August 28, 2025

Cari Fais, Acting Director
New Jersey Division of Consumer Affairs
124 Halsey Street
PO Box 45027
Newark, NJ 07101

RE: Proposed rules to implement the New Jersey Data Privacy Act

Dear Acting Director Fais,

Thank you for your ongoing work and the opportunity to comment regarding draft regulations for implementing the New Jersey Data Privacy Act ("NJDPA").[1] The Future of Privacy Forum ("FPF") is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.[2] In response to the Agency's public comment on the proposed rules, FPF recommends that the Division consider the following:

I. Clarifying and aligning definitions of key terms with comparable state privacy laws where appropriate;
II. Ensuring that consumer controls and opt-out rights operate as expected to adequately enable consumer choice;
III. Considering where consumer rights requirements can be adjusted to promote socially beneficial activities, such as bias testing, or provide additional flexibility in light of technical and administrative challenges; and
IV. Leverage existing business practices and standards set by comparable state privacy laws in setting requirements for data protection impact assessments.

I. Definitions

A. Consider clarifying the "scraping" exemption from the definition of "publicly available information"

Like many comprehensive and sectoral U.S. privacy laws, the NJDPA exempts "publicly available information" from coverage.[3] However, the draft regulations propose narrowing the scope of public data by excluding "the ***scraping*** of personal data or personal data obtained from data

[1] Press release, N.J. Div. Consumer Affairs, Murphy Administration Announces Proposed Rules Establishing Comprehensive Consumer Data Privacy Protections, (June 2, 2025), https://www.njconsumeraffairs.gov/News/Pages/06022025.aspx.
[2] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.
[3] Jordan Francis, Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends at 8 (Nov. 2025), https://papers.ssrn.com/abstract_id=5309115.

brokers that is not publicly available"[4] without providing a definition of "scraping." As described in recent case law and scholarship, "scraping" could include a wide range of practices, from automated bots indexing public web content to manual copying of data for research purposes.[5] Without a clearly articulated, commonly accepted definition, the current draft rules present a risk that many socially beneficial activities—including routine web indexing, journalist investigations, or civil rights audits—using publicly accessible data could be unintentionally swept into the scope of the NJDPA and curtailed.

Developing a clear definition of scraping is challenging, as the case law regarding the bounds of permissible versus unlawful scraping is not settled. However, limiting the collection and use of publicly available information exacerbates the risk of First Amendment challenges to the final regulations. For example, in *Sandvig v. Sessions*, the United States District Court for the District of Columbia acknowledged that scraping may be necessary for academic research or civil rights auditing, suggesting that prohibiting such activity could chill constitutionally protected speech.[6]

Given the still-developing legal landscape of scraping and the fact that scraping was not a specific issue contemplated by the legislature in drafting the NJDPA, the Division may consider a range of possible resolutions:

1. **Removal:** Removing this proposed addition from the definition of "publicly available information" would align New Jersey with other state comprehensive privacy laws, creating more interoperability for interstate businesses.
2. **Narrowed Scope:** Rather than excluding all scraped data from the definition of "publicly available information," the regulations could focus on higher-risk scraping practices, such as the collection of public data for biometric profiling, which often involves sensitive data and greater privacy risks. For example, this has been accomplished in the California and Connecticut privacy laws, as well as Texas' newest AI law, by clarifying that publicly available information "does not mean biometric information collected by a business without the consumer's knowledge."[7]
3. **Defined Term:** At a minimum, defining the term "scraping" is necessary for business compliance with the law.

B. Consider clarifying the scope of"data brokers" to align with frameworks found in other state privacy laws

As currently drafted, the proposed regulations would introduce obligations specific to "data brokers" that are not found in the underlying law, defined as anyone who "collects, purchases, or

[4] Draft N.J.A.C. 13:45L-1.2 (emphasis added).
[5] Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clashing Between Scraping and Privacy,* 113 Calif. L. Rev. 7-8 (2024) (discussing scraping definition and use).
[6] Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018). https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2016cv01368/180080/67/
[7] Cal. Civ. Code § 1798.140, subd. (v)(2)(ii) (2025); *accord* S.B. 1295, Public Act No. 25-113, 2025 Reg. Sess. (Conn. 2025), Sec. 5 (amending the Connecticut Data Privacy Act (CTDPA)); Texas Responsible Artificial Intelligence Governance Act, H.B. No. 149, 2025 Reg. Sess. (Tex. 2025).

sells to third parties" the data of consumers with whom they do not have a direct relationship.[8] While the draft regulations appear designed to target what are commonly understood as data broker practices (e.g., selling marketing lists or profiling individuals for targeted advertising), they may also inadvertently encompass socially beneficial or routine practices that are expressly exempt under other analogous laws.

For example, Vermont's data broker registration law, from which the draft regulations appear to draw, includes exemptions not included in the proposed regulations here.[9]

New Jersey Proposed Language	Vermont Current Language
"Data broker" means a person or legal entity, including a controller, that knowingly collects, purchases, or sells to third parties the personal data of a consumer with whom the person or legal entity does not have a direct relationship. Examples of a direct relationship include if the consumer is a past or present: 1. Customer, client, subscriber, or user of the person or legal entity's goods or services; 2. Employee, contractor, or agent of the person or legal entity; 3. Investor in the person or legal entity; or 4. Donor to the person or legal entity.[10]	(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. (B) Examples of a direct relationship with a business include if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business's goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business. (C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker: (i) developing or maintaining third-party e-commerce or application platforms; (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (iii) providing publicly available information related to a consumer's business or profession; or (iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes. (D) The phrase "sells or licenses" does not include: (i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or (ii) a sale or license of data that is merely incidental to the business.[11]

[8] Draft N.J.A.C. 13:45L-1.2.
[9] *See* Vt. Stat. Ann. tit. 9, § 2430.
[10] Draft N.J.A.C. 13:45L-1.2.
[11] Vt. Stat. Ann. tit. 9, § 2430.

Beyond Vermont, more recent data broker laws, such as the ones in Texas and Oregon, include exemptions for service providers acting on behalf of a controller, health care entities under HIPAA, entities regulated by GLBA, and entities handling data in employment or commercial contexts.[12] The Division's draft definition of "data broker" is significantly broader than most comparable state laws, as it would extend to businesses that only *collect* data of a consumer with whom the business does not have a direct relationship, rather than *collect and sell or license to third parties* such data, as is the case in Vermont, meaning that controllers that do not "broker" personal information could still be treated as "data brokers" under the NJDPA.

Additionally, the breadth of the data broker definition means that entities that compile and analyze publicly accessible data without a direct consumer relationship could be inadvertently treated as data brokers, even for uses such as academic research, journalism, or civil rights auditing.

C. Under the definition of "sensitive data," consider clarifying"financial information"

Unlike other data privacy laws, the draft regulations could be construed as leaving the scope of "financial information" open-ended, which would create uncertainty as to what qualifies as sensitive information. As written, the statute states that financial information "*shall include* a consumer's account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account."[13] However, the phrase"which shall include" could suggest that this list is non-exhaustive and there may be potentially other types of financial information that should be considered as sensitive data. Such an open-ended approach could be overly broad and create business and consumer confusion, given that financial information commonly includes other information beyond account credentials.[14] For example, a broad interpretation of "financial information" could include a record of whether a customer chooses to pay with cash or card, which could prompt a disruptive and necessary consent requirement at checkout.

To promote clarity and consistency, the Division may consider clarifying that the examples provided in the definition of "financial information" represent a closed-list definition or otherwise provide guidance on how to evaluate whether sensitive data will be treated as financial information under the NJDPA. In doing so, the Division may look to the privacy laws in California and Connecticut, which both clearly define the types of information that will be treated as sensitive financial information. The California Consumer Privacy Act defines "sensitive information" *to include* "Personal information that reveals: . . . A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or

[12] Tex. Bus. & Com. Code Ann. §§ 509.002–509.003; Or. Rev. Stat. § 646A.593.
[13] N.J.S.A. 56:8-166.4.
[14] For example, the federal Gramm-Leach-Bliley Act Privacy Rule defines "personally identifiable financial information" to mean any information that a consumer provides to a financial institution to obtain a product or service from it, information about a consumer "resulting from any transaction involving a financial product or service between [the financial institution] and a consumer," or any information a financial institution "otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer." 13 C.F.R. § 313.3(o) (2024).

access code, password, or credentials allowing access to an account."[15] Furthermore, Connecticut recently amended its comprehensive privacy law to state that "sensitive data" *means* "a consumer's financial account number, financial account log-in information or credit card or debit card number that, in combination with any required access or security code, password or credential, would allow access to a consumer's financial account."[16]

D. Consider maintaining the New Jersey Privacy Act's definition of biometric data

The NJDPA's current definition of "biometric data" generally aligns with comparable state privacy laws by encompassing information that is **"*used or intended to be used*"** for identification of a specific individual (emphasis added).[17] The proposed regulations would depart from this statutory definition and significantly expand the definition of "biometric data" under the NJDPA by bringing into scope data generated from photographs or recordings that "***relates to*** a specific individual's biological, physical, or behavioral characteristics" (emphasis added).[18]

Although there is some nuance between jurisdictions, the focus on information that identifies, or in some cases, is intended to identify, a specific individual is considered a key component of what makes something "biometric information."[19] The proposed "relates to" language would significantly expand this understanding of biometric data, and in the context of photos, could implicate any individual who appears in a photo, even just partially. From an operational standpoint, this could result in the unintended limitation of other computer vision technologies that do not collect personally identifiable information, like detection (e.g., "is there a face in this photo" for photo filters) or characterization (e.g., "what is the skin tone of this person in the photo" to adjust lighting for cameras). It also may conversely require businesses to collect personal information for non-users. In *Zellmer v. Meta Platforms*, an individual filed a lawsuit under the Illinois Biometric Information Privacy Act ("BIPA") after his photo was uploaded to Facebook (Meta), alleging that Facebook captured his biometric identifiers.[20] In siding with Meta, the United States Court of Appeals for the Ninth Circuit relied on a declaration from a product manager that it would be impossible to identify a non-user of Facebook in a photo. While a unique "face signature" was collected (and thus could have been considered "data that relates to" under the draft regulations), it was not one that could identify the plaintiff, and thus not a biometric identifier for purposes of BIPA.

While New Jersey properly considers biometric data sensitive and thus subject to heightened protections, this proposed language would make it challenging for a covered business to collect

---

[15] Cal. Civ. Code § 1798.140, subd. (ae).
[16] S.B. 1295, Public Act No. 25-113, 2025 Reg. Sess. (Conn. 2025), Sec. 5 (amending the Connecticut Data Privacy Act (CTDPA)).
[17] N.J.S.A. 56:8-166.4. *See generally* Jordan Francis, Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends at 8, 23–24, 23–30, 36 (Nov. 2025) https://papers.ssrn.com/abstract_id=5309115 (discussing the regulation of biometric data under state privacy laws).
[18] Draft N.J.A.C. 13:45L-1.2.
[19] *See* Tatiana Rice, *When is a Biometric No Longer a Biometric?*, FPF (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric.
[20] Zellmer v. Meta Platforms, Inc., 104 F. 4th 1117 (9th Cir. 2024).

consent for any bystander in the background of a photograph that is not the consumer with which a covered business is interacting with. While bystander privacy is an important issue, it may be more prudent to let the existing definition of the statute remain unaltered.

E. Consider defining and clarifying "artificial intelligence" under the "internal research" exception

As currently drafted, the regulations would modify the NJDPA's exception for "internal research to develop, improve, or repair products, services, or technology" to exclude the use of personal data for training artificial intelligence ("AI") systems unless the consumer has affirmatively consented.[21] This would introduce a novel requirement for businesses operating in New Jersey, as most U.S. state privacy laws address personal data use, profiling, or automated decision-making more broadly, without specifically identifying "AI training" as a distinct category or technology requiring affirmative consent.

If the Division proceeds to modify the "internal research" exception, we strongly urge that, at a minimum, the Division should define the term "artificial intelligence."[22] Requiring controllers to obtain affirmative consent for using personal data to train AI, without defining it, introduces significant ambiguity. Many controllers have built their privacy compliance programs around more clearly scoped, commonly accepted, technology-neutral terms used in comparable consumer privacy laws, such as "automated decision-making" and "profiling." It is unclear whether "artificial intelligence" is intended to include, overlap with, or go beyond those concepts. The absence of a definition risks inconsistent interpretations and makes it difficult for businesses to determine which technologies, models, or practices the provision applies to. Providing a clear definition—or aligning the terminology with established concepts—would help facilitate compliance, reduce uncertainty, and ensure consumers' rights are meaningfully protected.

Moreover, subsection (ii) of the exception does not follow the structure of subsection (i) regarding data sharing for research, which incorporates the exemptions for (1) de-identified data, and (2) uses consistent with subsection (c), such as compliance with law, security and fraud detection, product functionality, and public interest research. As currently written, subsection (ii) prohibits the undisclosed use of personal data to train AI without affirmative consent, but does not include exceptions for de-identified data or internal uses consistent with (c).

This creates ambiguity for controllers using machine learning for internal research and development, where continual data ingestion is essential to model performance and improvement. While subsection (i) permits the sharing of data when it is de-identified or used for a permitted purpose, subsection (ii) could be interpreted as prohibiting AI training altogether, even when those same conditions are met. These limitations create significant challenges for common and legitimate uses that rely on continuous data input to improve performance—a core

[21] Draft N.J.A.C. 13:45L-1.3(d).

[22] A majority of U.S. state laws and regulations utilize the Organization for Economic Cooperation and Development's (OECD) definition of artificial intelligence: "A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

part of many expected product features, such as fraud detection, recommendation engines, or personalization. For example, a user of video or audio media platforms may reasonably expect the service to improve its recommendations over time based on prior interactions—an improvement that typically involves AI training and internal machine learning processes. Consumer-facing financial platforms may use de-identified transaction data to train fraud detection models. Requiring affirmative consent for every form of model development or tuning may go beyond the reasonable expectations of consumers and introduce unnecessary friction into practices that are privacy protective, beneficial to consumers, and widely accepted across industries.

II. Consumer Controls and Opt-Out Rights

A. Distinguish between consumer deletion rights and opt-out mechanisms

The NJDPA empowers users in two primary ways. First, it provides a set of consumer controls which includes the rights to (1) confirm whether processing is taking place, (2) access such data, (3) correct inaccurate data, (4) delete personal data, and (5) receive such data in a portable format.[23] Second, the NJPA creates consumer rights to opt out of the processing of personal data for three *specific* purposes: (1) targeted advertising, (2) data sales, and (3) profiling in furtherance of certain significant decisions.[24] In order to maintain the efficacy of these rights and controls, the Division should ensure that its draft regulations clearly distinguish between mechanisms for consumers to opt out of certain practices and their right to delete personal data–each of which carries a distinct consumer purpose and framework for compliance.

Specifically, the draft regulations appear to establish a new requirement that, in response to an *opt-out* request, a covered business must *delete* any underlying personal data that is processed for an opt-out purpose (e.g., sales, targeted advertising, certain profiling decisions).[25] We note that the same personal data subject to an opt-out right (such as processing a consumer's name and contact information to facilitate targeted advertising) may also be necessary to sustain an account, deliver products, or provide a service. Therefore, under the novel combination opt-out/deletion request contemplated in the draft regulations, a consumer who exercises an opt-out right may unexpectedly cause the deletion of their personal data, resulting in interference or interruptions with the core services that they are intentionally using.

To avoid business and consumer confusion, and potentially inadvertent loss of access to services for consumers, the Division should empower consumers to delete their personal data through the established "right to delete" under the NJDPA and avoid conflating this control with other data subject rights, such as opt-outs.

B. Clarify the role of authorized agents

[23] N.J.S.A. C.56:8-166.10(a).
[24] *Id.*
[25] Draft N.J.A.C. 13:45L-3.4(a)2.

The NJDPA states that a person can serve as an authorized agent to "opt out of the *processing* (emphasis added) and sale of the consumer's personal data."[26] This provision is ambiguous because while the NJDPA creates a right to opt out of certain processing activities (data sales, targeted advertising, and some profiling), it does not create a generalized right to opt out of processing personal data separate from the right to delete. The statute separately provides that an individual may designate an authorized agent "using technology" to opt out of the "collection and processing for the purpose of any sale of data or for the purpose of targeted advertising,"[27] which is more closely tied to established opt-out rights.

Despite ambiguity in the statutory text, the overall intent of the NJDPA appears to be allowing authorized agents to exercise statutory *opt-out rights* on behalf of consumers, rather than broader consumer controls such as accessing, correcting, and deleting personal data. This approach would be consistent with the majority of state privacy laws that provide for authorized agents to exercise opt-out rights under the state law.[28] States have largely followed this approach because the risk of third parties exercising opt-out rights (e.g., losing access to potentially desired targeted ads) is lower than the risk of third parties exercising the data rights of access, correction, and deletion, which can lead to account compromises, data breaches, and data loss.[29]

The draft regulations raise an internal inconsistency as to which rights authorized agents may exercise on behalf of consumers. On one hand, there is language in the draft regulations suggesting that authorized agents are only intended to exercise statutory opt-out rights. This includes the summary of the draft regulations, which discusses "the authority of an authorized agent submitting an opt out request on behalf of a consumer"[30] and Rule 13:45L-2.2(a)7, which requires that businesses disclose in their privacy notices "how an authorized agent may opt out of the processing of personal data on a consumer's behalf." On the other hand, the draft regulations create a new definition of "data rights" which encompasses both consumer opt-out rights (concerning data sales, targeted advertising, and certain profiling decisions) and consumer controls (the ability confirm whether data processing is taking place and to access that data, correct inaccuracies, delete, and obtain data in a portable format) and includes language that "[i]f a consumer uses an authorized agent to exercise a data right [then]" proof of permission may be required.[31] This new language could potentially empower authorized agents to attempt to exercise the full scope of NJDPA privacy rights, not just the opt-out rights clearly anticipated in the statute, but also higher-risk consumer controls.

FPF recommends that the Division clarify precisely which consumer rights may be exercised by authorized agents. Should the Division decide to expand the authority of authorized agents beyond opt-out rights to higher-risk consumer controls, we encourage the Division to consider whether any additional verification processes and procedural mechanisms may be appropriate in

---

[26] N.J.S.A. C.56:8-166.11(8)a.
[27] *Id.*
[28] Jordan Francis, Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends (Nov. 2025), https://papers.ssrn.com/abstract_id=5309115.
[29] *See, e.g.*, James Pavur & Casey Knerr, *GDPArrrr: Using Privacy Laws to Steal Identities*, Blackhat USA 2019 Whitepaper (2019), https://arxiv.org/pdf/1912.00731.
[30] Data Privacy - Proposed New Rules: N.J.A.C. 13:45L, 57 N.J.R. 1101(a), p. 1103.
[31] Draft N.J.A.C. 13:45L-4.4.

the context of exercising access, correction, and deletion rights to account for the greater risks. For example, a business might be empowered to provide data directly to a consumer in response to an authorized agent access request rather than to a third-party agent.

C. Should the regulations expand universal opt-out mechanisms to the consumer right to opt out of certain profiling decisions, create a review and approval process for qualifying signals

The NJDPA provides that a consumer may utilize a "user-selected universal opt-out mechanism" ("UOOM") to opt out of the collection and processing of personal data for sales and targeted advertising.[32] A UOOM is an important mechanism that enables individuals to exercise key privacy preferences at scale rather than on a website-by-website basis and is an increasingly popular aspect of comprehensive state data privacy laws.[33] The regulations take a helpful step in recognizing an "opt-out preference signal" ("OOPS"), which is the specific communication transmitted by a UOOM that invokes a consumer's right(s). Critically, the same OOPS can be sent by different UOOMs in both valid and invalid ways, which underscores the importance of clear rules that empower consumers to make informed choices about their privacy that businesses will respect.

The draft regulations depart from the plain statutory text (and the twelve other states that recognize UOOMs) by providing that a UOOM transmit an OOPS that invokes the right to opt-out of certain profiling decisions "to the extent such technology exists."[34] While the NJDPA does provide that a consumer may "designate an *authorized agent*" through a variety of mechanisms that may exercise all three consumer opt-out rights (sales, targeted advertising, and, "when such technology exists," certain profiling decisions), it does not provide for the exercise of profiling opt-outs through UOOMs/OOPS.[35]

Using signal mechanisms to invoke profiling opt-out rights would raise novel technical, policy, and design challenges that require careful consideration. Targeted advertising and data sales are use cases focused on a business's monetization of personal data that are largely consistent across industries, making them appropriate choices for informed consumers to exercise these rights on a global and default basis. In contrast, data profiling for significant decisions varies significantly across different industries and has a greater ability to impact the core services offered to a consumer. For example, diverging use cases such as data processing to make health recommendations and processing to make a credit eligibility determination could both be subject to a right to opt out of profiling. These elements would make it significantly more difficult for a UOOM provider to give required disclosures that ensure that an individual is able to make an informed opt-out of all automated profiling decisions on a default basis. Furthermore, creating a new class of signal mechanism intended to invoke differing rights from those used in twelve other states may create uncertainty for both consumers and businesses.

---

[32] N.J.S.A. 56:8-166.11(b).
[33] *See*, Samuel Adams & Stacey Gray, "Survey of Current Universal Opt-Out Mechanisms" Future of Privacy Forum (Oct. 12, 2023), https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms.
[34] Draft 13:45L-3.2(a)2.
[35] N.J.S.A. 56:8-166.11(b).

If the Division proceeds with expanding UOOMs/OOPS to profiling opt-out rights, we recommend considering Colorado's example[36] by establishing an open, authoritative process through which technical and policy challenges associated with the expansion of signal mechanisms can be explored. Through this process, any potential signals and signal mechanisms can be reviewed and formally approved to ensure adherence to statutory and regulatory requirements. Ideally, this process would ensure maximum clarity for both consumers and businesses about which signals have legal effect and the practical impact of sending or receiving a signal.

III. Notice requirements and consumer rights

A. The regulations should consider alternative methods to incentivize system testing and evaluations

The draft regulations require that controllers using personal data for profiling in decisions producing legal or similarly significant effects disclose in their privacy notice if the system "has been evaluated for accuracy, fairness, or bias, including the impact of the use of sensitive data, and the outcome of any such evaluation."[37] While consumer transparency is an essential component of trustworthy systems, this provision, as currently drafted, may inadvertently discourage both testing and transparency.

A controller that has not conducted any evaluation may simply disclose that fact with no further obligation. However, a controller that has conducted such an evaluation would be required to disclose the "outcome," even if the results raise concerns or require contextual explanation. This requirement may thus potentially disincentivize organizations from engaging in proactive testing and self-assessment, as it may expose them to reputational or legal risk without sufficient opportunity to provide meaningful context.

A relevant example is New York City's Local Law 144, which mandates that employers disclose the results of bias audits conducted on automated employment decision tools.[38] The law has been criticized in part because it places employers in the difficult position of requiring the publication of technical audit results that are often nuanced and may be misinterpreted by the public.[39] Additionally, some employers have expressed concern that disclosing audit outcomes—even when the results do not indicate a legal violation and reflect the reality that no system is entirely free from bias—could expose them to reputational risk or legal uncertainty.[40]

---

[36] Off. of the Colo. Att'y Gen., *Universal Opt-Out and the Colorado Privacy Act*, https://coag.gov/opt-out (last accessed August 13, 2025).
[37] Draft N.J.A.C. 13:45L-2.2(b)5.
[38] L.L. 144 (enacted), New York City, 2021, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9.
[39] *See, e.g.*, *Studying How Employers Comply with NYC's New Hiring Algorithm Law*, Citizens and Tech, https://citizensandtech.org/research/2024-algorithm-transparency-law (last accessed August 13, 2025).
[40] Lara Groves et al., *Auditing Work: Exploring the New York City Algorithmic Bias Audit Regime*, arXiv (June 5, 2024), https://arxiv.org/html/2402.08101v1#S4; Lucas Wright et al., *Null Compliance: NYC Local Law 144 and the Challenges of Algorithm Accountability*, FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (June 3, 2024), https://dl.acm.org/doi/10.1145/3630106.3658998.

The Division may consider alternative methods utilized in other state data privacy laws to incentivize such testing, including the use of anti-bias testing as a documented safeguard in a data protection assessment or the creation of an exemption for the collection of data used for system testing.[41]

Anti-Bias Testing as an Exemption for Data Collection. The draft regulations could create an unintended Catch-22: controllers are required to disclose the results of bias testing, yet may be limited in their ability to conduct meaningful testing in the first place. Testing often requires processing large volumes of personal data, upon which access may depend on consumer consent, which is not guaranteed. Because effective bias testing for AI systems typically requires large, representative datasets, the current framework may unintentionally discourage testing altogether by both limiting the necessary data and requiring disclosure of potentially unfavorable outcomes.

Recent amendments to the Connecticut Data Privacy Act aim to address this challenge by allowing controllers to process personal data solely for the purpose of bias testing in automated decision-making systems ("ADMTs")—exempting such processing from certain legal obligations while still incorporating safeguards to prevent misuse and ensure responsible handling of the data.[42] Under that exemption,

> [the personal data must] (A) [be] processed only to the extent necessary to detect or correct any bias that may result from processing such data for such purposes, such bias cannot effectively be detected or corrected without processing such data and such data are deleted once such processing has been completed, (B) [be] processed subject to appropriate safeguards to protect the rights of consumers secured by the Constitution or laws of this state or of the United States, (C) [be] subject to technical restrictions concerning the reuse of such data and industry-standard security and privacy measures, including, but not limited to, pseudonymization, (D) [be] subject to measures to ensure that such data are secure, protected and subject to suitable safeguards, including, but not limited to, strict controls concerning, and documentation of, access to such data, to avoid misuse and ensure that only authorized persons may access such data while preserving the confidentiality of such data, and (E) not [be] transmitted, transferred or otherwise accessed by any third party.[43]

Particularly in the absence of a similar exemption for de-identified or aggregated data in the New Jersey regulations mentioned above, adopting such an approach could encourage bias testing in a privacy-protective and practical way.

B. Consider allowing some flexibility in the requirement to delete sensitive data after a consumer revokes consent for processing.

State privacy laws vary regarding whether controllers are explicitly required to provide consumers with a mechanism to revoke consent for processing activities and how controllers

---

[41] *See* S.B. 1295, Public Act No. 25-113, 2025 Reg. Sess. (Conn. 2025), https://www.cga.ct.gov/2025/ACT/PA/PDF/2025PA-00113-R00SB-01295-PA.PDF.
[42] *Id.*
[43] *Id*. at sec. 12(b)(4).

must respond to the revocation of consent. The NJDPA follows the strongest iterations of existing comprehensive state privacy laws: a controller must establish a mechanism by which consumers may revoke consent for data processing, and that controller must respond to the revocation of consent by ceasing to process the personal data at issue "as soon as practicable, but not later than 15 days after the receipt of such request."[44] The draft regulations would depart from this statutory provision by providing that, as part of a controller's data minimization obligations, the controller must "document its efforts to . . . *immediately* delete sensitive data concerning the consumer" after the consumer revokes consent for processing the data at issue (emphasis added).[45] Notably, there are no provisions discussing the deletion of sensitive data within the NJDPA subsection on revoking consent, and it is unclear if this is a new obligation on controllers or if controllers must simply "document efforts" to immediately delete data.

If the Division intends for this to be a substantive new deletion obligation, it should carefully consider the technical capabilities for immediate data deletion. In modern IT infrastructure, personal information is typically distributed across multiple systems, databases, cloud services, third-party processors, and backup archives. Achieving truly "immediate" or instantaneous deletion would require real-time synchronization across all these environments – a technical impossibility for many companies. This would likely have a significant impact on how companies handle data backups. Companies typically have multiple levels of backup, and each level may need a different deletion approach, which is likely to significantly increase costs and potentially increase the likelihood of errors such as over-deletion or partial deletion of records.

This approach could also be disproportionately challenging for small and medium-sized enterprises (SMEs) if the only way to effectuate an "immediate" deletion of specific data across an entire organization would be to establish new technical, automated processes.[46] Rather than requiring that sensitive data be deleted "immediately," the regulations could instead reiterate the statutory standard, which provides greater flexibility by requiring that data be deleted "as soon as practicable" following the revocation of consent. The "as soon as practicable" standard could help SMEs in the scope of the Act comply with this provision by deleting data manually, should they choose, instead of implementing more costly, scaled systems.

IV. Data Protection Assessments

The proposed requirements for data protection assessments under these regulations largely align with those under the Colorado Privacy Act regulations, which currently are the most detailed such requirements under any U.S. state comprehensive privacy law. Two key areas where New Jersey's draft regulations differ, however, include (A) a potentially broad requirement to list "[t]echnology to be used" in the processing activity, and (B) no explicit provision allowing

[44] N.J.S.A. 56:8-166.12(a)6.
[45] Draft N.J.A.C. 13:45L-6.3(b)6.
[46] An analogous dilemma is how processors should be required to assist controllers in responding to consumer rights requests. *See* Business Software Alliance, *Consumer Rights to Access, Correct and Delete Data: A Processor's Role*, BSA (June 11, 2025), https://www.bsa.org/files/policy-filings/06112025controllerprorights.pdf (suggesting that processors can assist controllers by either (1) responding to consumer requests one-by-one, or (2) creating a scalable tool that the controller can use).

controllers to forego conducting duplicate assessments if they have already conducted a similar assessment for compliance with another jurisdiction's law or regulation.

A. Technology to be Used in the Processing

Under the draft regulations, data protection assessments must include the "elements of the processing activity," which includes "[t]echnology to be used." As drafted, this requirement may be unintentionally broad. "Technology to be used" in the processing can include anything from novel and potentially high-risk uses of technology, such as facial recognition or ADMTs, to individual components of computer systems, to pencils and other writing utensils. If the intent of this requirement was to require controllers to detail potentially risky applications of novel technologies, then consider the framing of Colorado's comparable requirement. The Colorado regulations allow the controller to tailor their disclosure of operational elements to a level of detail and specificity commensurate with the level of risk posed. Below, we compare the proposed N.J.A.C. language against that in Colorado's law:

New Jersey Proposed Language	Colorado Current Language
The elements of the processing activity, including: i. Sources of personal data; ii. Technology to be used; iii. Processors to be used; iv. Names or categories of personal data recipients, including third parties, affiliates, and processors that will have access to the personal data, the processing purpose for which the personal data will be provided to those recipients, and compliance processes that the controller uses to ensure the security of personal data shared with such recipients; v. Operational details about the processing, including planned processes for personal data collection, use, storage, retention, and sharing; and vi. Specific types of personal data to be processed.[47]	The nature and operational elements of the Processing activity. In determining ***the level of detail and specificity*** to provide pursuant to this section, the Controller shall consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will have on the level of risk presented by the Processing activity, and any relevant unique relationships. Relevant operational elements ***may include***: a. Sources of Personal Data; b. Technology or Processors to be used; c. Names or categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data, the processing purpose for which the Personal Data will be provided to those recipients, and categorical compliance processes that the Controller uses to evaluate that type of recipient; d. Operational details about the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing; and e. Specific types of Personal Data to be processed.[48]

[47] Draft N.J.A.C. 13:45L-8.1(b)4.
[48] 4 Colo. Code Regs. § 904-3, Rule 8.04(A)(4) (emphasis added).

The California Privacy Protection Agency considered similar language to that currently in the proposed N.J.A.C. regulations as part of the CPPA's ongoing rulemaking concerning risk assessment requirements. However, the CPPA ultimately removed that language in recent updates to its proposed regulations.[49]

B. Compliance with Another Jurisdiction

Another key difference between the NJDPA and other state comprehensive privacy law regimes is that the data protection assessment requirements do not include an explicit provision providing that an assessment conducted for compliance with another jurisdiction's law can satisfy the NJDPA's requirements if the assessment is similar in scope and includes all required information.

For example, the Colorado Privacy Act provides that"[i]f a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section," and a controller can supplement any such assessment with information necessary to make it similar in scope to that required under the regulations.[50] Provisions like these ease compliance burdens by avoiding duplicative paperwork requirements that add little to no protection beyond work already conducted. We encourage the Division to consider adding such language.

* * *

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

Sincerely,

Bailey Sanchez
Deputy Director, U.S. Legislation

Justine Gluck
AI Legislation Fellow, U.S. Legislation

---

[49] *Compare* Cal. Priv. Prot. Agency, Text of Proposed Regulation, § 7152(a)(3)(G), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf, *with* Cal. Priv. Prot. Agency, Modified Text of Proposed Regulations, § 7152(a)(3)(G), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf.

[50] 4 Colo. Code Regs. § 904-3, Rule 8.02(B).