July 31, 2025

Submitted via electronic mail to: DCAProposal@dca.lps.state.nj.us

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

Re: Comments on the Proposed Rules Implementing the New Jersey Data Privacy Act (NJDPA)

Dear Acting Director Fais:

On behalf of the Network Advertising Initiative (the "NAI"), thank you for the opportunity to comment on the Division of Consumer Affairs' proposed rules implementing the New Jersey Data Privacy Act ("NJDPA") (the "Proposed Rules").[1]

The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000, promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. The NAI's members are providers of advertising technology solutions, and include ad exchanges, demand side platforms, supply side platforms, as well as other companies that power the digital media industry. Our member companies help digital publishers generate essential ad revenue, advertisers reach audiences interested in their products and services, and ensure consumers are provided with ads relevant to their interests.[2] Earlier this year, the NAI launched its new Self-Regulatory Framework (the "NAI Framework") to promote strong privacy practices for NAI members and to facilitate their compliance with new state privacy laws, including the NJDPA.[3]

The NAI is supportive of the Division of Consumer Affairs (the "Division") as it joins the ranks of other states that have undertaken rulemaking to implement new privacy laws. The NAI has been highly engaged in state privacy law rulemaking for years and has consistently submitted comments on rulemaking efforts in California, Colorado, and privacy-related rulemaking in other jurisdictions.[4] While the NAI is offering comments on many detailed points in the Proposed Rules, we also recommend that the Division focus

---

[1] 57 N.J.R. 1101(a) (June 2, 2025) (proposed N.J.A.C. 13:45L), https://www.njconsumeraffairs.gov/ProposalPDF/ocp-06022025-proposal.pdf.
[2] *See generally* About the NAI, https://thenai.org/about-the-nai-2/.
[3] *See* The NAI Self-Regulatory Framework, https://thenai.org/self-regulatory-framework/.
[4] *See generally* Public Policy Updates, https://thenai.org/policy-news/policy-priorities/ (listing the NAI's comments to regulators and policymakers in Colorado, California, New York, the U.S. Department of Justice, the U.S. Federal Trade Commission, and others).

on three overarching principles as it considers comments and works toward finalizing the Proposed Rules:

1. **Harmony with Statutory Text.** The purpose of regulations is to implement, not alter statutory requirements. Where proposed rules exceed or diverge from statutory language, the intended goals and balance achieved by lawmakers will be frustrated.

2. **Interoperability Across State Frameworks.** A patchwork of materially different rule sets across states breeds consumer confusion and compliance friction without commensurate privacy gains. Where consistent with the aims of lawmakers and the statutory text, the Division should seek harmony with requirements in other states.

3. **Feasibility for Consumers and Businesses Alike.** Effective rules must be technologically achievable by controllers subject to them at scale; and must also promote the ability of ordinary consumers to understand and exercise their privacy rights.

The recommendations below apply these principles section-by-section and include additional legal analysis and empirical policy support. Our comments below are organized into six sections.

- Section I: Definitions
- Section II: Exemptions
- Section III: Consent and Choice Architecture
- Section IV: Transparency
- Section V: Consumer Requests & Authorized Agents

I. Definitions

A. The Division should remove the newly defined term "Data Broker" from the Proposed Rules, or else Update it to Align with National Consensus.

The Proposed Rules include a new definition of "data broker" as follows:

> *"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."*[5]

The NAI recommends that the Division remove this definition of "data broker" from the Proposed Rules altogether. Newly proposed definitions should have a clear connection to controller obligations or consumer rights under the NJDPA; and likewise facilitate controller compliance with relevant obligations or consumer exercise of relevant rights. However, the newly defined term "data broker" is used only in a limited way in the Proposed Rules to specify categories of third parties that the controller should disclose in certain privacy notices.[6] Neither the NJDPA nor the Proposed Rules impose any corresponding substantive obligations or rights that hinge on whether an entity qualifies as a "data broker." Removing the definition would reduce complexity without affecting the operation of any other provisions in the Proposed Rules and would reduce interpretive confusion for businesses trying to align multi-state compliance efforts, as other state and federal laws also put forward their own definitions for businesses that qualify as data brokers.[7]

---

[5] N.J.A.C. §13:45L-1.2 (proposed). The Proposed Rules further define that a direct relationship includes "situations when a consumer is a past or present customer, client, subscriber, or user of the person or legal entity's goods or services; employee, contractor, or agent of the person or legal entity; investor in the person or legal entity; or donor to the person or legal entity." *Id.*

[6] *See* N.J.A.C. § 13:45L-1.5(a)(4)(ii) (proposed) (providing example of impermissible bundling of consent where a controller sells geolocation data to data brokers for purposes incompatible with the original context of collection); 13:45L-2.2(a)(4)(ii) (proposed) (listing data brokers as an example of a sufficiently granular category of third party to which personal data may be disclosed or sold); 13:45L-2.5(e)(4) (proposed) (requiring loyalty program notices to disclose whether personal data will be provided to data brokers); 13:45L-6.4(b)(4) (proposed) (directing controllers to consider whether personal data originated from a data broker when assessing appropriate data security safeguards) (emphasis added).

[7] *See, e.g.*, Cal. Civ. Code § 1798.99.80(d) (defining "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship); O.R.S. 646A.593(c)(A) (defining "data broker" as a business entity that collects and sells or licenses brokered personal data to another person); Vt. Stat. Ann. tit. 9, § 2430(4) (defining "data broker" as a business that knowingly collects and sells or licenses to third parties brokered personal information of a consumer with whom it has no direct relationship); Protecting Americans' Data from Foreign Adversaries Act of 2024, § 2(3)(A) (defining "data broker" as an entity that makes available, for valuable consideration, data of U.S. individuals that it did not collect directly and provides it to another entity not acting as a service provider) (emphasis added). *But see* Tex. Bus. & Com. Code § 509.001(4)

Recommended Amendment to the Proposed Rules:

(1) Delete the following definition from N.J.A.C. § 13:45L-1.2:

~~*"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.*~~

(2) Delete all other subsequent references to "data brokers" in the proposed New Jersey statute provisions.[8]

Alternatively, if the Division retains a definition of "data broker" in the Proposed Rules, it should amend the definition to align with those put forward in other leading states. As it stands, the proposed definition of "data broker" is expansive and captures entities that merely *collect* personal data outside of a direct relationship with a consumer, without requiring that the entity sell or otherwise monetize that data.

This broad definition would sweep in many businesses that an average consumer would not consider to be a data broker. For example, a brand advertiser might show digital ads to promote its products with consumers who are not yet customers and collect information to measure whether or how long the consumer viewed the ads. However, the advertiser might lack a direct relationship with those consumers in those circumstances. Under the proposed definition of "data broker," though, merely collecting that information would cause the brand advertiser to be classified as a data broker, even though this is far from the everyday understanding of that term. Such breadth risks diluting a consumer's ability to distinguish between entities that are truly in the business of buying and reselling personal data and those that merely participate in ordinary digital advertising workflows.

To understand the gap between the definition of "data broker" in the Proposed Rules and how other leading states define data broker, consider California's definition, which refers to a business that:

> *"knowingly collects **and sells to third parties** the personal information of a consumer with whom the business does not have a direct relationship."*[9]

Unlike the definition in the Proposed Rules, California's definition does not cover entities that merely collect or process personal information for operational purposes without engaging in an onward sale of that information.[10] Other leading states like Vermont and

(defining "data broker" as a business whose principal revenue comes from collecting, processing, or transferring personal data not collected directly from the individual).

[8] *See supra* note 6.

[9] Cal. Civ. Code § 1798.99.80(c) (2024) (emphasis added).

[10] *Id.*

Oregon also include this key element of re-selling personal data.[11] If New Jersey adopts an overbroad definition of "data broker," that would risk both undermining consumer understanding of who is truly in the business of collecting and re-selling personal data; and would create misalignment with statutory regimes in other states.

Instead, by following other states in tethering the definition of data broker to **sales**, the Proposed Rules can help consumers discern who is in the business of data resale.

Recommended Amendment to the Proposed Rules (Alternative to Deletion): Revise the definition of "data broker" in N.J.A.C. § 13:45L-1.2 as follows:

> "Data broker" means a person or legal entity, including a controller, that knowingly collects~~, purchases, or~~ and sells to third parties the personal data of a consumer with whom the person or legal entity does not have a direct relationship.

B. The Division Should Retain the Proposed Definition of "Opt-Out Preference Signal" (OOPS), but Also Define Universal Opt-Out Mechanism (UOOM) and Clarify How these Terms are Related to Promote Strong User-Interface Standards for UOOMs.

The NJDPA recognizes the key role of technical mechanisms or signals that may facilitate consumers' ability to opt out of sales and targeted advertising online through a "universal opt-out mechanism" (UOOM), and it requires controllers to allow consumers to opt out of sales and targeted advertising using a valid UOOM.[12]

Neither the NJDPA nor the Proposed Rules define "UOOM." However, the Proposed Rules introduce a related, but separate, definition for an "opt-out preference signal" (OOPs) as follows:

> *"a signal that is sent on behalf of the consumer, which communicates the consumer's decision to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legally or similarly significant effects concerning a consumer."*

The NAI supports the addition of this new definition in the Proposed Rule because it appropriately recognizes that there is a significant distinction between a *mechanism* (a UOOM) that a consumer may interact with to initiate an opt-out request, from a *signal* (an OOPS) that may be generated by such mechanism and subsequently sent to

[11] *See supra* note 6.
[12] *See* NJ Rev. Stat. § 56:8-166.11.

controllers online. The NAI views this distinction as crucial for effective implementation because it allows the Division to clearly assign criteria and standards for consumer-facing UOOMs; while also clarifying how technical signals should be sent, received, and honored by controllers with respect to OOPS sent as a result of user choices made through a UOOM.

Separating the concepts of UOOM and OOPS is an important clarification that other state laws and regulations have not addressed. For instance, a specific web browser or browser extension that that implements the Global Privacy Control (GPC) technical specification to enable users to send opt out signals is UOOM; but the GPC signal itself, that is transmitted by such a browser (*i.e.*, the header signal that is seen by websites the user visits), is an OOPS.

Although the Colorado Department of Law's process for implementing its UOOM requirements under the Colorado Privacy Act (CPA) established a very open and thorough process for stakeholder engagement,[13] their designation of Global Privacy Control (GPC)[14] as the only UOOM currently recognized under Colorado law[15] leaves out important details describing how certain CPA requirements for a valid UOOM could be satisfied by GPC.[16] That is because GPC itself is a signaling specification for communicating opt-out choices to businesses online and does *not* include any

[13] *See* Colo. A.G., *Universal Opt-Out and the Colorado Privacy Act*, https://coag.gov/opt-out/, (describing the Office of the Attorney General's process for soliciting applications and designating valid UOOMs under the Colorado Privacy Act); *see also* Colo. A.G., *Universal Opt Out Applications*, https://comments.coag.gov/s/universal-opt-out-applications, (collecting public comments submitted in response to the Office's UOOM designation process, including comments from the NAI).

[14] *See* Global Privacy Control, https://globalprivacycontrol.org/ (describing GPC as a technical specification for sending opt-out signals to websites via browser settings).

[15] *See* Colorado Attorney General, *Universal Opt-Out and the Colorado Privacy Act*, https://coag.gov/opt-out/ (providing Colorado's list of recognized UOOMs under the CPA and listing only GPC as of this writing, while noting that additional UOOMs may be recognized in the future); *see also* Future of Privacy Forum, *Colorado's Approval of Global Privacy Control: Implications for Advertisers and Publishers*, (Feb. 14, 2024), https://fpf.org/blog/colorados-approval-of-global-privacy-control-implications-for-advertisers-and-publishers/ (explaining that, following a public comment period, the Colorado AG designated only GPC for inclusion on the public UOOM list).

[16] *See* Network Advertising Initiative, *NAI Comments on Colorado Universal Opt-Out Shortlist*, [4], [5], [7], [2], (Dec. 12, 2023), https://thenai.org/nai-comments-on-colorado-universal-opt-out-shortlist/ ("[T]echnical signal specifications presented independently of a user interface … cannot satisfy the Consumer Choice Principle…"; "If GPC displays a value of "1", for example, this does not by itself reflect any information about how a choice to Opt Out was presented to a consumer or whether such a choice was presented at all (i.e. if it is a default setting)"; "The signal transmitted by the GPC does not currently encode information about the source of the GPC signal…"; and recommending that "only specific implementations of GPC that … satisfy the Consumer Choice Principle" be approved").

specifications or standards for the *mechanism* a consumer might interact with to activate or deactivate that signal.[17]

The NAI is supportive of GPC as a signal standard for communicating consumer opt-out choices online, provided that GPC signals originate from and reflect authentic consumer choices to opt out. Conversely, if a browser activates a GPC signal for its users by default, therefore presupposing a consumer's choice to send a GPC signal without the consumer making an active choice, this would not be in compliance with the specific NJDPA requirements about the proper implementation of UOOMs.

By leveraging the distinction between a UOOM and an OOPS, the Department has an opportunity to enhance utilization and trust in the market for the GPC signal *as an OOPS*, while applying the NJDPA requirements for a valid UOOM[18] to mechanisms that consumers actually use and interact with – such as web browsers and browser extensions. We encourage the Division to run a process similar to Colorado's to evaluate different UOOMs with a strong focus on user interface requirements found in NJDPA, even though many such UOOMs may ultimately send the same signal (GPC) as an OOPS. The NAI is currently developing a GPC implementation we believe will meet the NJDPA requirements for a valid UOOM and would welcome the opportunity to engage with your office further on how it achieves that goal.

If the Division does not focus on UOOMs that *implement* an OOPS like GPC, an unfortunate status quo in the market may continue. Currently, controllers that encounter GPC signals online may be unsure about the validity of those signals. Indeed, research has shown that different *mechanisms* implementing GPC (*i.e.*, different browsers or browser extensions) "significantly differed in configuration options for when and where to send the GPC signal."[19]

As a result of these vastly different implementations of GPC, companies may struggle to determine whether they are seeing a valid user-initiated opt-out or simply a default

---

[17] *See* Global Privacy Control, *About GPC*, https://globalprivacycontrol.org/#about, (describing GPC as a technical specification for transmitting opt-out signals through user-enabled browser or device settings, but offering no accompanying standards for how a user interface should present or obtain consent for activating the signal); *see also* IAPP, *Is GPC the New "Do Not Track"?* (Oct. 25, 2022), https://iapp.org/news/a/is-gpc-the-new-do-not-track, (noting GPC's reliance on supported browsers and extensions, lack of UX standards, and functional similarities to earlier efforts like Do Not Track).

[18] *See* NJ Rev. Stat. § 56:8-166.11(b)(2) (requiring that opt-out mechanisms "not permit its manufacturer to unfairly disadvantage another controller", avoid default opt-in settings, be "consumer friendly, clearly described, and easy to use by the average consumer," align with similar mechanisms under other laws, and enable accurate determination of a consumer's residency and legitimate opt-out intent).

[19] Future of Privacy Forum, *Survey of Current Universal Opt-Out Mechanisms* (Oct. 12, 2023), https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms/ (surveying eight GPC-endorsed tools and highlighting inconsistent configuration defaults, installation processes, and signal transmission behaviors across implementations).

signal emitted by a web browser.[20] This ambiguity stems from the lack of a regulatory distinction between technical signals (OOPS) and user interfaces (UOOM). By introducing the OOPS concept and clearly distinguishing it from UOOMs, New Jersey has an opportunity to avoid this confusion and promote clarity and enforceability for all parties.

Recommended Amendments to the Proposed Rules

Amend the definition of "opt-out preference signal" as follows:

> *a signal that is sent on behalf of the consumer through a universal opt-out mechanism, which communicates the consumer's decision to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legally or similarly significant effects concerning a consumer.*

Add a new definition of "universal opt-out mechanism" as follows:[21]

> *a user-selected mechanism that enables a consumer to clearly communicate, by sending an opt-out preference signal, the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data pursuant, to P.L.2023, c.266 (C.56:8-166.4 et seq.) and which meets the requirements set forth in P.L.2023, c.266 (C.56:8-166.11).*

[20] The Brave browser, for example, sends the GPC signal by default and does not offer a consumer-friendly, easy-to-use mechanism for consumers to stop sending it. *See* Brave, *Global Privacy Control*, https://brave.com/web-standards-at-brave/4-global-privacy-control/, (last updated Sep. 8, 2023) (explaining that GPC is on by default); *see also* Brave Help Center, https://support.brave.app/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings, (providing only technical instructions for how to disable GPC, but no user interface for controlling it).

[21] *Compare* 4 Colo. Code Regs. § 904-3, Rule 2.02 (defining "Universal Opt-Out Mechanism" as a mechanism that clearly communicates a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for targeted advertising or sale and noting that it must meet separate technical requirements set out in Rule 5.06; *see also id.* § 904-3:5.06 (establishing technical specifications for UOOMs, including compatibility with multiple controllers, signal format standards, data security, and safeguards against illegitimate requests and unfair competitive advantages).

II. Exemptions

A. The Proposed Rules Should Clarify that HIPAA De-Identified Data Qualifies as "De-Identified Data" under the NJDPA to Avoid Conflicts with HIPAA and Preserve Beneficial Uses of De-Identified Data.

The Proposed Rules exempt from the NJDPA any personal data that is protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).[22] This exemption is helpful because it recognizes and defers to the policy decisions made by Congress around the regulation of PHI and avoids potential conflicts between the NJDPA and HIPAA.

However, a potential for conflict between HIPAA and NJPDA still remains because this exemption does not explicitly extend to PHI that has been de-identified in accordance with HIPAA's de-identification standards.[23] PHI that has been de-identified in compliance with the HIPAA de-identification standard – and that is therefore no longer PHI under HIPAA – could remain subject to the NJDPA under the current structure of the Proposed Rules. To avoid this result, the Division should amend the definition of "de-identified data" under the Proposed Rules to clarify that it includes data de-identified under the HIPAA standard.

Taking this approach would follow a helpful example set by Oregon's consumer privacy law, which explicitly recognizes de-identified PHI as meeting Oregon's de-identification standards by incorporating the HIPAA de-identification standard directly into its definition of de-identified data.[24] This ensures that entities using HIPAA-deidentified data for research, analytics, operational improvement, or other beneficial uses are not burdened by overlapping or inconsistent state-level obligations.

Recommended Amendments to Text of Proposed Rules:

(1) Revise N.J.A.C. § 13:45L-1.2 as follows:

> "De-identified data" means data that cannot be reasonably used to infer information about, or otherwise be linked to, an identified or identifiable

[22] N.J.A.C. § 13:45L-1.3(a)(1) (proposed).
[23] *Id*. HIPAA's de-identification standards are defined under 45 C.F.R. § 164.514(b)(2). In addition to de-identified data under HIPAA, the statute largely does not cover de-identified data. N.J.A.C. 13:45L summary (p.2) ("Among other things, the NJDPA grants consumers certain rights regarding their personal data . . . with exceptions for 'de-identified data or publicly available information.'").
[24] *See* ORS 646A.570(11)(b) (A-B) (defining "de-identified data" to include patient information originally handled by HIPAA-regulated entities and de-identified in accordance with the federal HIPAA standard at 45 C.F.R. 164.514).

individual, or a device linked to such an individual, if the controller that possesses the data:

1. Takes reasonable measures to ensure that the data cannot be associated with an individual;

2. Publicly commits to maintain and use the data only in a de-identified fashion and not to attempt to re-identify the data;

3. Contractually obligates any recipients of the information to comply with the requirements of this paragraph.

...

; or

1. Is:
   (A) Derived from patient information that was originally created, collected, transmitted or maintained by an entity subject to regulation under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as in effect on the effective date of this Act, or the Federal Policy for the Protection of Human Subjects, codified as 45 C.F..R. part 46 and in various other deferral regulations, as codified in various sections of the Code of Federal Regulations and as in effect on the effective date of this Act; and
   (B) Deidentified as provided in 45 C.F.R. 164.514, as in effect on the effective date of this Act.

These amendments would mirror the approach adopted in Oregon, promoting alignment in interpretation across states, and ensure that HIPAA-deidentified data is treated consistently across legal frameworks.

B. Artificial Intelligence Training – The Proposed Rules Should be Amended to Avoid Creating a Hidden, Higher Consent Standard.

The Proposed Rules, mirroring the NJDPA,[25] detail certain data processing activities that are exempt from the requirements of the NJDPA.[26] However, as currently drafted, these exemptions in Proposed Rules would actually create a heightened consent standard for personal data processing related to training artificial intelligence (AI). Specifically, the Proposed Rules state:[27]

[25] *See* NJ Rev. Stat. § 56:8-166.13 through 166.15 (exempting from the Act certain uses of personal data).
[26] *See generally* N.J.A.C. § 13:45L-1.3 (proposed).
[27] *Id.* § 13:45L-1.3(d) (proposed) (emphasis added).

(d) The obligations imposed on controllers or processors pursuant to this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to:

1. Conduct internal research to develop, improve, or repair products, services, or technology. Collection, use or retention of data shall not be considered to be for the purpose of internal research if:

ii. The data or resulting research is used to train artificial intelligence, ***unless the consumer has affirmatively consented to such use****.*

While limiting the applicability of wholesale exemptions from the NJDPA to data used to train AI may accomplish a worthy policy aim by promoting transparency around the use of personal data to train AI models, the Proposed Rules appear to be doing this quietly by imposing an unprecedented consent requirement within a subsection that is otherwise devoted to *exemptions* from statutory obligations. The NAI views this structure as problematic for two reasons.

First, it is disconnected from the text of the NJDPA. Nothing in the NJDPA conditions AI training on opt-in consent. Indeed, the NJDPA does not single out AI training at all; and instead, appears to treat any such activity as ordinary "processing" subject to baseline duties of transparency, data-minimization, purpose limitation, and consumer rights (including deletion, access, and correction).[28] By creating a novel opt-in mandate for AI training in the exemptions section of implementing rules, the Proposed Rules would be making a crucial policy decision better reserved for lawmakers considering AI regulation.

Second, the inclusion of the proposed opt-in consent requirement creates structural confusion within the Proposed Rules. Nesting a heightened consent mandate within a paragraph headed "Exemptions" is counter-intuitive: stakeholders reasonably expect entries in that list to specify activities that policymakers do not wish to impose burdens on – not add new ones. By inverting that expectation, the Proposed Rules risk burying a major obligation where compliance teams—and consumers—are unlikely to look. This drafting choice invites inadvertent non-compliance and undermines the clarity that is essential for effective enforcement.

To avoid these problems, the NAI recommends that the Division simply remove reference to AI training in the section on exemptions. The result would be that personal data used for AI training would remain fully subject to the NJDPA's transparency, purpose-limitation, data-minimization, and consumer-rights provisions without imposing a heightened opt-in consent standard. The effect is to treat AI training like any other

[28] *See generally* NJ Rev. Stat. § 56:8-166.4 et seq. (containing no reference to artificial intelligence or consent requirements specific to AI training).

non-exempt processing activity—fully subject to the NJDPA's general requirements—without layering on a special opt-in standard not found elsewhere in the statute.

Recommended Amendments to Text of Proposed Rules:

Revise N.J.A.C. § 13:45L-1.3(d)(1)(ii) as follows:

> *(d) The obligations imposed on controllers or processors pursuant to this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to:*
>
> > *1. Conduct internal research to develop, improve, or repair products, services, or technology. Collection, use or retention of data shall not be considered to be for the purpose of internal research if:*
> >
> > …
> >
> > ~~*ii. The data or resulting research is used to train artificial intelligence, unless the consumer has affirmatively consented to such use.*~~

III. Consent and Choice Architecture

A. Bundled Consent – The Proposed Rules Should Follow the NJDPA's Approach to Consent to Align with Legislative Intent and Avoid a Confusing User Experience.

The Proposed Rules prohibit controllers from obtaining consent by bundling multiple data processing purposes into a single choice interface if those purposes are "incompatible with the context in which the personal data was collected."[29] The Proposed Rules illustrate this prohibition with an example: a mobile application that finds gas prices near a consumer's location must not bundle consent for its use of the consumer's geolocation data for the purpose of finding local gas prices with the sale of the consumer's geolocation data to data brokers.[30] The Proposed Rules suggest that the latter data processing purpose is an incompatible use of geolocation data; while the former is a "reasonably necessary and proportionate use of geolocation data for providing [a] location-based service.[31] In order for a controller to comply with this aspect of Proposed Rules, a consumer's consent would need to be obtained separately for each specific purpose, effectively requiring a standalone prompt for each individual use of

[29] N.J.A.C. §13.45L-1.5(a)(4)(ii) (proposed) ("The methods shall not impair or interfere with the consumer's ability to make a choice, exercise their choice, or give free, specific, informed, and unambiguous consent; for example … [b]undling choices so that the consumer is forced to consent to the use of personal data for any purposes that are incompatible with the context in which the personal data was collected.").
[30] *Id.*
[31] *Id.*

data – not only for sales to data brokers but also for advertising, personalization, or analytics.[32]

Separate, standalone prompts for consent for many different data uses would significantly disrupt existing user experience designs and compliance frameworks, especially in mobile or cross-platform environments. For example, in both iOS and Android mobile operating systems, app developers have some flexibility to provide text explaining why the app is asking for permission to access location services and can therefore disclose an app's different processing purposes before the user grants permission; but cannot use the operating system prompt to obtain separate consents for different purposes for accessing location services.[33] As such, in order to prompt users for separate consents for different purposes for processing location data, app developers would need to add additional consent prompts beyond the general prompt for access to location services. This is likely to be confusing to consumers and degrade the user experience, even though today users are already made aware of the fact that an app is requesting access to location services and the purposes for that access before granting or denying permission (*i.e.*, consenting).

Decisions about implementing the NJDPA requirements that are expected to have a high impact on businesses and user experience – such as this one – should align with the policy balance achieved by the text of the NJDPA itself. However, requiring separate consents appears to go beyond the intent of the legislature. Separate consents for each purpose of personal data processing goes well beyond the general "consent" definition in the NJDPA, which specifically addresses this issue by prohibiting consumer agreement to broad or general terms of service from serving as a proxy for informed consent. Specifically, the NJDPA's definition of consent states that consent shall not include "acceptance of a general or broad terms of use . . . that contains descriptions of personal data processing along with other, unrelated information[.]"[34]

To address these issues, the Division should remove the requirements in the Proposed Rules to separately obtain consent for different processing purposes so long as the baseline standard in the NJDPA is respected – by prohibiting companies from relying on

---

[32] *See id.* §13:45L-7.2(a)(3)(i) (proposed) ("When controllers request consent to process personal data for more than one processing purpose, and those processing purposes are not reasonably necessary to one another, consumers must have the ability to consent or not consent to each purpose separately.")
[33] *See generally* Apple Developer, *Requesting authorization to use location services*, https://developer.apple.com/documentation/corelocation/requesting-authorization-to-use-location-services (describing the location services authorization process in iOS, including how apps can request different levels of access and provide justification strings to explain usage to users); *see also* Android Developer, *Request location permissions*, https://developer.android.com/develop/sensors-and-location/location/permissions (explaining Android's location permission framework, including distinctions between foreground and background access and the corresponding permission requirements for app developers).
[34] NJ Rev. Stat. § 56:8-166.4.

a consumer's agreement to general terms of service to count as consent for personal data processing that should be prompted separately from terms of service that do not relate to personal data.

Recommended Amendments to Text of Proposed Rules:

Remove text of N.J.A.C. § 13:45L-1.5(a)(4)(ii):

> *"4. The methods shall not impair or interfere with the consumer's ability to make a choice, exercise their choice, or give free, specific, informed, and unambiguous consent; for example:*
>
> ...
>
> ~~*ii. Bundling choices so that the consumer is forced to consent to the use of personal data for any purposes that are incompatible with the context in which the personal data was collected. For example, a controller that provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, shall not require the consumer to consent to incompatible uses (for example, the sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation data for providing the location-based service."*~~

Remove text of N.J.A.C. § 13:45L-7.2(a)(3)(i):

> ~~*"When controllers request consent to process personal data for more than one processing purpose, and those processing purposes are not reasonably necessary to one another, consumers must have the ability to consent or not consent to each purpose separately."*~~

B. Disclosure of Names of Third Parties – Focus on What Users Understand

The Proposed Rules require controllers to disclose in their consent request interfaces:

> *"[t]he controller's identity" and "[t]he **names** of any third parties receiving sensitive data through sale."*[35]

This disagrees with the transparency requirement for sales of personal data to third parties found in NJDPA, which instead requires disclosure of the **"*categories*** of all third parties to which the controller may disclose a consumer's personal data."[36]

---

[35] N.J.A.C. § 13:45L-7.3(c)(1), (5) (proposed) (required information that a "controller's request for consent must provide") (emphasis added).
[36] NJ Rev. Stat. § 56:8-166.6(3)(a)(3) (emphasis added).

Departing from the NJDPA in this way is problematic for several reasons. First, it would be unlikely to aid in consumer comprehension or promote informed decision-making. Second, it would create new challenges for business implementation. Third, it would take New Jersey out of alignment with other authorities that have addressed the issue of third-party transparency. And finally, it would create tension with other requirements in the NJDPA that protect trade secrets.

First, from a consumer perspective, it is unlikely that naming which specific vendors or business partners a controller may sell personal data to will meaningfully enhance an average consumer's understanding of the data processing at issue or be material to that consumer's decision about whether to opt out of sales of personal data; or to grant or withdraw consent to a controller's processing of sensitive data. A primary purpose of giving consumers transparency into a controller's processing of their personal data is to help consumers make informed choices about how or whether to exercise their privacy rights. However, a balance must be struck between providing consumers with information that is *material* to those choices without overburdening them with details that will not impact their decision and may instead prove overwhelming or distracting.[37] Requiring controllers to give consumers transparency into the *categories* of third parties they may sell personal data to strike an appropriate balance. Consumers are still put on notice, for example, if a controller shares their personal data to third-party advertisers. This will be enough for an average consumer to decide whether to allow that activity. Providing the names of dozens of such third-party advertisers may make it harder for consumers to process the information they are being given and stymie their ability to make a simple, informed decision.

Second, from a business perspective, requiring disclosure of the specific names of third parties—particularly in real-time user interfaces[38]—would prove challenging because many businesses work with numerous vendors and business partners that may change dynamically over time, even on a weekly or monthly basis. Requiring businesses to adopt the type of time- and resource-intensive processes that would be needed to accurately make dynamic and vendor-specific updates to their consumer disclosures could only be

---

[37] *See* Network Advertising Initiative, *Best Practices: Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes*, (June 2020), https://thenai.org/wp-content/uploads/2021/07/nai_nonmarketing-bestpractices-0620_final-1.pdf (recommending that companies apply a materiality test to determine whether non-marketing uses of information should be disclosed separately in just-in-time notices, based on whether such uses would be material to a consumer's choice to grant consent); *see also In re X-mode Social, Inc & Outlogic, LLC*, Decision and Order, Docket No. C-4802 (Apr. 11, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf (requiring "affirmative express consent" to include disclosure of the purposes of collection and the **types** of entities receiving data, and suggesting that nondisclosure of data sales to government contractors was a deceptive practice because it was material to consumers' decisions to grant location permissions) (emphasis added).

[38] N.J.A.C. § 13:45L-7.3(d) (proposed) ("A controller must provide the disclosures required pursuant to (c) above on the *request interface itself*.") (emphasis added).

justified by a significant privacy benefit to consumers. However, as discussed above, providing consumers transparency into the names of specific third parties does not rise to that level.

Third, considering alignment with other authorities, a requirement to name third parties in public-facing disclosures would be unique. After specifically considering this issue, the California Privacy Protection Agency chose not to require businesses to name individual third parties in its regulations implementing the California Consumer Privacy Act, instead relying on category-based disclosures.[39] Both Colorado and Delaware similarly follow this standard for disclosure.[40] Beyond state law, platform privacy standards key required disclosure of downstream parties to high-level categories. For example:

- Apple's App Store policies require developers to use standardized "privacy nutrition labels" to disclose categories of data collected and shared, but they do not include fields for listing specific vendors. These labels are subject to App Store Review Guidelines § 5.1.1 and are constrained by platform design.[41]
- Google's Play Console Data Safety section requires developers to disclose categories of data collected and shared and to affirm that their practices align with public disclosures.[42] However, developers are not required or expected to list individual partners.[43]

Finally, requiring disclosure of specific third parties creates tension with a NJDPA provision stating that nothing in the NJDPA shall be construed to require a controller or

---

[39] *Compare* Cal. Privacy Protection Agency *Text of Proposed Regulations*, § 7012(e)(6) (as initially proposed, requiring that "if a business allows third parties to control the collection of personal information, [it must disclose] **the names of all the third parties**; or, in the alternative, information about the third parties' business practices") (emphasis added), https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf; *with* Cal. Code Regs., tit. 11 § 7012(e)(2)(A) (as finalized, requiring only that businesses disclose "the categories of third parties to whom the business discloses personal information," rather than the individual names of businesses), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

[40] *See* 4 Colo. Code Regs. § 904-3, Rule 6.03(1)(e) ("A privacy notice must include categories of [t]hird [p]arties to whom the controller sells, or with whom the [c]ontroller shares [p]ersonal [d]ata, if any. Categories of [t]hird [p]arties must be described in a level of detail that gives [c]onsumers a meaningful understanding of the type of, business model of, or processing conducted by the [t]hird [p]arty."); 6 Del. Code § 12D-106(c)(5) (requiring controllers to include in their privacy notice "the categories of third parties with which the controller shares personal data, if any"). *But see* Or. Rev. Stat. §§ 646A.574 (1)(a)(B), 646A.578(4)(e) (requiring controllers to disclose, in response to consumer requests, "a list of specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data", while requiring only "categories of third parties with which the controller shares personal data" in public-facing privacy notices)

[41] *See* Apple Inc., *App Privacy Details*, https://developer.apple.com/app-store/app-privacy-details/.

[42] *See* Google, *Data Safety Section*, https://support.google.com/googleplay/android-developer/answer/10787469.

[43] *Id.*

processor to disclose a trade secret.[44] The identities of integration partners or data recipients may, in some cases, reflect proprietary commercial relationships and contractual arrangements.[45] Compelling disclosure of these entities—particularly in environments such as real-time digital advertising—may force controllers to reveal competitively sensitive business information. The Proposed Rules should be updated to respect this statutory limitation. Courts and regulators have long recognized that customer and vendor lists may qualify as trade secrets when they are not publicly known, confer competitive advantage, and are subject to reasonable confidentiality measures.[46]

In summary, the Proposed Rules should not impose a name-by-name disclosure requirement for third parties, which would impose cost without measurable consumer benefit, all while taking New Jersey out of alignment with the treatment of third-party disclosure standards set by other authorities.[47]

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-7.3(a)(2) as follows:

> *A controller's request for consent must provide the following information . . . the ~~names~~ categories of any third parties receiving sensitive data through sale.*

C. The Proposed Rules Should Clarify That a Prohibition in Default Options in Choice Mechanisms Does Not Prohibit Common User Interfaces That Are Free of Dark Patterns.

When a controller provides consumers with choices for exercising their privacy rights, those choices should be presented in a way that accurately presents the right at issue (for example, consent vs. opt-out rights) and is free of dark patterns.[48] The Proposed

---

[44] N.J. Rev. Stat. § 56:8-166.10(1), (5) (requiring that in complying with a consumer exercising their rights of confirmation and data portability, controllers are not required "to provide the data to the consumer in a manner that would reveal the controller's trade secrets").

[45] *See* California Privacy Protection Agency, California Consumer Privacy Act Regulations, Final Statement of Reasons (March 2023), Appendix A, at p. 84 (several comments cautioned against a proposed requirement in the CCPA regulations to name third parties, noting that the disclosure "may conflict with confidentiality provisions in contracts[.]" The CPPA ultimately deleted the proposed requirement.), https://cppa.ca.gov/regulations/pdf/20230329_final_sor_app_a_comments.pdf.

[46] *See, e.g.*, *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1521–23 (1997) (holding that customer lists may qualify as trade secrets where the information is nonpublic, commercially valuable, and protected from disclosure with reasonable efforts).

[47] While our comments her focus on N.J.A.C. § 13:45L-7.3(a)(2) (proposed), we also note that

[48] Federal Trade Commission, *Bringing Dark Patterns to Light* 1 (Sept. 2022) (describing dark patterns as manipulative design practices that "can have the effect of obscuring, subverting, or impairing consumer

Rules appear to reflect this basic principle when they require that "[c]hoice options shall not be presented with a preselected or default option."[49]

However, the wording of this requirement may have unintended consequences. It may prevent controllers from continuing to rely on user interfaces for opting out that are fair, accurate, and free of dark patterns just because they use easily recognizable and usable mechanisms like checkboxes or toggle switches.[50] For example, many websites present users with a checkbox that enables them to opt out by clicking the box.[51] However, because checkboxes reflect a mutually exclusive, binary choice (checked or unchecked), it is impossible to present a checkbox that does not have "presented with a preselected or default option."[52] Similarly, many websites use toggle switches that enable consumers to change their preferences from opted-out to opted-in.[53] Like checkboxes, it is impossible to present these toggle switches without a "preselected or default option."[54] While these types of user interfaces *can* be used improperly – for example, presenting them to a user with the more permissive default when opt-in consent is required – they are entirely appropriate for opt-out rights where the expectation is that consumers will take an affirmative action (*e.g.*, un-checking a checkbox or toggling off a switch) to exercise their opt-out rights.

---

autonomy and decision-making"), https://www.ftc.gov/reports/bringing-dark-patterns-light; NAI, *Best Practices for User Choice and Transparency* 9-14 (April 2022) (detailing best practices for companies to avoid dark patterns when providing effective notice and choice for consumers), https://thenai.org/best-practices-for-user-choice-and-transparency/.

[49] N.J.A.C. § 13:45L-1.5(a)(8) (proposed).

[50] *See generally* Eduard Kuric, *What Makes a Great Toggle Button?* Smashing Magazine (Aug. 22, 2022) ("With toggle switches, it's **relatively simple** [to make evident which button is active]. With a direct label present (on/off), you can read the toggle state quite easily.") (emphasis added), https://www.smashingmagazine.com/2022/08/toggle-button-case-study-part-1/; U.S. Web Design System, *Checkbox*, U.S. General Services Administration ("Checkboxes are an **easily understandable** way to indicate that users can select one or more answers to a question or items from a list.") (emphasis added), https://designsystem.digital.gov/components/checkbox/; *User Interface Design Tips: Checkboxes vs Toggle Switches*, DMC (Nov. 27, 2018) (describing checkboxes and toggle switches as "two of the most common controls" to facilitate user input as user make choices on an interface or application), https://www.dmcinfo.com/blog/22434/user-interface-design-tips-checkboxes-vs-toggle-switches/#:~:text=When%20to%20Use%20a%20Toggle,settings%20before%20they%20apply%20them).

[51] *See*, *e.g.*, Nike.com, Nike, Inc. (2025) (presenting users with a checkbox to exercise privacy choices after scrolling to the bottom of the webpage and clicking the footer link titled "Your Privacy Choices").

[52] DMC, *supra* note 49 (describing a checkbox control as having "two states: unselected and selected"). U.S. Web Design System, *supra* note 49 ("Each checkbox has two different states: selected or unselected, which are similar to an on and off switch.").

[53] *See*, *e.g.*, cnn.com, Warner Bros. Discovery (2025) (presenting users with a toggle switch to exercise privacy choices after scrolling to the bottom of the webpage and clicking the "Do Not Sell or Share My Personal Information" link in the website footer.).

[54] DMC, *supra* note 49 (describing a toggle switch as an "'either/or' control that allows users to turn things on or off, like a light switch."). Kuric, *supra* note 48 ("[T]here are two states that a light switch can be in: on or off, with nothing in between. Similarly, a digital toggle is a control with two … mutually exclusive states with one of them always set as the default value.").

The Proposed Rules already address abuses of user interfaces like the ones described above both through the definition of consent (requiring a "clear, affirmative action")[55] and through its separate prohibition on the use of dark patterns.[56] It is therefore both unnecessary and burdensome to impose overly-prescriptive design standards that would prevent controllers from properly using common opt-out user interfaces. To address this issue, the Proposed Rules should remove this requirement.

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-1.5(a)(8) as follows:

> ~~Choice options shall not be presented with a preselected or default option.~~

D. The Proposed Rules Should Be Amended to Reconcile Different Standards for Prompting Consumers for Consent After They Have Opted Out.

A defining feature of personal data processing with consumer permission – whether through consent or the exercise of opt-out rights – is that consumers must be free and unconstrained in making and updating their choices to reflect their preferences. That means consumers should be able to provide or withdraw their consent to certain processing at will; as well as to opt-out of processing easily and consent to processing they have previously opted out of. On the other hand, it is possible to abuse consumer choice structures by unduly manipulating consumers into making a choice that does not reflect their true preferences. One possible vector for this type of abuse would be to constantly pepper consumers with requests to consent to certain personal data processing after the consumer has opted out. Possibly to prevent that type of abuse, the Proposed Rules would require a controller to:

> *"wait at least 12 months from the date that a consumer cho[o]ses to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer before asking the consumer to consent to such processing."*[57]

However, the above blanket prohibition on prompting consumers for consent after they have opted out does not align well with an explicit allowance in the Proposed Rules for

[55] *See* N.J.A.C. § 13:45L-1.2 (proposed).
[56] *See id.* § 13:45L-1.5(c) (proposed).
[57] N.J.A.C. § 13:45L-3.4(f) (proposed).

controllers to request a consumer's consent after the consumer has opted out in certain circumstances. For example, the Proposed Rules allow that if a consumer has "opted out of the processing of personal data, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt out . . . [then] the controller may request the consumer's consent to process the consumer's personal data for that purpose[.]"[58] Similarly, when a controller detects a conflict between a consumer's opt-out request represented by an opt-out preference signal and a choice that consumer's specific privacy preferences set with that controller, the Proposed Rules allow the controller to prompt the consumer for consent.[59]

To align the Proposed Rules' general prohibition against requesting consent too frequently with other explicit allowances for requesting consent, the Division should simply clarify that the specific allowances control.

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-3.4(f) as follows:

> *Except as otherwise explicitly allowed by this chapter, a controller shall wait at least 12 months from the date that a consumer cho[o]ses to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer before asking the consumer to consent to such processing."*[60]

E. The Proposed Rules Should Be Amended to Allow a More Flexible Standard for Refreshing Consent.

The Proposed Rules require a controller to refresh consent for processing a consumer's personal data processing if the controller has not interacted with that consumer in the prior 24 months.[61]

While this proposed requirement would help prevent consumer consent from going "stale" or from allowing indefinite processing by a controller once granted consent, it also presents an arbitrary timeframe within which consent would need to be refreshed. New Jersey should adopt a more flexible standard that better aligns with other states that have addressed this issue by creating an exception to this requirement similar to the

[58] N.J.A.C. § 13:45L-7.5(d) (proposed).
[59] *See* N.J.A.C. § 13:45L-5.1(c)(3) (proposed).
[60] N.J.A.C. § 13:45L-3.4(f) (proposed).
[61] *See* N.J.A.C. § 13:45L-7.7(a) (proposed).

one found in the regulations implementing the Colorado Privacy Act.[62] It should do so by adopting the exception found in the Colorado regulations for circumstances where a consumer can easily access and update their opt-out preferences at any time.[63]

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-7.7(a) as follows:

> *(a) When a consumer has not interacted with a controller in the prior 24 months, the controller shall refresh consent in compliance with all requirements of this subchapter to continue processing sensitive data concerning a consumer or personal data concerning a known child pursuant to N.J.S.A. 56:8-166.12(a)4, or pursuant to N.J.S.A. 56:8 166.12(a)7, to continue processing the personal data of a consumer for purposes of targeted advertising, the sale of the consumer's personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer when the controller has actual knowledge, or willfully disregards, that the consumer is at least 13 years of age, but younger than 17 years of age.*
>
> …
>
> *(c) Controllers are not required to refresh consent under part (a) of this section where a consumer has access and ability to update their opt-out preferences at any time through a user-controlled interface.*

F. The Proposed Rules Should be Amended to Clarify How Controllers May Notify Consumers About a Conflict in Privacy Settings.

The Proposed Rules state that a controller shall not "[d]isplay a notification, pop-up, text, graphic, animation, sound, video, or any other interstitial content that degrades or obstructs the consumer's experience on the controller's web page or application in response to the opt-out preference signal."[64] However, given this restriction on obstructive content, the regulations should further clarify how controllers may "notify

[62] *See* 4 Colo. Code Regs. § 904-3, Rule 7.08(B) ("Controllers are not required to refresh [c]onsent . . . where a [c]onsumer has access and ability to update their opt-out preferences at any time through a user-controlled interface.").
[63] *See id.*
[64] *See* N.J.A.C. § 13:45L-5.1(c)(1)(iii) (proposed) (prohibiting controllers from displaying a notification, pop-up, text, graphic, animation, sound, video, or any other interstitial content that degrades or obstructs the consumer's experience" in response to an opt-out preference signal); *see also* N.J.A.C. § 13:45L-5.1(c)(1)(ii) (prohibiting controllers from changing the functionality or user experience of their product or service based on whether a consumer uses an opt-out preference signal, and giving as an example that users should have the "same experience" regardless of opt-out status).

the consumer" of a conflict between an opt-out preference signal and controller-specific privacy settings.[65] As it stands, the Proposed Rules appears to both prohibit and allow a "notification" from a controller in response to an opt-out preference signal in certain circumstances.

To address this issue, the Division should amend the Proposed Rules to clarify that notifications are allowed to address conflicting privacy settings.

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-5.1(c)(1)(iii) as follows:

> *[The controller shall not] display a notification, pop-up, text, graphic, animation, sound, video, or any other interstitial content that degrades or obstructs the consumer's experience on the controller's web page or application in response to the opt-out preference signal, except as reasonably necessary to notify the consumer of a conflict in privacy settings as permitted by N.J.A.C. §13:45L-5.1(c)(3).*

G. The Proposed Rules Should be Amended to Refine the Scope Opt-Out Choices Indicated by an Opt-Out Preference Signal.

The Proposed Rules define the scope that a controller must apply to a consumer's opt-out choice expressed through an opt-out preference signal as follows:

> *"The controller shall treat the opt-out preference signal as a valid choice to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or both, as indicated by the universal opt-out mechanism, for the associated browser, network, or device(s), and any consumer profile **associated** with that browser, **network**, or device(s), including pseudonymous profiles."*[66]

This language raises at least two significant concerns. First, it suggests that an opt-out preference signal transmitted from a single browser may require the controller to apply the opt-out across an entire network, to all devices using that network, and to any consumer profiles linked to that browser or network—including pseudonymous profiles. However, multiple consumers often share the same network connection (for example,

---

[65] *See id.* § 13:45L-5.1(c)(3) (proposed) ("If the opt-out preference signal conflicts with a consumer's controller-specific privacy setting that allows the controller to sell or share their personal data . . . the controller may notify the consumer of the conflict and give the consumer an opportunity to consent to the sale or sharing of their personal data") (emphasis added).

[66] N.J.A.C. § 13:45L-5.1(c)(1) (proposed) (emphasis added).

roommates in a shared house)[67] and extending one consumer's opt-out choice to other consumers on the network would not reflect those other consumers' preferences. As such, this expansive interpretation goes far beyond device-specific applicability and risks over-attributing a single individual's choice to other users in the same household, public setting, or shared workspace.

Because networks are routinely shared by multiple users[68] and IP addresses may rotate dynamically over time,[69] scoping the impact of an opt-out preference signal to the *network level* is overbroad.

Recommended Amendment to the Proposed Rules:

Revise N.J.A.C. § 13:45L-5.1(c)(1) as follows:

> *The controller shall treat the opt-out preference signal as a valid choice to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or both, as indicated by the universal opt-out mechanism, for the associated browser~~, network,~~ or device(s), and any consumer profile associated with that browser~~, network,~~ or device(s), including pseudonymous profiles.*

This revision preserves the efficacy of consumer choices expressed by opt-out preference signals, while preventing the choices made by one consumer from being applied to other, distinct consumers who may be using the same network.

IV. Transparency

A. The Proposed Rules Should Align the Required Timing of Disclosures to The NJDPA Statutory Standard.

In order for consumers to benefit from transparency into a controller's personal data processing activities, they must have timely access to information about that processing. The Proposed Rules would meet that goal by requiring controllers to provide certain

[67] *See, e.g.* Network Guides, *Network Address Translation (NAT): Sharing A Single IP Address*, https://network-guides.com/network-address-translation-nat-sharing-a-single-ip-address/ (explaining how multiple devices may connect to the same network and share the same IP address).
[68] *See id.*
[69] *See* Hztime LLC, *Understanding the difference: Dynamic vs. Static IP addresses* (2025), https://www.rsinc.com/dynamic-ip-address-is-better-than-a-static-one.php (describing that a dynamic IP address does not directly identify a person, and the same dynamic IP address may be used by different users at different times).

information to consumers a privacy notice "at or before the point of collection" of personal data.[70]

However, the "at or before" standard goes beyond the NJDPA statutory standard, which provides a more flexible standard directing controllers to provide consumers with privacy disclosures that are "reasonably accessible, clear, and meaningful[.]"[71]

The Division may have sought to align the required timing of disclosures in the Proposed Rules with those found in California. The CCPA's implementing regulations also use the "at or before" standard."[72] However, unlike the NJDPA, the statutory basis for that requirement in California is unquestionable, because the CCPA explicitly mandates that the relevant privacy information be provided "at or before the point of collection."[73] This is a key distinction: California's regulations are implementing a timing standard that the legislature embedded in the statute itself.

More concerning is a proposed requirement that the controller disclose the purpose for which the personal data is processed *before* the point of collection.[74] This phrasing imposes a specific timing mandate not present in the statute and could have significant operational effects. For example, it could require that disclosures appear *prior* to any data processing workflow or trigger screen interruptions—such as overlays, cookie walls, or splash pages—that delay access to content and may lead users to click past the notice without meaningful engagement.

While aligning requirements in New Jersey with those in other states is an important objective, and one the NAI is generally supportive of throughout our comments here, the pursuit of that objective by the Division through rulemaking must nevertheless be limited by boundaries of the NJDPA. Fortunately, other states that lack CCPA's

---

[70] *See* N.J.A.C. § 13:45L-2.1(c)(3) (proposed) ("A privacy notice shall . . . enable a consumer to understand, at or before the point of collection of any personal data, the nature and scope of the controller's processing operations") (emphasis added); 13:45L-2.1(d) ("A controller shall make the privacy notice . . . where consumers will encounter it at or before the point of collection of any personal data) (emphasis added); 13:45L-2.1(e) ("If a controller does not give the privacy notice . . . to the consumer at or before the point of collection of the consumer's personal data, the controller shall not collect personal data from the consumer") (emphasis added); 13:45L-2.4(b) ("A controller shall provide the notice to opt out . . . at or before the point of collection of personal data.") (emphasis added); 13:45L-6.2(b) ("When considering whether a new processing purpose is reasonably necessary to or compatible with the purposes disclosed to a consumer at or before the point of collection, a controller shall consider [multiple factors]") (emphasis added).

[71] N.J. Rev. Stat. § 56:8-166.6(a).

[72] *See* Cal. Code Regs., tit. 11 § 7012(c) ("The Notice at Collection shall be made readily available where consumers will encounter it *at or before* the point of collection of any personal information") (emphasis added).

[73] *See* Cal. Civ. Code § 1798.100(a) ("A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers . . .") (emphasis added).

[74] N.J.A.C. § 13:45L-6.1(b) (proposed) ("The purpose [for processing personal data] must be disclosed before the collection of a consumer's personal data") (emphasis added).

statutory mandate for the "at or before" standard provide another model focusing on disclosures that are reasonably accessible to consumers, and the Division has an opportunity to follow those states without stretching its rulemaking authority. A "reasonably accessible" standard – focusing on general accessibility, rather than specific timing – mirrors the standard set in other states that share a statutory structure more similar to the NJDPA, such as in Colorado.[75]

To better align with the statutory standard and preserve implementation flexibility, the Division should revise the language revert to the "reasonably accessible" standard in the statute, instead of the more prescriptive "at or before the point of collection" standard that departs from the statute.

Recommended Amendments to Text of Proposed Rules: Revise N.J.A.C. § 13:45L-2.1(c)(3) and other relevant parts of the Proposed Rules noted above as follows:

> *A privacy notice shall . . . [e]nable a consumer to understand~~, at or before the point of collection of any personal data,~~ the nature and scope of the controller's processing operations in a reasonably accessible, clear, and meaningful manner, consistent with N.J.S.A. § 56:8-166.6(a).*

Regardless as to whether the Division adopts this recommendation, the Division should also consider clarifying with examples what satisfies its expectations under the NJDPA for how and when disclosures should be presented, such as providing links or illustrations of acceptable timing of notice disclosures. California, for example, lists five "[i]llustrative examples" to demonstrate the timing of notice disclosure.[76] Further, if the Division declines to adopt this recommendation and retains a notice-at-collection standard at odds with the NJDPA, it should also consider addressing the issue of collection of personal data by a third party via a first party digital property to align with California.[77]

---

[75] *See* 4 Colo. Code Regs. § 904-3, Rule 3.02(A)(4) (requiring that disclosures be made available through a "readily accessible interface" that consumers use "in conjunction with the [c]ontroller's product or service", rather than prescribing a specific moment when the disclosure must appear).

[76] *See* Cal. Code Regs., tit. 11 § 7012(c) (1-5) (providing illustrative examples of how and when a business must provide a Notice at Collection, such as posting a conspicuous link on webpages where personal information is collected or linking to the notice on a mobile application's download page and within the app, including via its settings menu).

[77] *See id.* § 7012(g).

V. Consumer Requests & Authorized Agents

A. The Proposed Rules Should be Amended to Limit the Scope of Deletion to What the Consumer Has Requested.

The Proposed Rules provide instructions to controllers for how to comply with a valid request from a consumer to delete that consumer's personal data. Specifically, they state:

> *"[w]hen a consumer exercises the right to deletion, the controller shall . . . [n]otify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the need to delete the consumer's personal data."*[78]

Similarly, the Proposed Rules provide instructions for complying with opt-out requests as follows:

> *"[w]hen a consumer exercises the right to opt out, a controller shall . . . [n]otify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the consumer's choice to opt out and direct them to comply with the consumer's choice and forward the request to any other person to whom the third party has made the personal data available during that time period."*[79]

Notably, these instructions would extend the meaning of a deletion or opt-out request submitted by a consumer beyond the consumer's expressed intent. Instead, the Proposed Rules would apply the consumer's request to an indeterminate set of additional controllers with whom the consumer has not made an opt-out or deletion request. The Proposed Rules should refrain from presupposing that a consumer's requests extend to controllers that the consumer has not directly submitted a deletion request to.

Further, the statutory language in NJDPA does not support this extension of consumer requests. In contrast, California's CCPA includes statutory language that directly requires businesses to forward deletion requests to third parties, a requirement that is also implemented in California's CCPA regulations. In contrast, the NJDPA does not include any statutory basis for forwarding deletion requests to third parties, and the Division should not attempt to extend its rulemaking authority to an area that other states have relied on their legislature to speak to. Still, not even California purports to

[78] N.J.A.C. § 13:45L-3.7(a)(3) (proposed).
[79] *Id.* § 13:45L-3.4(a)(4) (proposed).

extend consumer opt-out requests to third parties.[80]

Recommended Amendments to the Proposed Rules:

Revise 13:45L-3.7(a)(3) as follows:

(a) When a consumer exercises the right to deletion, the controller shall:

1. *Delete the consumer's personal data;*
2. *Using technical, organizational, or other measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e), instruct the processors that process personal data on the controller's behalf to delete the consumer's personal data held by the processors; and*
3. ~~*Notify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the need to delete the consumer's personal data*~~

Revise § 13:45L-3.4(a)(4) as follows:

(a) *When a consumer exercises the right to opt out, a controller shall:*

1. *Refrain from processing the consumer's personal data for the opt-out purpose, or purposes, if the controller has yet to process any of the consumer's personal data;*
2. *Cease processing the consumer's personal data for the opt-out purpose, or purposes, as soon as possible, but no later than 15 days from the date the controller receives the request, and delete any of the consumer's personal data processed for the opt-out purpose, or purposes, after the consumer exercised the right to opt out;*
3. *Use technical, organizational, or other appropriate measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e) to ensure that the processors that process personal data on the controller's behalf stop processing the personal data, as needed, to effectuate the consumer's choice to opt out;*
4. ~~*Notify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the consumer's choice to opt out and direct them to comply with the consumer's choice and forward the request to any other*~~

[80] *See* Cal. Civ. Code § 1798.120 (describing controller's post opt-out obligation to not sell or share, but no obligation specified to notify third parties). *But see* Cal. Code Regs., tit. 11 § 7026(f)(2) (a business must notify "all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period."). The Division could consider following this standard from the California regulations in lieu of a blanket requirement to notify third parties.

~~*person to whom the third party has made the personal data available during that time period.*~~

B. Authorized Agent Verification – Require Agents to Follow Controller Instructions

The Proposed Rules require that a privacy notice must include "[c]lear and conspicuous instructions on how an authorized agent may opt out of the processing of personal data on a consumer's behalf."[81] The use of authorized agents can represent a powerful method to assist consumers in exercising their privacy rights across multiple businesses. However, in order for authorized agents to act effectively on behalf of consumers without creating new privacy risks,[82] it is imperative not only that controllers post instructions for authorized agents, but that authorized agents are required to *adhere* to those instructions.

As such, the Division should update the Proposed Rules to include a corresponding requirement that authorized agents follow the instructions posted by controllers when submitting privacy rights requests on behalf of consumers.

In addition, the NAI is supportive of the requirement in the Proposed Rules that an "authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information"[83] because authorized agents often handle potentially sensitive information about consumers and should not send it to controllers who cannot act on it or do not need it to act on consumer requests.

Recommended Amendment to the Proposed Rules:

Add a new section 13:45L-4.4(e) as follows:

> *(e) An authorized agent shall reasonably adhere to instructions provided by a controller in compliance with N.J.A.C. § 13:45L-2.2(a)(7)(ii) for opting out of the processing of personal data on behalf of a consumer.*

---

[81] N.J.A.C. § 13:45L-2.2(a)(7)(ii) (proposed).
[82] *See* Tony Ficarrotta, *Some Authorized Agent Providers Are Selling Privacy Snake Oil and Why it Needs to Stop*, IAPP (Feb. 13, 2024), https://iapp.org/news/a/some-authorized-agent-providers-are-selling-privacy-snake-oil-and-why-it-needs-to-stop (op-ed describing how some authorized agent services mislead consumers, submit excess personal data inappropriately, and create new privacy risks by failing to follow consistent, secure, and lawful procedures).
[83] N.J.A.C. § 13:45L-4.4(c) (proposed).

*****

The NAI appreciates the opportunity to submit comments to the Division on the Proposed Rules. If we can provide any additional information or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at tony@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

Respectfully submitted,

Tony Ficarrotta

Vice President, General Counsel

Network Advertising Initiative (NAI)