# Comments of Consumer Reports
# In Response to the New Jersey Division of Consumer Affairs' Proposed Rules Implementing the New Jersey Data Privacy Act

by

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

September 2, 2025

Consumer Reports[1] appreciates the opportunity to provide comments on the Proposed Rules (rules) issued by the New Jersey Division of Consumer Affairs (Division) implementing the New Jersey Data Privacy Act (NJDPA). We thank the Division for its diligent work to create these rules and solicit stakeholder feedback. Consumer Reports' comments are informed by our extensive state-level privacy work—including multiple rounds of comments on previous rulemaking proceedings in California[2] and Colorado[3] that resulted in rules similar to the ones proposed by the Division.

Our comments reflect our learnings and research on the real-world impact of those existing rules, as well as our guiding belief that privacy regulations should seek to interpret the law in a way that is maximally protective of consumers while remaining within the confines of the underlying statute.

On that front, we should note that we've previously written that the NJDPA is not as strong as it should be.[4] Like many state privacy laws, it relies on the failed notice-and-choice framework that puts the onus of protection almost entirely on consumers themselves, rather than regulated businesses. This structure allows businesses to continue collecting whatever personal data they

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] See e.g., Justin Brookman, Maureen Mahoney, and Nandita Sampath, Comments of Consumer Reports In Response to the California Privacy Protection Agency Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21), November 8, 2021, https://advocacy.consumerreports.org/wp-content/uploads/2021/11/Consumer-Reports-CPRA-Comments-No.-01-21-11.08.21.pdf; Justin Brookman, Comments of Consumer Reports In Response to the California Privacy Protection Agency's Proposed Rules under the California Privacy Rights Act of 2020, (August 23, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/08/CPPA-regs-comments-summer-2022-1.pdf

[3] Justin Brookman, Initial Comments of Consumer Reports In Response to the Colorado Department of Law's Proposed Draft Rules Interpreting the Colorado Privacy Act, Consumer Reports, (November 7, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-initial-CPA-regs-Nov-2022-4.pdf; Justin Brookman and Matt Schwartz, Comments of Consumer Reports In Response to the Colorado Department of Law's Revised Draft Rules Interpreting the Colorado Privacy Act, (January 18, 2023), https://advocacy.consumerreports.org/wp-content/uploads/2023/02/1-18-23-Comments-of-Consumer-Reports-In-Response-to-the-Colorado-Department-of-Laws-Revised-Draft-Rules-Interpreting-the-Colorado-Privacy-Act-1.pdf

[4] Matt Schwartz, Consumer Reports Opposes New Jersey S. 332, (December 18, 2023), (though the final legislation ultimately added universal opt-outs and administrative rulemaking, which improved it substantially), https://advocacy.consumerreports.org/wp-content/uploads/2023/12/Consumer-Reports-Opposes-NJ-S.-332-12-15-23-1.pdf

want and using it for essentially any reason they want as long as they disclose that practice in their privacy policies—policies that very few consumers read or could even decipher if they did—meaning the status quo of massive data collection and sale continues uninterrupted. It also simply contains too many loopholes and instances of ambiguous drafting. We plan to continue to advocate to New Jersey lawmakers to improve the law. With that said, we appreciate the Division has clearly gone to great lengths to attempt to clarify many of these areas and advance the statute's underlying goal of advancing consumer privacy protections.

Many of our comments involve the proposed standards for universal opt-out mechanism (UOOM). Consumer Reports is a founding member of the Global Privacy Control (GPC) project, an open-source, web-based Universal Opt Out Mechanism (UOOM) with over 50 million unique users each month.[5] Consumer Reports's Director of Technology Policy Justin Brookman is a contributing editor to the project. However, these comments reflect the views only of Consumer Reports and are not necessarily representative of other project participants.

Consumer Reports is supportive of a substantial portion of the Proposed Rules. For example, we appreciate that the following requirements are currently included and would urge the Division to retain them in any future version of the rules:

- Controllers must establish and maintain a data inventory (Section 13:45L-6.3(b)(2))
- Controllers are not required to authenticate identity for opt-out requests (Section 13:45L-4.1(b))
- Controllers must wait at least 12 months after opt-out before requesting opt-in consent (Section 13:45L-3.4(f))
- The use of personal data for developing AI can only be achieved with consent (Section 13:45L-1.3 (d)(1)(ii))
- Controllers must test opt-out flows for functionality (Section 13:45L-1.5(a)(5))
- Controllers cannot bundle consent for incompatible processing purposes and cannot force consumers to consent to the unnecessary processing of personal data as a condition of receiving the product or service (Section 13:45L-1.5(a)(4)(ii) and Section 13:45L-7.2(a)(2)(ii))
- Controllers cannot obtain consent via dark patterns (Section 13:45L-1.5(a))
- Publicly available information does not include personal data collected via scraping or collected from data brokers (Section 13:45L-1.2)

At the same time, we recommend a number of narrow modifications on a few key points to ensure that the NJDPA's new rights are functionally usable and effective for consumers. Specifically, we urge the Division to:

- Amend or provide additional clarity regarding certain key definitions, including the definition of "access request", "data broker", "publicly available information", and "targeted advertising"

[5] Global Privacy Control, https://globalprivacycontrol.org/.

- Clarify the scope of the proposed restrictions against bundling of incompatible consent requests
- Issue clearer guidance on how companies may authenticate residency and legitimacy
- Require controllers to clearly disclose that they are covered by the NJDPA and list New Jersey if they list other states where they are required to honor privacy rights
- Clarify that consumers may opt-out of sales of personal information collected through loyalty programs without withdrawing from the program entirely
- Clarify that opt-out requests do not always double as deletion requests
- Clarify that entities that indirectly collect consumer data must abide by deletion requests
- Certify GPC as a legally-binding opt-out mechanism
- Remove unnecessary burdens on UOOMs that will result in opt-out friction

We will explain each of these points further below in discussing various sections of the Proposed Rules:

**Section 13:45L-1.2 (Definitions)**

*"Access request"*

The current definition of "access request" seems to imply that access requests only confer the ability for consumers to *confirm:* 1) whether the controller processes the consumer's personal data, *or* 2) that the controller provides access to the data. This definition should be amended to clarify that access requests allow consumers to both confirm that a controller processes their personal data *and* to actually receive access to their personal data. **Section 13:45L-3.5** clearly envisages a right that operates in this manner (which also reflects how the other 18 states with similar access rights function),[6] so the definition should be updated to harmonize with the rest of the proposed framework .

*"Data broker"*

We appreciate the strength of the existing definition of data broker, which covers persons or legal entities that collect, purchase or sell to third parties the personal data of consumers "with whom the person or legal entity does not have a direct relationship." However, we encourage the Division to include a definition for the term "direct relationship," to help establish the bounds of that term more clearly than in the provided examples, as well as to recognize that the practice of data brokerage is context specific. Modern businesses process data in a wide variety of circumstances. A controller may maintain a business line where they sell information about consumers that they did not directly collect from them (e.g. information collected from tracking technologies placed on third-party websites), while having another business line where they

[6] IAPP, US State Privacy Legislation Tracker, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

directly interact with consumers.[7] The fact that the business sometimes interacts with consumers directly shouldn't allow them to escape regulatory scrutiny entirely.

Other jurisdictions are actively working to amend their laws to accommodate this understanding. For example, the California Privacy Protection Agency (CPPA) is in the process of finalizing its rules to include a definition for "direct relationship" that would clarify that "a business is still a data broker and does not have a direct relationship with a consumer as to personal information it sells about the consumer that it collected outside of a "first party" interaction with the consumer."[8] We encourage the Division to adopt a similar approach.

*"Publicly available information"*

The proposed definition of "publicly available information" is also quite strong—including important exclusions whereby publicly available information "shall not include the scraping of personal data or personal data obtained from data brokers that is not otherwise publicly available."

We are sympathetic to the view that scraping the contents of public webpages on an automated basis, collecting and arranging personal data derived from those webpages into a comprehensive dossier, and then selling those dossiers to third-parties goes beyond consumers' reasonable expectations about publicly available information. Companies like Clearview AI have deeply eroded the public trust by scraping billions of photographs of individuals (primarily sourced from publicly available websites) in the service of a product that allows anyone to instantly identify anybody else in real-time without their knowledge or consent.[9] We agree that controllers that scrape consumers' personal data in such a manner should, at a minimum, be required to allow consumers to exercise control over that information, such as deleting it, correcting it, or opting out of its sale or use for targeted advertising. However, there may be pro-social use-cases for scraping[10] (e.g. monitoring of records related to public officials, monitoring for bias in AI products) that this provision may negatively impact. We suggest the following narrowing language:

> *"Publicly available information" shall not include the scraping of personal information where the personal information is subsequently processed for commercial purposes.*

---

[7] Justin Sherman, Lawfare, Federal Privacy Rules Must Get "Data Broker" Definitions Right, (April 8, 2021) https://www.lawfaremedia.org/article/federal-privacy-rules-must-get-data-broker-definitions-right

[8] California Privacy Protection Agency, Proposed Regulations on Accessible Delete Mechanism – Delete Request and Opt–out Platform ("DROP") System Requirements (Text of Proposed Rules), https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_text.pdf

[9] Kashmir Hill, the New York Times, The Secretive Company That Might End Privacy as We Know It, (January 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[10] Joe Jerome, Center for Democracy and Technology, Ethically Scraping and Accessing Data: Governments Desperately Seeking Data, (May 3, 2018) https://cdt.org/insights/ethically-scraping-and-accessing-data-governments-desperately-seeking-data/

Relatedly, the Division should clarify that no obligations under the NJDPA or Rules shall be construed to limit "noncommercial" activities, which should include, at a minimum, activities that state or federal courts have recognized as political speech and journalism.The Colorado privacy rules incorporate a similar concept.[11]

At the same time, we recommend that the Division clarify that consumer profiles based on a combination of public and private information are not "publicly available information." Data brokers often combine publicly available information with non-public information, sometimes further appended with the data broker's own inferences about the consumer, to create consumer profiles that are then sold to third-parties.[12] These profiles and inferences should not be considered publicly available information just because they may have been created in part from publicly available information—especially when they are being sold to third-parties without the awareness or consent of consumers.

We also ask that the Division clarify that non-public information *held* by data brokers is also not considered publicly available information. The Division's proposed exclusion for "personal data *obtained* from data brokers that is not otherwise publicly available" [emphasis added] may otherwise give data brokers the impression that non-public information is in fact publicly available information until they share it with third parties.

In addition, the Division should consider excluding from the definition of publicly available information any personal data that is made available for sale. Such a construct would allow people to delete commercial data profiles about them that are purely compiled from public sources (e.g. people search site results) that can lead to immense risk for individuals and public officials.[13]

*"Targeted advertising"*

The treatment of targeted advertising is one of the most important aspects of a privacy law. As discussed above, many state privacy laws, including the NJDPA, don't include any default protections against harmful secondary data uses, leaving it up to consumers to opt-out of unwanted data sales and sharing for the purposes of targeted advertising. It is therefore critical that the definition of "targeted advertising" and scope of the corresponding opt-out are protective and aligned with reasonable consumer expectations. Unfortunately, like many other state laws

---

[11] Colorado Privacy Act Rules, Rule 2.02 ("Noncommercial Purpose"), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

[12] Yael Grauer, Vice, What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?, (March 27, 2018), https://www.vice.com/en/article/what-are-data-brokers-and-how-to-stop-my-private-data-collection/

[13] Lily Hay Newman, Wired, Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses, https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/, (June 16, 2025)

based on a similar model,[14] New Jersey's statutory definition of "targeted advertising" is contested.

Under the NJDPA, targeted advertising means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests."[15] While in our view it is clear that this definition is inclusive of the practice of re-targeting (displaying targeted ads on a third-party's website based on the consumer's behavior on the first-party website), some businesses disagree,[16] arguing that data needs to be shared between *multiple* websites before the definition of targeted advertising is triggered.

As an initial matter, such advertising—such as a pair of shoes that follows you all over the internet after you had left a merchant's site—are the stereotypical example of targeted advertising; it is difficult to believe that legislators intended on excluding it from the scope of the law. But even on a technical level, this type of targeted advertising in many cases *does* require the collection of personal data by multiple parties (1. the retailer site that collects the browsing history and creates a persistent identifier, 2. the publisher that also collects personal data and then matches the consumer to that persistent identifier, and 3. other ad-tech intermediaries that help to place ads on behalf of businesses [sometimes comingling data from *dozens* of different retailers]).

The Division should propose an illustrative example in order to clarify this distinction along the lines of the following:

> *Retailer A shows personalized ads to consumers on third-party websites after they leave Retailer A's website. When a consumer visits Retailer A's website and views a pair of shoes, Retailer A collects that information and shares it Ad Tech Company B, which then gives the consumer a unique identifier.*
>
> *Later, when the consumer visits Publisher C's website, the consumer is shown an ad for the same pair of shoes they viewed on Retailer A's website. Ad Tech Company B selects and delivers this advertisement by matching information they have collected about the consumer from Retailer A with information they collected from Publisher C.*

---

[14] Of the state comprehensive laws, only California has a meaningfully different definition of targeted advertising.
[15] NJDPA, C.56:8-166.4, https://pub.njleg.state.nj.us/Bills/2022/PL23/266_.PDF
[16] Matt Schwartz et al., Consumer Reports, Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws, https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf (April 1, 2025). In response to our findings that Pottery Barn had engaged in retargeting, ignoring consumer opt-out requests, they responded: "The advertising activity that you described is not meant to be controlled by GPC or by do not sell or share opt outs under applicable state privacy laws. GPC and those laws provide an opt out from advertising based on interactions with multiple websites, often called cross-context behavioral advertising."

*This practice constitutes targeted advertising under the NJDPA, as it involves displaying advertisements to a consumer that are selected based on personal data obtained over time and across nonaffiliated websites to predict consumer preferences or interests. Both Retailer A and Publisher C must provide the consumer with appropriate disclosures and honor the consumer's opt-out of targeted advertising rights under the law.*

**Section 13:45L-1.5 (Requirements related to user interface design, choice architecture, and dark patterns)**

**Section 13:45L-1.5(a)(4)(ii)** contemplates a restriction where controllers may not force consumers to consent to "the use of personal data for any purposes that are incompatible with the context in which the personal data was collected" at the same time that consumers must consent to processing purposes necessary to provide the service. The Division illustrates this by providing an example of an impermissible consent structure, where a gas price finder app requires a consumer to consent to the sharing of their geolocation data with data brokers at the same time as consenting to "a reasonably necessary and proportionate use of geolocation data for providing the location-based service" (e.g. the collection of the consumer's geolocation data).

A related requirement articulated in **Section 13:45L-7.2(a)(2)(ii)** contemplates a similar concept: consent must be freely given, and consent is not freely given when "[t]he performance of a contract depends on consent to process personal data that is not necessary to provide the goods or services contemplated by the contract."

Together, these two provisions seem intended to avoid a persistent problem with compliance with the vague consent structure under many similar state privacy laws.[17] As the gas finder example illustrates, businesses often make it impossible for consumers to meaningfully protect themselves by bundling unnecessary requests for data processing along with necessary requests. In the given example, if a consumer did not want to allow their data to be sold to data brokers, they would have no choice but to simply forgo using the app altogether. By requiring controllers to obtain separate consent for incompatible data uses, consumers will at least have the option to receive the core product or service without ceding total control over how their data is processed.

However, for both **Section 13:45L-1.5(a)(4)(ii)** and **13:45L-7.2(a)(2)(ii)** the Division should clarify that disclosures buried in privacy policies do not absolve controllers of the responsibility of obtaining separate consent. For example, under **Section 13:45L-1.5(a)(4)(ii)**, if a business simply discloses that they share personal data with data brokers in their privacy policy, that should not suddenly make the processing compatible with the context. That's how we read the current rules, but that isn't entirely clear. And in **Section 13:45L-7.2(a)(2)(ii),** what exactly are "the goods or services contemplated by the contract"? In our view, the "goods or services"

[17] Maggie Oates et al., Consumer Reports, Companies Continue to Share Health Data Despite New Privacy Laws, pg. 29, (January 16, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf

should simply mean the "product or service requested by the consumer", but controllers may argue that it includes every processing purpose they list in their privacy policy (e.g. sharing data with third-party social media companies). The Division should ensure that this is not a permissible interpretation.

In addition, we note that one side effect of the framework proposed in these rules is that consumers are going to be asked to make *more* consent decisions at a time when they are already suffering from extreme consent fatigue.[18] More than 15 years ago, researchers from Carnegie Melon University estimated that the average internet user encounters an average of 1,462 privacy policies a year, and that it would take a user an average of 244 hours per year to read the privacy policy of every website they visited.[19] The number (and length) of privacy policies, permissions, and consent notice, have surely only skyrocketed since then.

That's why CR supports the concept of data minimization—the idea that privacy laws should restrict businesses to only collect and use personal information that is necessary to provide the service requested by consumers. By putting the onus of protection on businesses, consumers are spared from making endless consent choices or having to read company privacy policies. With that said, we recognize that the Division is limited by the underlying statute that relies on notice-and-choice. In the given context, ensuring that consumers have a more meaningful choice (even if that means a deluge of notices) is the more privacy-protective option, and we support the Division's approach.

Finally, we appreciate that **Section 13:45L-1.5(a)(5)** requires companies to test their opt-out processes to ensure they are functional. Through our research[20] and work as an authorized agent,[21] we consistently observe opt-out flows that are simply broken, circular, or do not appear to change the controller's data sharing behavior.[22] And when we tested how major retailers are abiding by opt-out provisions in other state privacy laws, we found that a significant portion of them appeared to be out of compliance.[23] Opt-out provisions aren't a niche component of state privacy laws; they are in many ways the core consumer protection. They provide consumers with an actionable step to protect their data from flowing in unwanted directions and if businesses aren't complying with them, it makes one wonder how they are complying with the other requirements present in the law. By creating an affirmative obligation to test these opt-out

---

[18] Luis Montezuma and Tara Taubman-Bassirian, IAPP, How to Avoid Consent Fatigue, (January 29, 2019), https://iapp.org/news/a/how-to-avoid-consent-fatigue

[19] Aleecia M. McDonald and Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society, The Cost of Reading Privacy Policies, (2008), https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[20] Matt Schwartz et al., Consumer Reports, Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws, https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf, (April 1, 2025)

[21] Consumer Reports, Permission Slip, https://innovation.consumerreports.org/initiatives/permission-slip/

[22] Maggie Oates et al., Consumer Reports, Companies Continue to Share Health Data Despite New Privacy Laws, pg. 29, (January 16, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf

[23]

flows, controllers will have little excuse if enforcers determine that there are compliance issues later on.

**13:45L-2.1 Privacy notice required**

**Section 13:45L-2.1(b)** states that "[a] controller is not required to provide a separate New Jersey-specific privacy notice or section of a privacy notice, as long as the controller's privacy notice meets all requirements of this subchapter." While we understand the intent of this provision (businesses should not be expected to maintain different privacy policies for each of the 19 [largely overlapping] state privacy laws), we urge the Division to add some additional disclosure requirements to ensure that New Jersey residents will better understand what rights are available to them.

Without an explicit acknowledgement that a given business is covered by the law, it can be difficult for consumers to know when the business is obligated to comply. Consumers typically have no visibility into the criteria used to determine coverage under the law (e.g. number of consumer records processed in a calendar year, or annual revenue) and there are a large number of exemptions that may relieve the business of their obligation to comply that are likely confusing to the average person.

Furthermore, in practice, businesses often list in their privacy policy the states where they are obligated to provide consumer privacy rights. If a controller uses this formulation, they should be required to state that they provide privacy rights to New Jersey residents as well—otherwise consumers may not realize that they are protected. The Oregon DOJ highlighted this exact concern in their 6-month enforcement report earlier this year, saying: "notices that name one or two states in the "your state rights" section but not Oregon, giv[e] consumers the impression that privacy rights are only available to people who live in those named states."[24]

We suggest that the Division introduce a requirement along the lines of recent guidance from the Delaware AG:

> *While the DPDPA does not require a Delaware specific section, the description of consumer rights must unambiguously indicate those rights are available to Delaware residents. Statements such as "you may have rights" or "if your state has a data privacy law" are not sufficiently clear to inform Delaware residents of their rights and, therefore, do not comply with the DPDPA. Businesses must state the described consumer rights may be exercised by either (i) all users or all United States users or (ii) clearly describe the subset of users, including explicitly identify Delaware residents, among residents of other states.*[25]

---

[24]Oregon Department of Justice, Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months, (March 2025), https://www.doj.state.or.us/wp-content/uploads/2025/03/OCPA-Six-Month-Enforcement-Report.pdf

[25] Delaware Department of Justice, Delaware Personal Data Privacy Act Frequently Asked Questions, "Does the DPDPA require a businesses include a Delaware specific consumer rights section in its privacy

**13:45L-2.4 (Privacy notice content)**

We recommend the Division provide for clear and prominent disclosure to consumers *outside* of a privacy policy for any profiling that produces "legal or similarly significant effects." While the proposed rules provide for notice of the possibility of such processing within a privacy policy, consumers generally do not read privacy policies and anyway such generalized notice will not meaningfully inform consumers when such sensitive processing will actually happen. Due to the high stakes and relative infrequency of such data processing, pre-use notice outside of a privacy policy is justified.

Companies are increasingly using AI—and less sophisticated algorithms—to make important decisions about consumers: who is selected for a rental unit, who is approved for a mortgage, who is hired for a dream job, who gets what medical care, and more. While these products can speed decision making, they can also be flawed. They can bake in bias,[26] rely on incorrect information,[27] or make recommendations based on spurious connections.[28]

These notices of automated profiling with significant legal or similar effects could include:

- the specific decision that is about to be made about the consumer,
- the categories of personal data that will be processed as part of the specific profiling decision,
- the type of output generated by the profiling if relevant, and
- A reminder that consumers have a right to access under NJ privacy laws, the fact that they could use it to access what specific information the controller has about them, and how to use it.

Such a pre-use notice would be consistent with California's recently promulgated regulations, which require a plain language description of the specific purpose for which the business plans to use profiling, how the profiling processes personal information to make the decision about the consumer, what categories of personal information affect the output of the profiling, the type of output generated by the profiling, and how the output is used to make the significant decision.[29]

**13:45L-2.5 (Loyalty program notice)**

---

notice?",
https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions/

[26] See eg. Ziad Obermeyer, Brian Powers, Christine Vogeli, Sendhil Mullainathan, "Dissecting racial bias in an algorithm used to manage the health of populations" Science 366, 447–453 (2019). https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-ziad_obermeyer.pdf

[27] Cyrus Farivar, NBC News, "Tenant screening software faces national reckoning", March 14 2021, https://www.nbcnews.com/tech/tech-news/tenant-screening-software-faces-national-reckoning-n1260975

[28] See eg. Elisa Harlan, Oliver Schnuck, BR24, "Objective or Biased: On the questionable use of Artificial Intelligence for job applications" February 16, 2021, https://interaktiv.br.de/ki-bewerbung/en/

[29] [cite to CA regs section 7220]

We are concerned that the Division's proposed rules regarding loyalty programs will allow businesses to unacceptably discriminate against consumers who use their opt-out rights under the law—a result that would significantly undermine one of the statute's core protections.

**Section 5 (C.56:8-166.8)** of the NJDPA provides that controllers are prohibited from discriminating against consumers for exercising their opt-out rights. This is a critical protection—without it businesses could simply deny consumers the underlying product or service they've requested in response to receiving an opt-out request, rendering the law's opt-out right meaningless. However, the section goes on to state that:

> *"[t]he provisions of this section shall not prohibit the controller's ability to offer consumers discounts, loyalty programs, or other incentives for the sale of the consumer's personal data, or to provide different services to consumers that are reasonably related to the value of the relevant data, provided that the controller has clearly and conspicuously disclosed to the consumer that the offered discounts, programs, incentives, or services include the sale or processing of personal data that the consumer otherwise has a right to opt out of.*

The Division should clarify that a consumer's decision to opt-out of sales and targeted advertising using their data never[30] ***prohibits*** a controller's ability to offer a loyalty program. Controllers do not strictly need to sell data to others or to engage in cross-context behavior advertising in order to operate loyalty programs—such behaviors have nothing to do with the tracking of purchases to offer discounts or the ability to offer first-party advertising. While the secondary (and unanticipated) repurposing of data collected through loyalty programs is certainly a newer and growing phenomenon, this is simply an additional monetization tactic,[31] rather than the purpose of the program as such. Indeed, the idea that companies are quietly selling consumers' data behind their backs is precisely why strong privacy protections are needed in the first place.

Worryingly, **Sections 13:45L-2.5(a), (c),** and **(d)** suggest just the opposite—that loyalty programs can *only* be offered when the benefits offered are reasonably related to the value of the processing or sale of the consumer's personal data. This structure ignores the fact that businesses may offer loyalty programs for any number of reasons (e.g. to gain market share over a competitor, to drive a higher frequency of purchase, to promote a given product) that have nothing to do with data sales.

---

[30] Depending on the Division's interpretation of the term "sale," certain joint loyalty programs that allow consumers to spend loyalty rewards on other brands (such as an airline loyalty program that allows conversion of accrued miles to a partner hotel chain's point programs) could be impacted on a blanket prohibition on data "sales" conducted pursuant to a loyalty program. We would support an accommodation that allows consumers to engage in joint loyalty programs or programs that allow transfer of loyalty rewards to other merchants, so long as the data is only used to facilitate the loyalty program benefit and is not further sold.

[31] Jon Keegan, the Markup, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you (February 16, 2023)

Moreover, **Section 13:45L-2.5(e)(1)** requires controllers to provide a loyalty program notice that states that the consumer may opt out of the sale of personal data "if the consumer chooses not to participate in the loyalty program." Again, this is precisely backward. Consumers should have the ability to opt out of sales of their personal data collected through loyalty programs and still retain the benefit of the program. The Division should consider including an illustrative example along the lines of the following:

> *A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory and prohibited by the NJDPA.*

To be clear, we understand why privacy laws may need to include some exceptions to allow loyalty programs to function properly. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing that is functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. But that is not what the statute provides for—and, in fact, it is silent on how the anti-discrimination provisions apply when consumers utilize their non-opt-out rights (e.g. right to correct, delete, and know).[32]

This is also not to say that we read the statute as prohibiting financial incentives (e.g. one time gift cards) or differentiated services (e.g. pricing tiers) that are reasonably related to the value of the relevant data. Section 5 of the NJDPA clearly allows for these types of arrangements, and the proposed rules addressing them are generally reasonable. But there is a clear difference between these types of explicitly transactional arrangements for the sale of consumer data and loyalty programs, which present a fundamentally different value proposition to consumers.

**13:45L-3.2 (Exercising the right to opt out)**

The NJDPA affords consumers the right to opt out of the processing of their personal data for (a) targeted advertising, (b) the sale of their personal data, and (c) profiling in furtherance of decisions that produce legal or similarly significant legal effects. While processes for opting out of targeted advertising and data sale are relatively understood and mature (if not always effective), the practical application of the right to opt out of profiling is less clear, despite several states now offering it in their privacy statutes.

---

[32] Unlike many other state privacy laws, NJDPA's anti-discrimination provision only applies to opt-out rights, implying that businesses can discriminate against consumers who take advantage of their other rights (e.g. right to delete, right to know, right to correct) under the law. That deeply undermines the consumer rights under this bill— for example, a business could lock a consumer out of their account in response to receiving a request to delete or deny service to a consumer who requests to correct their data—and should be addressed by the legislature as soon as possible.

We recommend the Division adopt the approach recently taken by California by allowing companies to choose between offering a *post hoc* right to *appeal* a consequential profiling decision or to let consumers opt out altogether.[33] In many cases, an undefined right to opt out will be of limited utility to consumers who have little ability to assess whether a company's automated systems or human reviewers will be more advantageous; at the same time, allowing consumers to manually request a human perform a task in the same exact way as an automated system can be resource intensive for companies without offering any consumer benefit. In many cases, a right to appeal will be more valuable to consumers and more workable for companies if a consumer who has been denied a meaningful opportunity by a flawed profiling system has the ability to challenge a particular automated technique as unfair, ineffective, or inadvertently misconfigured.

In order to make sure a right to appeal is meaningful, the Division should also require companies that use profiling techniques for legal or similar consequences to inform consumers via an adverse action notice if a profiling system denied them such an opportunity. Such a requirement would mirror similar obligations under the Fair Credit Reporting Act where consumers denied credit or a similar opportunity because of an algorithmic credit report are entitled to be made aware of that fact. Such a notice should be delivered directly to the impacted consumer, and should include in clear and concise language:

- The specific decision that was made with respect to the individual consumer, and the result of that decision with respect to the consumer
- A plain language explanation of how the profiling software works
- 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
- The categories of personal information that affect the result of the profiling
- The role that profiling played in the decision and decision-making process (eg. Did automated profiling create a recommendation for a human decision-maker, or was the decision fully automated)
- Information about a consumer's right to access more information under NJDPA, along with their right to correct, and, if relevant, right to appeal.

By making consumers aware of the adverse action, they would have the opportunity to inspect the data the company holds about them and challenge the decision if they have good cause to believe there was an error.

**13:45L-3.4 (Right to opt out)**

**Section 13:45L-3.4 (a)(2**) states that upon receiving an opt-out request, a controller shall "[c]ease 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***"** [emphasis added].

[33] [cite to CA regs 7221]

While we are sympathetic to this provision, as it appears that it is intended to advance consumer privacy, it may result in unintended consequences that subvert consumer autonomy. There are many circumstances in which a consumer may wish to opt-out of sales or targeted advertising, but not delete their information from a business. For instance, a consumer may instruct a retailer to stop selling their data to third-parties, but it doesn't automatically follow that they'd also wish to delete their purchase history or account information. We urge the Division to simply delete the italicized portion of the provision above.

**Section 13:45L-3.4 (e)** states that "[a] consumer may use an authorized agent to opt out on the consumer's behalf if the consumer *expressly confirms* that the authorized agent may act on the consumer's behalf" [emphasis added]. Later in that Section, the Division writes, "the requirement to obtain and provide *written permission* from the consumer does not apply to requests made through an opt-out preference signal." **Section 13:45L-4.4(a) and (b)** then refers to a "*signed permission.*" It appears that these provisions are all referring to the same underlying requirement—we'd simply urge the Division to harmonize these different terms for the sake of clarity.

**13:45L-3.7 Right to deletion**

**13:45L-3.7(f)** replicates a requirement from Section 7(b) of NJDPA that a "controller that has obtained personal data about a consumer from a source other than the consumer shall comply with a consumer's deletion request" by *either:*

> *1. Retaining a record of the deletion request and the minimum data necessary to ensure the consumer's personal data remains deleted from the controller's records, provided that such data shall not be used for any other purpose; or*
> *2. Deleting such personal data.*

The Division should re-write this provision to clarify that controllers that have indirectly collected personal data about consumers must delete personal data upon request *and* maintain a record of the deletion for list-suppression purposes. It is unclear why the provision is presented as an option—even if a controller takes option #1, it is implied that the consumer's personal data must be deleted. If a controller takes option #2, they'd be deleting the consumer's data without maintaining a suppression list, which would undermine their ability to ensure the consumer's data stays deleted from their systems. The Division should remedy this drafting ambiguity by simply clarifying that controllers must delete personal data and maintain a suppression list.

**13:45L-5.1 Universal opt-out mechanism requests**

First, we appreciate that the Division has included FAQs that indicate that companies must treat Global Privacy Control (GPC) as a legally binding universal opt-out mechanism under the

NJDPA.[34] However, we urge New Jersey to align with other jurisdictions that designate rulemaking authority under their privacy laws, such as Colorado, that have already formally granted GPC legally binding status in their rules. Without clear guidance from regulators, controllers may take advantage of the statute's ambiguity or the rules' complex series of requirements to adopt a reading that allows them to ignore consumer opt-out requests sent in this manner.

To our knowledge, GPC is the only UOOM that has received widespread consumer adoption (over 50 million users) and business implementation (including at some of the largest privacy compliance software companies, like OneTrust).[35] California's Attorney General first legally blessed GPC via Tweet,[36] and later formalized his statement in FAQs.[37] Meanwhile, the Colorado Privacy rules provided for the Department of Law to "maintain a public list of Universal Opt-Out Mechanisms that have been recognized to meet the standards of this subsection."[38] The Department of Law accepted applications for UOOMs in late 2023 and selected a list of three potential UOOMs for consideration. The Department accepted public comment on the shortlist of UOOMs through December 2023, before releasing the final "list" of recognized UOOMs, which consists solely of GPC.

In order to solidify the legal standing of GPC, the Division could create an UOOM registry similar to Colorado's or could simply state that UOOM implementations included on another state's registry are deemed binding under New Jersey law. Some state privacy laws already utilize similar reciprocity frameworks for the concept of UOOMs in general.[39] Even more simply, the Division could state in the rules or related guidance that GPC meets the qualifications for UOOMs described therein. Recognizing GPC will help clarify to consumers how the law is intended to function, and will ward off any potentially bad faith readings of the law that conclude that GPC does not constitute an UOOM under the law.

Moving to the substantive requirements of this section, **Section 13:45L-5.1(c)(2)** states that:

> *[t]he controller shall not require additional personal data beyond that which is strictly necessary to:*

---

[34] New Jersey Division of Consumer Affairs, Cyber Fraud Unit, New Jersey Data Privacy Law FAQs, (FAQ 8), (January 15, 2025), https://www.njconsumeraffairs.gov/ocp/Pages/NJ-Data-Privacy-Law-FAQ.aspx
[35] Alex Cash, "Global Privacy Control: How to honor consumer opt-out requests," OneTrust, (August 25, 2022), https://www.onetrust.com/blog/global-privacy-control-how-to-honor-consumer-opt-out-requests/
[36] See: https://x.com/AGBecerra/status/1354849778819948545?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1354850321692934144%7Ctwgr%5E065e7273791d0d5c2dc3555e0bdd4e456603dfcf%7Ctwcon%5Es2_&ref_url=https%3A%2F%2Fdigiday.com%2Fmedia%2Fwhy-a-tweet-from-californias-ag-about-a-global-privacy-tool-has-companies-scrambling%2F
[37] Office of the California Attorney General, California Consumer Privacy Act (CCPA) FAQs 8-9, https://oag.ca.gov/privacy/ccpa
[38] See Colorado Privacy Act Rules, Rule 5.07(A), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf
[39] Texas Data Privacy and Security Act, Sec. 541.055 (e)(4), https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm; Nebraska Data Privacy Act, Sec. 11(5)(d), https://nebraskalegislature.gov/FloorDocs/108/PDF/Slip/LB1074.pdf

*i. Authenticate that a consumer is a resident of New Jersey; or*

*ii. Determine that the opt-out preference signal represents a legitimate request to opt out of the processing of personal data as permitted pursuant to N.J.S.A. 56:8-166.11(b).*

We strongly object to the idea that controllers should be permitted to request additional information to authenticate that the consumer is a resident of New Jersey in response to a universal opt-out request. Unlike other data rights (e.g. the right to delete), the risk of an erroneous opt-out request is very low to both the consumer and the business. Meanwhile, the burden of authentication to users can be so high that it has the effect of subverting their desire to opt out.

In Consumer Reports's investigation into the usability of privacy rights under an earlier version of CCPA, we found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.[40] CPPA has since clarified that businesses shall not require consumers to verify their identity for opt-out requests.[41] If every site in New Jersey responded to a UOOM signal with a request for residency verification, in practice UOOMs would be practically unusable and ineffective.

As a better alternative, many companies comply with state privacy laws by approximating geolocation based on IP address.[42] The Division should revise the rules to clearly state that estimating residency based on IP address is generally sufficient for determining residency and legitimacy for purposes of the NJDPA, unless the company has a good faith basis to determine that a particular device is not associated with a New Jersey resident or is otherwise illegitimate. The Rules should further state that additional data processing to confirm residency or legitimacy absent specific evidence to the contrary is prohibited.

We are also concerned that **Section 13:45L-5.1(c)(4)** replicates the Division's problematic approach for loyalty programs, as discussed above. It implies that an opt-out can conflict with a consumer's *participation* in a loyalty program, and allows controllers to notify consumers that abiding by the request would "withdraw the consumer from the loyalty program." We reiterate our position that data sales are never strictly necessary to operate a loyalty program and consumers should be able to opt out of such sales or targeted advertising, while remaining in the program. We urge the Division to remove this provision entirely.

---

[40] Maureen Mahoney, California Consumer Privacy Act: Are Consumers'Digital Rights Protected?, Consumer
Reports (Oct. 1, 2020),
https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

[41] California Consumer Privacy Act Regulations, Section 7060(b),
https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

[42]See, e.g., OneTrust, Configuring Geolocation Rules, (April 2, 2025),
https://my.onetrust.com/s/article/UUID-2229ff55-895a-11da-1b5f-79e1785b6e02?language=en_US

Finally, we urge the Division to amend **Section 13:45L-5.1(d)**, which stipulates that a controller "shall" give the consumer an opportunity to provide additional information in order to apply the requested opt-out in other contexts. As a general principle, the Division should exercise caution that its rules do not add undue friction to the experience of sending universal opt-outs, which was intended to be as easy and consumer friendly as possible. We are concerned that a mandate will empower controllers to throw up additional hurdles that make it harder for the consumer to effectuate their choice.

Many controllers simply will not need extra information in order to propagate the request to additional contexts, so asking for it will only create additional privacy risks. Only controllers that will extend the recognition of the consumer's use of the universal opt-out signal across platforms, devices, or offline should be permitted to ask for the additional information. This would align the Division's proposal with Colorado's Rule 5.05(C).[43] In addition, the Division should add a rule that states that in the event that the user is already authenticated to the controller, the controller should automatically and by default apply the requested opt-out rights to other contexts, such as on other devices when the consumer is authenticated, as well as offline use of that consumer's data.

**13:45L-5.2 Technical specification**

**Section 13:45L-5.2(a)(2)** states a universal opt-out mechanism must "clearly describe any limitations that may be applicable to the mechanism," such as that the mechanism "only allows the consumer to exercise the opt-out right for one specific purpose" or that it "applies only to a single browser or device."

We support the former requirement—UOOMs that are only intended to facilitate one or another of the opt-out purposes (e.g. sales or targeted advertising) should disclose that fact to consumers. However, we believe that it is inappropriate for the rules to require UOOMs to describe whether the effect of sending an opt-out request will be limited to a single browser or device. As contemplated in **Section 13:45L-5.1(d)** (discussed above), whether the signal is propagated to another context will be up to the controller, as well as the consumer's choice to input additional information. In other words, the UOOM itself would have no say in how controllers ultimately decide to interpret the signal. As such, **Section 13:45L-5.2(a)(2)(ii)** should be removed.

---

[43] Colorado Privacy Act Rules, Rule 5.05(C), reading: "Notwithstanding 4 CCR 904-3, Rule 5.05(B), a Controller may provide the Consumer with an option to provide additional Personal Data only if it will extend the recognition of the Consumer's use of the Universal Opt-Out Mechanism across platforms, devices, or offline. For example, a Controller may give the Consumer the option to provide their phone number or email address so that the Universal Opt-Out Mechanism or signal can apply to offline Sale of Personal Data or link the Consumer's opt-out choice across devices. Any information provided by the Consumer for this purpose shall not be used, disclosed, or retained for any purpose other than processing the opt-out request."
https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

We also urge greater clarity on **Section 13:45L-5.2(a)(6)** admonition that a UOOM developer must not allow its manufacturer to "unfairly disadvantage" any other controller. First, we'd note that the framing of this provision (i.e. "other controller") suggests that UOOMs are likely to be controllers. This is not necessarily the case—GPC, the only widely adopted UOOM, would not qualify as a controller under NJDPA (or any other state privacy law for that matter).[44] Nevertheless, we do recognize that there is a hypothetical risk of a future UOOM self-preferencing (e.g. a browser creating a UOOM that propagates opt-out requests to all websites except its own or that of its business partners).

But there are contexts where UOOMs *should* be allowed to treat different controllers differently. A consumer may want to install a UOOM that is targeted specifically at data brokers (or may configure a general purpose UOOM to only target data brokers); in that case, a consumer should be empowered to only send opt-out requests to data brokers. A UOOM may also process re-opt-in exceptions on behalf of the user, keeping track of the companies that a user grants an exception to to their general preference not to have used for certain processing. In that case, the UOOM may not send an opt-out signal to those companies to which the consumer has granted an exception. The Division should consider amending this provision to allow for selective UOOM implementations, or at least add an illustrative example of the narrow range of behavior this provision is explicitly intended to prevent, lest it prevent pro-consumer implementations.

**Section 13:45L-5.2(a)(7)** reflects a quirk[45] of the NJDPA whereby UOOMS may not opt consumers *into* the processing of their personal data. It is unclear how a UOOM could otherwise meet all of the obligations in the statute and proposed rules and behave in this manner, but we support the notion that UOOMs should not subvert consumer expectations in this way. We are not aware of any UOOM that opts consumers into data processing.

However, the statute and rules are currently silent on how UOOM defaults should work in the opposite direction; that is, whether UOOMs should be able to send opt-out signals by default. We urge the Division to adopt a new rule that clearly states that user agents specifically marketed as designed to safeguard privacy may reasonably infer a consumer's intent to broadcast a UOOM signal without further user interaction. This would align with Colorado Rule 5.04(B), which reads as such:

> [*A] consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed as a tool that will exercise a user's rights to opt out of the Processing of Personal Data using a Universal Opt-Out Mechanism, shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism. The marketing for such a tool may also describe functionality other than the exercise of opt out rights and it need not refer specifically to opt-out rights in the State of Colorado.*

---

[44] GPC is a technical specification—a HTTP header—on its own, it is incapable of collecting personal information, https://w3c.github.io/gpc/#expressing-a-do-not-sell-or-share-preference

[45] No other state privacy law envisages universal opt-outs opting people into data processing.

We also urge the Division to align itself with the CCPA regulations[46] and ensure that *preinstalled* privacy-focused user agents are also permitted to send universal opt-out signals by default. For example, a mobile phone or laptop could preinstall several different browsers from which a consumer selects in order to access the web. A consumer's choice of a privacy-focused one such as DuckDuckGo should be interpreted as an affirmative choice to stop unwanted tracking just as much as the user's installation of the same browser would be. Similarly, a user could choose to purchase a privacy-focused device that uses privacy-focused apps as default options (such as ProtonMail and Brave). In that case, the choice of the phone and use of those apps would be sufficient evidence of intent to protect their information.

**********

Thank you very much again for the opportunity to provide feedback on the proposed rules. We look forward to continuing to engage with the Division on this important proceeding. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwarz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.

[46] Rule 5.04(A) of the Colorado privacy rules currently forbid pre-installed devices (such as browsers or operating systems) from turning on universal opt-outs by default. California's rules contain no such prohibition.