus, although these factors from EDPB guidance may prove useful in assessing what is “necessary” under these novel substantive data minimization standards, it is still imperative that regulators provide their own guidance. Until either the law is amended to provide additional clarity or the Attorney General provides guidance through FAQs or enforcement, it will be up to businesses to interpret substantive data minimization's meaning in accordance with their own risk tolerance and business needs. In the meantime, the lack of clarity in the law will foster confusion and divergent approaches, potentially underscoring the need for a comprehensive federal privacy law.

B. Policy Considerations and Possible Rule Constructions

Policymakers who are interested in enacting a substantive data minimization rule but are mindful of the practical challenges and ambiguities raised above should consider how to proactively address some of the biggest challenges posed by such a rule, including the role of consent, how advertising and selling personal data fit into the equation, and the need for flexibility to accommodate practices that are novel, socially beneficial, or low-risk. Doing so requires engaging with the interpretive questions raised above as well as longer-term policy questions, such as the role of default protections versus individual control, how to provide businesses with reasonable certainty as to permitted conduct, risks of subjective enforcement, and the role of exceptions to the law. After considering these questions, policymakers will have to decide on the appropriate mechanism in a substantive data minimization rule to build-in necessary flexibility and ensure that the rule is forward-looking.

⁷³ Eduardo Ustaran & Elizabeth Campion, *The EDPB's Narrow View of Contractual Necessity*, Hogan Lovells (Apr. 16 2019), <https://www.hoganlovells.com/en/publications/the-edpbs-narrow-view-of-contractual-necessity>; see also EDPB Guidelines, *supra* note 71, ¶¶ 48–49 (stating that Art. 6(1)(b) “would [not] generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service”).

1. Default Protections versus Individual Control

Substantive data minimization exists within a broader policy debate over the merits of “privacy-as-control.”⁷⁴ Starting first with the perspective of substantive data minimization’s proponents, this framework is intended to upend the traditional regulatory model of “privacy-as-control” and place the onus of privacy protection on the entities collecting and using personal data rather than the individuals themselves. Under that perspective, procedural data minimization is inadequate because it merely entrenches notice-and-choice, enabling companies to do whatever they want with personal data, no matter how harmful to the individual or orthogonal to the commercial relationship, so long as the business discloses what it is doing in a dense, rarely-read privacy policy.⁷⁵ This perspective arguably gives short shrift to the protections afforded by procedural data minimization. Requiring covered entities to identify categories of personal data collected and the purposes for which such data is used, and to then adhere to those disclosures or obtain opt-in consent, is a meaningful protection. Furthermore, requiring covered entities to obtain opt-in consent for processing sensitive data is an additional, heightened protection that should, if properly enforced, restrict harmful, unnecessary collection of one’s most sensitive data. Procedural data minimization rules also acknowledge that individuals’ views can differ as to whether particular data practices are harmful, benign, or desirable. Nevertheless, if one believes that procedural data minimization is overly permissive, alternative rules tied to individual expectations (e.g., the rule in the CCPA regulations) or to what is necessary to provide a specific product or service (e.g., the MODPA substantive data minimization rules) could remedy the structural power imbalance between individuals making choices in the market and the companies offering products and services on take-it-or-leave-it privacy terms.

Historically, American privacy law has championed individual control of personal data, usually in the form of actionable rights, opt-outs, and notice-and-choice. But some scholars have long argued that a control-based model is overwhelming, due to the excessive options presented to individuals, and illusory, due to the lack of meaningful choices presented.⁷⁶ One potential remedy to the overwhelming nature of privacy-as-control is to exercise rights on a default, generalized basis, such as through technical measures like universal opt-out mechanisms and preference signals.⁷⁷ Yet there is an understandable growing desire for default protections that reverse this paradigm by taking the onus off of individuals and instead limiting how data can be collected and used. This may also be true for proponents of data use who see consent requirements as unduly burdensome for some socially beneficial activities, such as collecting and processing demographic data for the purposes of testing and mitigating bias in automated systems or public

⁷⁴ For background on privacy-as-control, see Michael Birnhack, *In Defense of Privacy-As-Control (Properly Understood)*, 65 *Jurimetrics* (forthcoming 2025), <https://papers.ssrn.com/id=5042930>.

⁷⁵ See, e.g., Consumer Reps. & Elec. Priv. Info. Ctr., *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf (calling on the FTC to establish strong data minimization requirements); Null, *supra* note 3.

⁷⁶ Woodrow Hartzog, *The Case Against Idealising Control*, 4 *Euro. Data Prot. L. Rev.* 423 (2018).

⁷⁷ Samuel Adams & Stacey Gray, *Survey of Current Universal Opt-Out Mechanisms*, FPF (Oct. 12, 2023), <https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms>.

health initiatives.⁷⁸ Substantive data minimization—which includes a normative component limiting the purposes for which data can be collected or processed—is a means to that end.

From the perspective of either a covered entity or a proponent of privacy-as-control, however, there are two immediate counterarguments to this abandonment of procedural data minimization. First, substantive data minimization rules arguably remove choice from individuals and potentially deprive them of certain desired data uses and features. Privacy advocates, however, are likely to argue that individuals face little choice to begin with beyond a binary decision of whether or not to use a particular product or service and some room at the margins to exercise consumer rights. Furthermore, under a MODPA-type data minimization rule, individuals arguably can opt-in to using a particular feature, which then becomes part of the product or service being provided. Whether that is a valid reading of the MODPA—or whether that runs into a consent-trap that is simultaneously frustrating to consumers and challenging for covered entities to implement—remains to be seen.

Another control-focused counterargument is that the vagueness of a substantive data minimization rule will actually empower covered entities to collect more, rather than less, personal data. Under that interpretation, covered entities are able to decide for themselves that certain processing activities, such as targeted advertising or selling data, are “necessary” to provide a product or service because that income stream contributes to the availability of the product or service. This is reminiscent of arguments in the EU about which lawful bases can be relied upon for behavioral advertising on social media.⁷⁹ Even if covered entities interpret substantive data minimization rules this way and read the rules expansively to justify a variety of processing activities, it is unclear that this would result in more data collection than under procedural data minimization. In the status quo, covered entities can engage in any of these activities so long as they disclose such purposes in a privacy notice, which is arguably a lower bar to legitimizing these kinds of practices. For sensitive data, there is a stronger argument that a covered entity can claim that a processing purpose is “strictly necessary” whereas under a procedural rule the entity would be required to obtain opt-in consent for processing. One alternative remedy to this problem is to include specific prohibitions and sub-rules (e.g., the MODPA’s ban on selling sensitive data), opt-in or opt-out rights, or a clear statement in law that specific activities are not reasonably or strictly necessary to provide or maintain a product or service. Taking that approach, however, risks adding to the complexity of the law and requiring constant updates to respond to emerging practices.

⁷⁸ See Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 261 (2013) (“[C]ollective action problems threaten to generate a suboptimal equilibrium where individuals fail to opt into societally beneficial data processing in the hope of free-riding on others’ good will.”).

⁷⁹ Vincent Manancourt, *€390M Fine Strikes Blow to Meta’s Ad-Fueled Business Model*, Politico (Jan. 4, 2023), <https://www.politico.eu/article/meta-fine-ad-business-model>.

2. Reasonable Certainty and Socially-beneficial Secondary Uses

Substantive data minimization creates a risk that businesses will not have reasonable certainty about permissible practices, impeding legitimate activity and penalizing cautious actors who try to comply with the spirit of the law. In particular, substantive data minimization could forbid processing activities that are outside of an individual's reasonable expectations based on the product or service requested by them but which nonetheless are socially-beneficial. Examples of these kinds of secondary uses include product development, launching of new features, and, critically, AI development.

As discussed above, there are several critical ambiguities that must be addressed in a substantive data minimization rule tied to providing or maintaining a product or service: What makes something 'reasonably' or 'strictly' necessary? What does it mean to provide or maintain a product or service? What does it mean for a product or service to be 'specifically requested' by an individual? Are things that we would consider legitimate business needs—such as fraud prevention, IT security, retaining log-in details, content moderation, etc.—implicitly allowed as reasonably necessary to provide or maintain a product or service?⁸⁰ If collecting and processing sensitive data is limited to what is strictly necessary to provide a product or service, would it be possible for businesses to process biometric information to verify customers? If so, can it be mandatory for the product or must customers opt-in to that feature? At the end of the day, pivoting from procedural to substantive rules raises broader questions as to profitability and the legality of different business models. What role is maintaining a certain level of profitability relevant to necessity? If restricting certain data collection or processing means that the service can be provided but at a different profit level, is it obligatory to operate on the minimum viable level? These are the questions which a substantive data minimization rule must address.

Looking at other substantive data minimization iterations other than the MODPA, the approaches taken in ADPPA and APRA raise their own unique ambiguities and trade-offs. Creating a list of permitted purposes for which covered entities can collect, process, and transfer personal data should be more forward looking, flexible, and ease objections about foreclosing legitimate business practices.⁸¹ Yet an enumerated "permitted purposes" approach could become ossified and under-inclusive if the law is not updated in response to emerging business needs.⁸² Policymakers could instead consider a more flexible 'legitimate interests' balancing test as an

⁸⁰ GDPR art. 6(1)(f); EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Oct. 9, 2024), https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en.

⁸¹ *Supra* Part I.C.2.

⁸² Joseph Jerome, *Can the American Privacy Rights Act Accomplish Data Minimization?*, Tech Policy Press (Apr. 11, 2024), <https://www.techpolicy.press/can-the-american-privacy-rights-act-accomplish-data-minimization> (noting that the permitted purpose approach in APRA could be "much less flexible for industry.").

alternative,⁸³ but that approach has its own challenges.⁸⁴ From a covered entity's perspective, it creates another uncertainty trap. From an privacy advocacy perspective, it creates a risk of being the exception that swallows the rule.⁸⁵

To be workable, therefore, a substantive data minimization rule must, at a minimum, anticipate and carve-out legitimate, socially-beneficial activities and low-risk activities that are critical for routine business activities. Such processing purposes could be implicitly read as being necessary to provide or maintain a product, they could be enumerated in a list, or they could be covered by a catch-all balancing test that weighs an activity's benefits against its risks of harm to consumers, such as the FTC's traditional approach to unfairness or the GDPR's legitimate interests balancing test. Each approach has its own trade-offs.

3. Subjectivity versus Objectivity

Another potential objection against substantive data minimization from a covered entity's perspective is that these "necessity" standards will allow enforcers to second-guess a covered entity's decisions in that a regulator is free to investigate a covered entity and, at any time, decide that collection or use of personal data was not necessary to provide or maintain a product of service. Under this theory, substantive data minimization is "subjective" whereas procedural data minimization is "objective." This argument likely overstates the difference between the two rules. Under the procedural data minimization standard, controllers have significant power to decide for themselves what uses of personal data are legal because legality is tied to the disclosures they make. Despite that rule clearly favoring a covered entity's ability to decide for itself what uses of personal data are necessary, it is not unlimited. Enforcers still have some leeway to "second-guess" whether processing activities are beyond the bounds of what was disclosed, because the procedural data minimization rule still has its own "subjective" elements: Collection is tied "to what is adequate, relevant and reasonably necessary in relation to the [disclosed] purposes"; and secondary uses "that are neither reasonably necessary to, nor compatible with, the disclosed purposes" are prohibited unless the controller obtains consent. Thus, while a substantive data minimization rule could increase the risk of subjective enforcement, that may be a difference of degree rather than kind.

4. Interplay with the Law's Exemptions

The turn from procedural to substantive data minimization rules will increase scrutiny on a law's exemptions, exceptions, or lack thereof. For example, narrowing the purposes for which covered

⁸³ This approach could be rooted in existing American legal concepts, such as the FTC Act's unfairness test, which considers whether an act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

⁸⁴ *Id.*

⁸⁵ Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687, 1724 (2020) (arguing that legitimate interests "seems to be largely focused on the business and operational interests of the data processor and the rights of and fairness to the data subject").

entities can collect and process personal data or sensitive data may inadvertently encourage covered entities to adopt more expansive readings of the law's exemptions and exceptions. For exemptions to the law, this is consequential for consumers because if a controller adopts a more aggressive interpretation of one of the law's exemptions, then that data or activity could be exempted from the law entirely, potentially leaving the consumer without any legal protections. Increased reliance on the law's exceptions, however, is less likely to pose risk to consumers as the laws' exceptions typically include requirements such as adherence to reasonable data security practices.⁸⁶

Substantive data minimization may also make the absence of certain exceptions more acute. For example, the Maryland Online Data Privacy Act does not include the exception commonly seen in other state comprehensive privacy laws allowing a controller to “engage in public or peer-reviewed scientific or statistical research in the public interest” in accordance with certain safeguards.⁸⁷ The absence of this exception, when coupled with the law's “strictly necessary” requirement for collecting, processing, or sharing sensitive data, could have serious downstream implications for socially beneficial research. Policymakers should consider addressing—either through enumerated exceptions, permitted purposes, or guiding factors—what kinds of commonplace, reasonably expected business practices like product improvement or data sharing with academic researchers fall within the scope of reasonably or strictly necessary to provide or maintain a requested product or service.

5. Options for Constructing a Substantive Data Minimization Rule

After identifying relevant policy tradeoffs and potential solutions to operational difficulties comes the difficult task of constructing an effective substantive data minimization rule. As the table of substantive data minimization proposals in Part I.C.2 above demonstrated, there are a variety of ways to construct a substantive data minimization rule, blending “necessity,” “consent,” and “permitted purpose” requirements. The following exercise explores several options for constructing a substantive data minimization rule if that is the desired course of action.

Assume that one's goal is to limit the collection, processing, maintenance, and disclosure of [personal / sensitive] data to what is [reasonably / strictly] necessary to provide or maintain a requested product or service. For this hypothetical, ignore ambiguity surrounding the meaning of a “requested” product or service. Further assume that one wants to provide reasonable flexibility to businesses to engage low-risk, socially beneficial activities such as product improvement, preventing or responding to security incidents, public interest research, and so forth. There are a variety of ways to approach this in crafting the data minimization (i.e., permissible processing) rule. At its core, this data minimization rule will include two parts: the general rule (rule 1), and the qualifiers/exceptions (rule 2).

⁸⁶ *E.g.*, Conn. Gen. Stat. § 42-524 (2024); Tex. Bus. & Com. Code Ann. § 541.204 (2024)

⁸⁷ *E.g.*, Conn. Gen. Stat. § 42-524(a)(10) (2024).

Rule 1

- A covered entity must:
 - Limit the [collection / processing / disclosure] of
 - [personal / sensitive] data to what is
 - [reasonably necessary and proportionate / necessary / strictly necessary]
 - to provide or maintain
 - a [specific] product or service
 - requested by the individual to whom the [personal / sensitive] data relates;

Rule 2

- **Option 2.1: Flexible Interpretation**
 - **Description:** The simplest option is to interpret the rule expansively, reading “requested” and “necessary” permissively so as to allow many desirable activities that are only indirectly related to running the business, or support broader, legitimate business activities.
 - **Potential Issues:** This option creates regulatory uncertainty for covered entities as it is not immediately clear what activities are within scope. It is also potentially less protective for consumers, as covered entities are incentivized to read the rule as capaciously as possible until told otherwise by a regulator.
 - **Potential Fixes:** The rule could be tied to consumers’ “reasonable expectations,” as in Cal. Code. Reg. tit. 11, § 7002, subd. (b).⁸⁸ The inclusion of additional factors such as these could bolster interpretation and provide more upfront clarity as to activities that are within scope.
- **Option 2.2: Exceptions or Permitted Purposes**
 - **Description:** State comprehensive privacy laws typically include a list of activities for which the law is not intended to restrict a covered entity’s ability to engage. *E.g.*, Conn. Gen. Stat. § 42-524 (2024). These exceptions could also be reframed as permitted purposes. *E.g.*, the American Data Privacy and Protection Act.⁸⁹
 - **Potential Issues:** This approach creates a “whack-a-mole” problem in that it requires updating those exceptions as business practices or policy priorities evolve.
 - **Potential Fixes:** A list of permitted purposes could include a catch-all for “similar” activities, or a narrow grant of rulemaking authority for a regulator (*e.g.*, the Federal Trade Commission for federal legislation or the Attorney General for state legislation) to add new exceptions over time.

⁸⁸ Privacy advocates have previously highlighted § 7002’s potential value as “instructive for properly framing a reasonable consumer expectation standard.” *E.g.*, Suzanne Bernstein, *Data Minimization: Centering Reasonable Consumer Expectation in the FTC’s Commercial Surveillance Rulemaking*, EPIC (Apr. 20, 2023), <https://epic.org/data-minimization-centering-reasonable-consumer-expectation-in-the-ftcs-commercial-surveillance-rulemaking>.

⁸⁹ H.R. 8152, 117th Cong. § 101(b) (2022) (version Dec. 30, 2022).

- **Option 2.3: Fairness or Legitimate Interests**

- **Description:** Rather than relying on a list of enumerated exceptions or permitted purposes, the law could include a broad, general catch-all “unfairness” or “legitimate interests” style balancing test that allows for the [collection / processing / disclosure] of [personal / sensitive] data with appropriate safeguards. E.g., 15 U.S.C. § 45(n); GDPR art. 6(1)(f).
- **Potential Issues:** This option again creates regulatory uncertainty, this time around the bounds of “legitimate interests” rather than what is “necessary.” It also risks being less protective for consumers if interpreted expansively or overrelied upon.
- **Potential Fixes:** Incorporating an “unfairness” standard would not require drawing on a blank canvas. Rather, the concept is bounded by a long history of FTC and Attorney General enforcement and interpretations of harm.

- **Option 2.4: Consent**

- **Description:** Covered entities could be required to obtain affirmative, opt-in consent for all processing activities that do not fall within the bounds of what is necessary to provide the product or service. E.g., Washington’s My Health My Data Act.⁹⁰
- **Potential Issues:** Obtaining meaningful consent is challenging by design, and requiring covered entities to do so for certain activities, such as fraud prevention, may be unduly burdensome.
- **Potential Fixes:** A consent requirement could be paired with one of the other options highlighted above (a flexible interpretation, enumerated exceptions, or a legitimate interest provision). E.g., New York Child Data Protection Act.⁹¹

Regardless of which approach a policymaker takes, it is imperative that they understand how the aspects of the rule fit together, alongside any other relevant exemptions or exceptions in the law, to impact the use of personal data in the economy. There are tensions and tradeoffs between these rules, and policymakers’ choice of model will have broad consequences for individuals and for companies subject to these laws.⁹²

⁹⁰ Wash. Rev. Code § 19.373.030 (2024).

⁹¹ N.Y. Gen. Bus. Code § 899-ff(1)–(2) (2024) (providing a broad set of permitted purposes in addition to consent and provision of a requested product or service).

⁹² See, e.g., Stacey Gray et al., *[Draft] Advertising in the Age of Data Protection: Background for a Proposed Risk-Utility Framework for Novel Advertising Solutions (v 1.0)*, FPF (Apr. 1, 2024), <https://fpf.org/wp-content/uploads/2024/04/FPF-Proposed-Advertising-Risk-Utility-Framework-April-2024-v1.0.pdf> (discussing tradeoffs in the digital advertising policy space).

Conclusion

The legislative turn towards substantive data minimization rules is an important development in the ongoing debate over the merits of privacy-as-control. Advocates and scholars alike have long lamented the notice-and-choice approach to privacy, which legitimizes most collection, processing, and sharing of personal data so long as those activities are adequately disclosed. Others have also criticized the status quo for an overreliance on consent where the underlying activity is socially beneficial and where consent may be a barrier, such as collecting and processing demographic data for the purposes of testing and mitigating bias in automated systems.⁹³ Under that perspective, substantive data minimization rules could be a welcome relief for covered entities who find opt-in consent requirements for sensitive data use to be overly burdensome. Regardless of who is criticizing procedural data minimization and for what reasons, it is evident that policymakers are listening. While laws like the Maryland Online Data Privacy Act, the Washington My Health My Data Act, and the New York Child Data Protection Act all break new ground with their substantive data minimization requirements, it remains to be seen whether other states will follow suit or if this is a brief legislative blip. Even if other states follow, however, the proof of the pudding is in the eating. We will not know whether substantive data minimization truly offers a paradigm-shift until these requirements go into effect and are publicly enforced.

If you have any questions, please contact us at info@fpf.org.

Disclaimer: This white paper is for informational purposes only and should not be used as legal advice.

⁹³ See Arushi Gupta, Victor Y. Wu, Helen Webley-Brown, Jennifer King & Daniel E. Ho, *The Privacy-Bias Tradeoff: Data Minimization and Racial Disparity Assessments in U.S. Government*, FAcCT '23, https://hai-production.s3.amazonaws.com/files/2023-06/Gupta_et_al_Privacy_Bias.pdf; Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 259–60 (2013).

Appendix

Table 1. Select Substantive Data Minimization Requirements in Proposed and Enacted Privacy Legislation, 2022–25.

Bill / Law	Requirements
<p>American Data Privacy and Protection Act (ADPPA), H.R. 8152</p> <p>(proposed 2022)</p> <p>Type: Comprehensive Consumer Privacy</p>	<p>Arguably the precipitating action for this legislative trend, the ADPPA introduced the “reasonably necessary” and “strictly necessary” two-tier framework for personal data and sensitive data:</p> <p>“In general.—A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to—</p> <ul style="list-style-type: none"> (1) provide or maintain a specific product or service requested by the individual to whom the data pertains; or (2) effect a purpose permitted under subsection (b) [note: the bill included 17 permitted purposes]. <p>...</p> <p>[U]nless an exception applies, with respect to covered data, a covered entity or service provider may not—</p> <ul style="list-style-type: none"> (2) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains, or is strictly necessary to effect [a limited number of the bill’s “permitted purposes”]; (3) transfer an individual’s sensitive covered data to a third party, unless [certain conditions are met; . . .]”⁹⁴ <p>Rule Subtype: Necessity or Permitted Purposes</p>
<p>American Privacy Rights Act (APRA), H.R. 8818</p> <p>(proposed 2024)</p> <p>Type: Comprehensive Consumer Privacy</p>	<p>“(a) In general.—A covered entity may not collect, process, retain, or transfer covered data of an individual or direct a service provider to collect, process, retain, or transfer covered data of an individual beyond what is necessary, proportionate, and limited—</p> <ul style="list-style-type: none"> (1) to provide or maintain— <ul style="list-style-type: none"> (A) a specific product or service requested by the individual to whom the data pertains, including any associated routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting; or (B) a communication, that is not an advertisement, by the covered entity to the individual reasonably anticipated within the context of the relationship; or

⁹⁴ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 101–102 (2022) (version Dec. 30, 2022).

Bill / Law	Requirements
	<p>(2) for a purpose expressly permitted under subsection (d) [note: there are 17 permitted purposes].</p> <p>(b) Additional protections for sensitive covered data.—Subject to subsection (a), a covered entity may not transfer sensitive covered data to a third party or direct a service provider to transfer sensitive covered data to a third party without the affirmative express consent of the individual to whom such data pertains, unless for [a limited number of permitted purposes].”⁹⁵</p> <p>The bill included additional protections for biometric information and genetic information.</p> <p>Rule Subtype: Necessity or Permitted Purpose [and Consent, for Sensitive Data]</p>
<p>Washington My Health My Data (MHMD) Act, Wash. Rev. Code tit. 19, ch. 373</p> <p>(enacted 2023)</p> <p>Type: Health Privacy</p>	<p>“[A] regulated entity or a small business may not collect any consumer health data except:</p> <p>(i) With consent from the consumer for such collection for a specified purpose; or</p> <p>(ii) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.</p> <p>(b) A regulated entity or a small business may not share any consumer health data except:</p> <p>(i) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect consumer health data; or</p> <p>(ii) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.”⁹⁶</p> <p>There is an additional, heightened “valid authorization” requirement for selling regulated health information.</p> <p>Rule Subtype: Necessity or Consent</p>
<p>New York Child Data Protection Act, N.Y. Gen. Bus. Law §§ 899-ee et seq.</p> <p>(enacted 2024; guidance issued 2025)</p>	<p>“1. . . . [A]n operator shall not process, or allow a processor to process, the personal data of a covered user collected through the use of a website, online service, online application, mobile application, or connected device, or allow a third-party operator to collect the personal data of a covered user collected through the operator’s website, online service, online</p>

⁹⁵ American Privacy Rights Act, H.R. 8818, 118th Cong. §§ 101–102 (2022) (version June 25, 2024).

⁹⁶ Wash. Rev. Code § 19.373.030 (2024). For more on MHMD’s “necessary” requirement, see 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>.

Bill / Law	Requirements
<p>Type: Youth Privacy</p>	<p>application, mobile application, or connected device unless and to the extent:</p> <p>...</p> <p>(b) the covered user is thirteen years of age or older and processing is strictly necessary for an activity set forth in subdivision two of this section, or informed consent has been obtained as set forth in subdivision three of this section.</p> <p>2. For the purposes of paragraph (b) of subdivision one of this section, the processing of personal data of a covered user is permissible where it is strictly necessary for the following permissible purposes:</p> <p>(a) providing or maintaining a specific product or service requested by the covered user;</p> <p>(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;</p> <p>(c) identifying and repairing technical errors that impair existing or intended functionality;</p> <p>(d) protecting against malicious, fraudulent, or illegal activity;</p> <p>(e) investigating, establishing, exercising, preparing for, or defending legal claims;</p> <p>(f) complying with federal, state, or local laws, rules, or regulations;</p> <p>(g) complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;</p> <p>(h) detecting, responding to, or preventing security incidents or threats;</p> <p>or</p> <p>(i) protecting the vital interests of a natural person.”⁹⁷</p> <p>Rule Subtype: Necessity or Consent or Permitted Purposes</p>
<p>The Connecticut Data Privacy Act (as amended by SB 3)⁹⁸</p> <p>(amended 2023)</p> <p>Type: Youth Privacy</p>	<p>“(b) (1) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall:</p> <p>(A) Process any minor's personal data</p> <p>...</p> <p>(ii) unless such processing is reasonably necessary to provide such online service, product or feature,</p> <p>(iii) for any processing purpose</p>

⁹⁷ N.Y. Gen. Bus. Code § 899-ff(1)–(2) (2024).

⁹⁸ Conn. Gen. Stat. §§ 42-529 *et seq.* (2024).

Bill / Law	Requirements
	<p>(l) other than the processing purpose that the controller disclosed at the time such controller collected such personal data, or</p> <p>(ll) that is reasonably necessary for, and compatible with, the processing purpose described in subparagraph (A)(iii)(l) of this subdivision, or</p> <p>(iv) for longer than is reasonably necessary to provide such online service, product or feature; . . . ”⁹⁹</p> <p>Similar provisions exist in Colorado’s and Virginia’s amended comprehensive consumer privacy laws.¹⁰⁰</p> <p>Rule Subtype: Necessity or Consent</p>
<p>California Age-Appropriate Design Code Act, Cal. Civ. Code §§ 1798.99.28 <i>et seq.</i></p> <p>(enacted 2022; currently enjoined)</p> <p>Type: Youth Privacy</p>	<p>“A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:</p> <p>...</p> <p>(2) Profile a child by default unless both of the following criteria are met:</p> <p>...</p> <p>(B) Either of the following is true:</p> <p>(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged.</p> <p>(ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.</p> <p>(3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children likely to access the online service, product, or feature.</p> <p>...</p> <p>(5) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.</p> <p>...</p>

⁹⁹ *Id.* § 42-529a(b).

¹⁰⁰ Colo. Code. Rev. § 6-1-1308.5(2)(a)(II) & (III) (2025) (slightly narrower than Connecticut’s language); Va. Code Ann. § 59.1-578(F).

Bill / Law	Requirements
	<p>(7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child’s physical health, mental health, or well-being.”¹⁰¹</p> <p>Rule Subtype: Necessity</p>

¹⁰¹ Cal. Civ. Code § 1798.99.31, subd. (b) (2025).



1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org