Comments of the Electronic Privacy Information Center,
Consumer Federation of America, New Jersey Citizen Action, TechEquity Action, and the
Virginia Consumer Council

to the

NEW JERSEY DIVISION OF CONSUMER AFFAIRS
On Proposed Rulemaking Under the New Jersey Data Privacy Act

August 1, 2025

The Electronic Privacy Information Center (EPIC), Consumer Federation of America (CFA), New Jersey Citizen Action (NJCA), TechEquity Action, and Virginia Consumer Council submit these comments in response to the New Jersey Division of Consumer Affairs' ("Division") invitation for public input concerning the Division's development of regulations under the New Jersey Data Privacy Act (NJDPA). We commend the Division for its work to establish data privacy protections for residents of New Jersey.

The state of privacy legislation and regulation in the United States is a patchwork of overlapping but non-identical requirements that are frequently shifting as new developments and technologies come to the fore. As we note many times throughout this comment, the NJDPA as enacted falls short of the rules needed to adequately protect New Jersey residents' privacy. We urge the New Jersey Legislature to consider amending the NJDPA to place substantive limits on data collection and processing rather than relying on businesses to determine the appropriate purposes for processing and simply disclosing those purposes to the consumer.

As the Division finalizes regulations, we urge you to lead in the protection of consumer rights as strongly as possible within the confines of a disclosure-and-consent-focused statute. We support the Division's proposal that clearly articulate the rules around adequate forms of consent and prohibitions on manipulative design and dark patterns, and we urge the Division to maintain these critical consumer protections. We urge the Division to strengthen the data security responsibilities imposed on entities that collect personal information. The rules should clearly define the scope of the NJDPA and identify specific forms of data collection, processing, and transfer that are permitted or prohibited.

OUR ORGANIZATIONS

EPIC is a public interest research center based in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[1] EPIC has long advocated for comprehensive privacy laws at the state and federal levels.[2]

CFA is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.[3]

NJCA is a statewide coalition and grassroots organization that fights for social, racial, and economic justice for all.[4]

TechEquity Action's mission is to ensure that the tech industry is a force for justice in our economy.[5]

VCC is a membership organization dedicated to consumer advocacy, financial education and championing the rights of all consumers.[6]

SUBCHAPTER 1: GENERAL PROVISIONS

<u>Definitions (13:45L-1.2)</u>

We support the Division's clarifications on the definitions of "decisions that produce legal or similarly significant effects concerning the consumer," "de-identified data," "publicly available information," and "sale" in **Section 13:45L-1.2** and make a recommendation on the definition of "personal data."

"Decisions that produce legal or similarly significant effects concerning the consumer"

[1] EPIC, *About EPIC*, http://epic.org/about.
[2] *See* e.g. EPIC, *The State Data Privacy Act: A Proposed Model State Privacy Bill,* https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/.
[3] CFA, *Overview*, https://consumerfed.org/overview/.
[4] New Jersey Citizen Action, *Who We Are,* https://www.njcitizenaction.org/who_we_are.
[5] TechEquity Action, *What We Believe,* https://www.techequityaction.org/values-and-platform/.
[6] Virginia Consumer Council, *Welcome to the Virigina Consumer Council,* https://vaconsumercouncil.org/.

By clarifying that "decisions that produce legal or similarly significant effects concerning the consumer" include "automated or algorithmic decisions," the Division is protecting New Jerseyans from many of the riskiest and most error-prone methods that companies use to make these high-stakes decisions about people's lives. By explicitly referencing automated and algorithmic decisions, the Division reiterates that consumers have the right to opt out of companies use of automated decision systems or algorithms to make important decisions about their housing, employment, finances, and other key parts of their lives. We urge the Division to maintain this definition.

"De-identified data"

"Pseudonymized data" is a major loophole in several state data privacy laws that the Division rightly closes through the definition of "de-identified data." Exempting pseudonymized data could exempt the majority of the online advertising ecosystem from the most substantive aspects of NJDPA's coverage. Online platforms and advertisers use pseudonymous identifiers (such as cookie and device IDs) to track users across websites, collecting extremely granular data about a user's search history, usage, personal characteristics, and interests in order to serve them targeted advertisements or to create profiles they can sell to other interested third parties. However, because the Division explicitly clarifies that "pseudonymized data that can be used to infer information about, or otherwise be linked to, an identified or identifiable individual or device linked to such an individual is not de-identified data," this potential loophole is avoided in the NJDPA. We urge the Division to retain this provision.

"Personal data"

The definition of "personal data" should be amended to explicitly include derived data, such as inferences made about a consumer. This would be consistent with how personal information is defined in California's law, which includes derived data/inferences.[7] We recommend the following change to the first sentence of the definition of personal data in this section:

> "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable person, *including derived data*.

[7] Cal. Civ. Code § 1798.140(v)(1)(K).

“Publicly available information”

We commend the Division for clarifying that the definition of “publicly available information” does not include personal data that has been scraped or obtained from data brokers that is not otherwise publicly available. Scrapers do not adhere to the privacy policies of the websites they scrape, nor do they ask our permission to take our data or process it. When our personal information is scraped, we lose control of that information. We can no longer limit who can view the information, control what it is used for, or delete it. The information can be used in ways we never intended or consented to when we posted the information. Scraped personal information might be:

- Combined and/or enriched with data from other sources to create detailed profiles on individuals;
- Sold to data brokers, scammers, or governments;
- Used to score you or otherwise make decisions about you;
- Used to create biometric profiles, like Clearview AI’s facial recognition database, which is built entirely from scraped photographs.[8]

The internet is an essential part of today’s society, and an online presence of some kind is practically a necessity. We often make information like our name, photo, and other information viewable to the public so that people can find us. Many professionals are expected to be on networking sites such as LinkedIn, where we sometimes disclose our names, photos, cities, work history, and education; students are expected to be on Snapchat or Instagram to hear about events on campus, and these profiles may make our names, photos, and other information publicly viewable. Many peer-to-peer services also involve some sort of public profile, like our names and photos on Venmo that help friends and family find the right account to pay.

When we make information available for the public to view on social media or the web, we do not expect or intend that others will take that information and do with it as they please. We expect that our data will only be used for purposes we choose, and that the privacy controls that we select for the data will be respected. We urge the Division to maintain this provision.

[8] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

"Sale"

While the text of the NJDPA states that disclosure of personal data to processors who will process the data on the controllers' behalf or third parties who will use the data to provide a product or service to the consumer is exempt from the sale definition, the Division rightly places limits on these exemptions that are consistent with the purpose limitations throughout the rest of these rules. The Division adds a qualifying condition to both of these exemptions stating that disclosures to processors or third parties are exempt only "provided that the processor/third party does not use the data for its own purposes." This qualifier ensures that processors and third parties cannot obtain personal information under the guise of providing a service to controllers or a product or service to consumers and then use that data for their own purposes without restriction. This restriction protects consumers' personal data by ensuring that if it is disclosed to other entities, those entities use it only for the purpose that a consumer has asked for and expects. This limitation is consistent with the data minimization principles that we recommend throughout these comments, and we urge the Division to retain these provisions in the final rules.

Exemptions (13:45L-1.3)

We strongly support the Division's inclusion of **Section 13:45L-1.3(d)(1)(ii),** which clarifies that the exemption allowing controllers and processors to "conduct internal research" does not allow them to use consumers' personal data to train AI models. The rule instead requires companies to obtain consumers' affirmative consent to use their personal data to train AI under this exemption. The rapid growth of the AI industry, particularly generative AI, has only increased the incentives for companies to collect and retain as much data as they can so they have the largest possible data set to use to train AI models. Therefore, it is especially important that privacy laws and regulations address this risk and require companies to obtain consumers' consent before using their personal data in this way. We commend the Division for this clarification and urge you to retain it in the final rules.

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

Design choices that purposely deter consumers from exercising their privacy rights undermine the very purpose of a privacy law—to protect and empower consumers. We commend the Division for including strong rules about prohibited deceptive designs/dark patterns, including the use of clear examples. As commerce has moved online, so have deceptive tactics, and they have become even more sophisticated and difficult for consumers to navigate given the control that companies have over the interfaces through which consumers access goods and services. In 2023, Google reached a $93 million settlement with the California Attorney General, whose complaint alleged that Google "deceived users in numerous ways regarding how it collected, stored, and used a person's location data."[9] TikTok was found liable by the Irish Data Protection Commission for employing dark patterns to nudge children toward less privacy-protective settings using bold text in pop-up notifications.[10]

The Federal Trade Commission has described dark patterns as "design practices that trick or manipulate users into making choices that they would not otherwise have made and that may cause harm."[11] These practices are especially harmful in the privacy context. Companies have pushed for decades to frame data collection and processing as an issue of consumer "choice" while deploying manipulative choice architecture to ensure that consumers always "choose" to permit more data collection, broader purposes, and loose or non-existent data sale or transfer restrictions. Strong rules prohibiting the use of dark patterns are particularly important as businesses' ability to manipulate individual users based on hyper-specific profiles is supercharged by the use of artificial intelligence.[12]

The rules prohibiting manipulative design set out in this subsection contain critical consumer protections to ensure fairness in consumer interactions with businesses. We commend the Division for requiring that data rights requests and methods for obtaining consent incorporate the following principles:

1. Must use plain, straightforward language and comply with the rules set forth in Section 13:45L-1.4;

[9] Press Release, Att'y Gen. Rob Bonta, *Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices* (Sept. 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-93-million-settlement-regarding-google's.

[10] Press Release, Irish Data Protection Comm'n, *Irish Data Protection Commission Announces €345 Million Fine of TikTok* (Sept. 2023), https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.

[11] Fed. Trade Comm'n, *Bringing Dark Patterns to Light* 2 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light.

[12] Federico Guerrini, *AI-Driven Dark Patterns: How Artificial Intelligence Is Supercharging Digital Manipulation* (Nov. 2024), https://www.forbes.com/sites/federicoguerrini/2024/11/17/ai-driven-dark-patterns-how-artificial-intelligence-is-supercharging-digital-manipulation/; Mark Leiser, *Dark Patterns, Deceptive Design, and the Law* (Bloomsbury Publishing, 2025).

2. Must avoid language or interactive elements that are confusing to the consumer such as double negatives or toggles or buttons that do not clearly indicate the consumer's choice;
3. Must avoid manipulative language or choice architecture, including using language or wording that guilts or shames the consumer into making a particular choice;
4. Must not impair or interfere with the consumer's ability to make a choice, exercise their choice, or give valid consent, including by bundling choices so the consumer is forced to consent to uses that are incompatible with the context in which the personal data was collected;
5. Must be easy to execute;
6. Must have symmetry in choice;
7. A consumer's silence or failure to take an affirmative action may not be interpreted as acceptance or consent;
8. Choice options may not be presented with a preselected or default option (We do recommend the Division amend this subsection to read "Choice options shall not be presented with a preselected or default option *unless the preselected or default option is the most-privacy protective option.*")
9. A consumer's expected interaction with a website, application, device, or product may not be unnecessarily interrupted or intruded upon to request consent;
10. May not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain consent;
11. Must take into consideration the vulnerabilities or unique characteristics of the target audience.

We particularly commend the Division for making clear in these rules that privacy choices should not be a "take it or leave it situation." Though we read these rules as already requiring this, we do suggest the addition of a new subsection to make clear that when controllers provide unbundled choices that present consumers with individual consent option for purposes that are both compatible and incompatible with the context in which the personal data is collected, they may not condition use of the product or service on consent to incompatible purposes, and they must make that clear to the consumer.[13] Using the illustrative example the Division provided in **Section 13:45L-1.5(a)(4)(ii)**, if a controller provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, it shall not require the consumer to

[13] As an example as to why this must be made clear to the consumer, *see, e.g.,* @patrickleavy.mastodon.social.ap.brid.gy (Patrick Leavy) (Nov. 25, 2024 2:41 PM), https://bsky.app/profile/did:plc:gdj3gszxnhizlvhewgvbjdc6/post/3lbsb7oa377m2.

consent to incompatible uses (for example, the sale of the consumer's geolocation to data brokers) in order to use the app. Such a rule would be consistent with the rule set out in **Section 13:45L-1.5(a)(9)(ii)** which says that controllers may not "[redirect] consumers away from the content or service they are attempting to interact with because they declined the consent choice offered, unless consent to process the requested data is strictly necessary to provide the website or application content or experience." To make the interaction between these two rules clear, we suggest adding **a new subsection (a)(12)** that reads:

> *The controller shall not prevent a consumer from using a website or application content or experience if the consumer does not consent to the processing of personal data for purposes that are incompatible with the context in which the personal data was collected, unless consent to process the requested data is strictly necessary to provide the website or application content or experience. The controller must make clear to the consumer that consenting to such incompatible uses is not required to use the website or application.*

Lastly, we commend the Division for clearly stating that any method that does not comply with the above may be considered a dark pattern and that an option chosen through a use of a dark pattern does not constitute valid consumer consent.

SUBCHAPTER 2. CONSUMER DISCLOSURES

Disclosures alone are simply not a sufficient way to protect consumers' privacy. Disclosures are the favorite tool of the failed "notice and choice" regime and can overwhelm consumers without providing meaningful protection. Consumers cannot reasonably be expected to read long, technical privacy policies for every website or app with which they interact, especially because these disclosures do not give consumers any real choices about their privacy—the all-or-nothing decision to either accept the terms of a privacy policy or to simply not access the service is not a meaningful choice.

We support the proposal to have clear rules for controllers on the specific elements necessary in a privacy notice, particularly concerning how New Jerseyans' personal data is used in profiling decisions. Specifically, the disclosures required by the regulations provide clear notice to consumers of their rights and notice of material changes. We support the requirement that privacy notices must describe categories of personal data processed in a level of detail that enables consumers to understand them. However, despite the clarity of these disclosure requirements, we encourage the Legislature to amend the NJDPA to include meaningful data minimization rules that better align businesses' data practices with what consumers expect, as further detailed in Subchapter 6 below, rather than requiring New Jersey residents to read lengthy privacy notices in order to determine how their personal data is being collected and used.

Privacy notice required (13:45L-2.1)

In Section **13:45L-2.1(b)**, the rules state that controllers do not need to provide a New Jersey-specific privacy notice. The Division may want to clarify this rule to add that if a controller does list other states specifically, they must name New Jersey as well or make clear that the rights extend to all U.S. users. The Delaware Department of Justice set out a similar rule in its guidance:

> 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.[14]

The Connecticut Attorney General raised a similar issue in its recent enforcement report.[15] Accordingly, we recommend that the Division amend **13:45L-2.1(b)** to read:

> (b) 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.~~ *description of consumer rights unambiguously indicates those rights are available to New Jersey residents. Statements such as "you may have rights" or "if your state has a data privacy law" are not sufficiently clear to inform New Jersey residents of their rights. Controllers must state the described consumer rights may be exercised by either (i) all users or all United States users or (ii) a clearly described subset of users, including explicitly New Jersey residents, among residents of other states.*

[14] Del. Dept. of Justice, *Frequently Asked Questions,* https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions/

[15] Conn. Att'y Gen., *Updated Enforcement Report Pursuant to Conn. Data Priv. Act, Conn. Gen. Stat. §42-515, et seq.* (Apr. 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf ("We are also troubled by privacy notices that create a misimpression that consumer rights are exclusive to residents in only one state, or only in certain states, and that are not sufficiently inclusive of states that have enacted consumer data privacy laws.")

Privacy notice content (13:45L-2.2)

A company engaging in profiling to make a critical decision in someone's life is a data practice that requires robust disclosures. This type of profiling can lead to lost opportunities or higher prices with no transparency or accountability. We support the current regulations, which reflect the need to have clear and robust disclosure when entities make significant decisions through profiling. We urge the Division to retain these robust disclosure requirements in the final regulations.

Changes to a privacy notice (13:45L-2.5)

We support the requirement to notify consumers of material changes to privacy notices and require valid consent prior to processing, sharing, or selling personal data collected before the change to the privacy notice. We do recommend the Division add a requirement that controllers maintain a public log of previous versions of its privacy policy for at least 10 years. We recommend the following language be added in a new subsection(c):

> *A controller shall maintain a log of material changes retained as copies of previous versions of its privacy notice for at least 10 years beginning after (the effective date of this rulemaking) and publish them on its website. The controller shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy policy over the past 10 years. The descriptions shall be sufficient for an average consumer to understand the material effect of each material change.*

Loyalty program notice (13:45L-2.5)

When "loyalty programs" first came into existence, they were designed to operate as their name indicates—a way for companies to incentivize loyalty from their customers. Consumers got discounts for signing up for the program, and in return, the retailer benefited from their repeated patronage. In the era of commercial surveillance, however, these programs have transformed retailers into data brokers that monetize their customers' personal data for profit. A recent Consumer Reports study found that grocery chain Kroger's "precision marketing" side business made a $527 million profit in 2024, representing more than 35% of the company's net income.[16]

[16] Derek Kravitz, *Inside Kroger's Secret Shopper Profiles: Why You May Be Paying More Than Your Neighbors* (May 2025), https://www.consumerreports.org/money/questionable-business-practices/kroger-secret-grocery-shopper-loyalty-profiles-unfair-a1011215563/.

Loyalty programs should not be confused with financial incentive programs. We recommend renaming **Section 13:45L-2.5** "Financial incentive programs" to more accurately label the types of programs this Section describes, wherein the consumer is given an incentive (such as discounts) in exchange for the sale of their personal data.

We commend the Division for requiring the benefits from incentive programs to be reasonably related to the value of the consumer's personal data in **Section 13:45L-2.5(b)(3)** and that controllers must explain how the price or service difference associated with participating in the loyalty program is reasonably related to the value of the consumer's personal data. While our organizations believe the use of data collected for loyalty programs should be limited to what is functionally necessary to operate the loyalty program and that companies should not be able to collect consumers' personal data with the promise of a discount or loyalty program perk and then turn around and sell that data to other companies to make a profit, we recognize that the Division is operating within the confines of the language in the NJDPA. Within those confines, it is important for the Division to retain the "reasonably related" rule in this section.

SUBCHAPTER 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

The NJDPA articulates similar consumer rights as those found in the European Union's General Data Protection Regulation and most state privacy legislation—namely: the right to know of and access personal information being collected about oneself, the right to delete such data, the right to correct such data, and the right to export this data in an easily useable format. Consumer rights alone are not sufficient to protect privacy but are an important component of any comprehensive privacy bill, provided they are easily accessible and usable for consumers.

One key change the Division should make to the rules regarding consumer rights is that those rights cover *all* personal data held by a controller, regardless of the source of that data. The Division should clarify in proposed **Sections 13:45L-3.5, 3.6, 3.7, and 3.8** that consumer rights apply to any personal data held about the consumer, including inferences. We recommend the following language from the Colorado Privacy Act rules issued by the Colorado Department of Law:

> *Specific pieces of Personal Data include final Profiling decisions, inferences, derivative data, marketing profiles, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual.*[17]

SUBCHAPTER 4. VERIFICATION OF REQUESTS

We commend the Division for properly balancing consumer usability with strong privacy protections throughout the verification requirements outlined in the rules. The rules rightly establish different levels of authentication requirements for different kinds of data based on its importance, sensitivity, and level of risk and based on whether the request is an opt-out request or a request to obtain, correct, or delete personal data. This layered approach ensures both consumer ease and convenience in making requests to controllers and data security based on the personal data at issue. The rules outline in **Section 13:45L-4.1(c)** criteria to help controllers determine what are commercially reasonable methods of authenticating consumers' identities. These factors are useful in helping controllers evaluate the potential harms from granting unauthorized or fraudulent consumer requests against the benefits to consumers from the ability to make simple, user-friendly consumer rights requests that do not require them to disclose more personal data.

The rules' differentiation of how to verify requests from consumers with password-protected accounts **(Section 13:45L-4.2)** versus non-account holders **(Section 13:45L-4.3)** is a good way to properly balance data security and privacy risks with usability for consumers. In particular, the requirements in **Section 13:45L-4.3(b)-(d)** are well-crafted to ensure that the level of certainty required to authenticate consumer rights requests increases with the specificity and sensitivity of the personal data at issue.

Similarly, consumer requests to opt out of targeted advertising, data sales, or profiling activities should not require authentication of the consumer's identity—which the rules properly note in **Section 13:45L-4.1(b)**—because opt-out requests do not present a threat to the security or privacy of consumers' personal data the way a request to access, correct, or delete such data would. Thus, the Division correctly treats opt-out requests differently from consumer rights requests in terms of authentication requirements. It is important to make this distinction clear. In

[17] *Colorado Privacy Act Rules*, 4 CCR 904-3 at 4.04(A)(1).

Consumer Reports' investigation into the usability of then-new privacy rights in California, it found examples of companies requiring consumers to fax in copies of their drivers' licenses to verify residency and applicability of CCPA rights.[18] This level of verification is unnecessary and, in fact, creates new privacy risks. We urge the Division to maintain this clarification.

We also commend the Division for **Section 13:45L-4.1(e)**, which requires the deletion of data that consumers provide for authentication upon successful authentication and limits the use of such data to the authentication process, and **Section 13:45L-4.4(d)**, which limits the purposes for which authorized agents can use consumers' personal data to only "verification, fraud prevention, or fulfilling the consumer's request." Employing data minimization principles such as required deletion and purpose limitations is the best way to ensure consumers' data privacy.

SUBCHAPTER 5. UNIVERSAL OPT-OUT MECHANISM

Universal opt-out mechanisms (UOOMs) are a critical consumer protection in any privacy law that requires consumers to opt out of harmful uses of their personal data. UOOMs, which allow consumers to broadcast to businesses they interact with online their preference to opt out from their personal information being sold or shared with third parties through a simple toggle, ensure that consumers can exercise their rights in a meaningful way.

Although it is important to establish strong baseline requirements applicable to all global opt-out mechanisms, the Division should not hesitate to address technology-specific considerations where appropriate. For example, while **Section 13:45L-5.2(a)(8)** requires that all universal opt-out mechanisms be "consumer-friendly, clearly described, and easy to use by the average consumer," controllers and consumers may benefit from the inclusion of specific considerations applicable to browser-based opt-out tools and operating-system-based opt-out tools. The Division could provide this detail through narrative examples and/or visual depictions of compliant and non-compliant opt-out mechanisms.

The Division should also clarify in **Section 13:45L-5.2** that a consumer's IP address is sufficient for authenticating that the consumer is a resident of New Jersey.

[18] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously*, Medium (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

Lastly, the Division should consider amending **Subchapter 5** to designate "Global Privacy Control" (GPC),[19] as a recognized protocol.[20] GPC has been approved by both Colorado and California as a valid UOOM.[21]

SUBCHAPTER 6. DUTIES OF CONTROLLERS

We commend the Division for providing clear and comprehensive duties for controllers, including detailed requirements for purpose specification for the use of personal data. It is also encouraging that the draft grounds purpose specification in a data minimization framework by distinguishing requirements for secondary use. To be clear, however, even the most effective notice and transparency requirements cannot, by themselves, fully protect against the abuse of personal data.[22] We have moved beyond the notion that notice and choice alone can legitimize commercial surveillance practices when those practices are too complex and numerous for even the most sophisticated consumer to understand. That is why it is critical that the Legislature consider amending the NJDPA to place substantive limits on data collection and processing.

Purpose specification (13:45L-6.1)

A core principle of privacy protection is that personal data should be used within the context of the primary purpose for which was collected. We commend the Division for setting forth strong purpose specification rules that make clear that controllers cannot identify one broad purpose to justify numerous processing activities, specify one broad purpose to cover potential future processing activities, or identify so many purposes for which personal data could be processed that the purpose or purposes become unclear or uninformative. Unfortunately, many of these practices are rampant online, but the proposed rules provide clarity that businesses may not bury their data processing purposes under a mountain of technical jargon and legalese.

However, even the clearest purpose specification rules still put the burden on the consumer to read (often lengthy and hard to decipher) disclosures, and they are left with little

[19] The standard is available at https://globalprivacycontrol.org/#gpc-spec.

[20] See more details at Global Privacy Control, https://globalprivacycontrol.org/.

[21] Colo. Att'y Gen., *Universal Opt-Out and the Colorado Privacy Act*, https://coag.gov/opt-out/; Cal. Att'y Gen., *Global Privacy Control*, https://oag.ca.gov/privacy/ccpa/gpc.

[22] *See* Philipp Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 Nw. J. Tech. & Intell. Prop. 1, 16–9 (2017) (discussing limits of transparency as accountability and consumer disclosure involving Big Data).

choice but to accept the terms and use the service or not use it at all. A shopper who agrees to a retailer's rewards program after seeing that their personal data will be used for "marketing purposes" likely does not expect that their shopping history will be sold to dozens of data brokers and used to make inferences about them such as their health and wealth.[23] This is why it is critical that the Legislature amend the NJDPA to limit the use of personal data to what is reasonably necessary and proportionate for the product or service the consumer has requested.

Restrictions on the use of personal data (13:45L-6.2)

We support the inclusion of rules consistent with California's regulations regarding factors for determining whether a new purpose is compatible with an already disclosed purpose.

Data minimization (13:45L-6.3)

Subsection 6.3 restates the rule from the NJDPA that controllers must limit the collection of personal data to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." Our organizations have long argued that businesses should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information.[24] We will note again that this Legislature should amend the NJDPA to limit the collection and use of personal data to what is reasonably necessary and proportionate for the product or service the consumer has requested.

Subsection (b) sets forth strong data minimization principles. We encourage the Division to amend the rules to make these affirmative requirements for controllers rather than simply requiring controllers to document their efforts to effectuate them.

We strongly support an affirmative obligation to conduct data mapping and data inventories, as outlined in **Section 13:45L-6.3(b)(2)**. Data mapping can ensure that a company understands the scope of what it must protect, what safeguards or security measures it should

[23] *See, e.g.,* Manuela López Restrepo, *Does Your Rewards Card Know if You're Pregnant? Privacy Experts Sound the Alarm*, NPR (Aug. 13, 2022), https://www.npr.org/2022/08/13/1115414467/consumer-data-abortion-roe-wade-pregnancy-test-rewards-card-target-walgreens.

[24] *See, e.g.,* Kara Williams & Caitriona Fitzgerald, *Data Minimization Is the Key to a Meaningful Privacy Law* (May 2024), https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/ ("The key words 'as disclosed to the consumer' mean that businesses are not really limited at all—they may collect and use data for any purposes they disclose in their privacy policies that no one ever reads.")

adopt, and the way it should respond when its security measures have failed to prevent a breach. As Professors Solove and Hartzog have explained:

> Privacy requirements such as data mapping provide awareness about potential security vulnerabilities. Data mapping shows what data is being collected and maintained, the purposes for having this data, the whereabouts of this data, and other key information.[25]

It is difficult to imagine a company could consider itself "prepared" to respond to a cyber incident if it does not map what data it collects and where it is stored. It also seems unlikely that a company could detect unauthorized access of data if it does not map out which users and partners are permitted to access which databases. Twitter whistleblower Peter "Mudge" Zatko highlighted this issue in testimony before Congress, stating, "I discovered two basic issues. First, they don't know what data they have, where it lives, or where it came from. And so unsurprisingly, they can't protect it."[26] The problem is not unique to Twitter—two Meta engineers questioned during a court hearing in 2022 admitted that there is no single individual within Meta who would be able to answer where all the data on a single user is stored, and moreover that "[i]t would take a significant team effort to even be able to answer that question."[27] The data inventory rule in **subsection (b)(2)** would require companies to account for the personal data they hold. We do recommend that the rule be updated to be explicit that the requirement to document who has access to the data includes processors and third parties.

We also strongly support the affirmative rules as outlined in the rest of **Section 13:45L-6.3(b)** that controllers: limit the collection of personal data to what is necessary for the specific purpose or purposes; maintain personal data in an identifiable form for no longer than necessary for the processing purpose and delete (and instruct processors to delete) any personal data no longer necessary for the specific processing purpose. These measures will greatly improve data security; personal data that has been properly de-identified or deleted cannot be breached. After a data breach at Marriott and its subsidiary Starwood Hotels & Resorts exposed the passport and

[25] Daniel J. Solove & Woodrow Hartzog, *Breached! Why Data Security Law Fails and How to Improve It* 156–57 (2022).

[26] *See Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (2022), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower.

[27] Isobel Asher Hamilton, *Senior Facebook Engineers Say No One at the Company Knows Where Your Data Is Kept*, Bus. Insider (Sept. 8, 2022), https://www.businessinsider.com/meta-doesnt-know-where-all-your-data-is-engineers-say-2022-9.

credit card information of over 344 million customers worldwide, the Federal Trade Commission required in its settlement with the companies that they "implement a policy to retain personal information for only as long as is reasonably necessary to fulfill the purpose for which it was collected."[28] This is a best practice for data minimization and security.

We also support the appropriately heightened requirements for sensitive data in **Sections 13:45L-6.3(b)(5) and (6)**. Consumers reasonably expect that if they revoke their previously given consent to process sensitive data, that the controller will delete their sensitive data. In particular, biometric identifiers, photos, and audio and voice recordings are uniquely sensitive and should not be stored any longer than necessary. Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. A requirement to annually review whether it is still necessary to store such data is an important and necessary protection, which we urge the Division to retain.

Duty of care (13:45L-6.4)

Consumers are facing an epidemic of data breaches and resulting identity theft and harm due to a lack of investment in and commitment to data security. The California Privacy Protection Agency recently detailed the harms to consumers that result from unauthorized actions related to their personal data, including "monetary losses, lost time and opportunities, and psychological and reputational harm."[29] These harms can include identity theft and the resulting out-of-pocket expenses, denials of financial services, and stress, as well as potential physical harms such as stalking, cyberstalking, harassment, and physical violence. A "duty of care" is the correct approach to controller requirements for handling personal data; if they can't protect it, they shouldn't collect it. A duty of care approach also focuses on the risk to consumers rather than the risk to a business in the case of a cyber incident. We commend the Division for approaching its data security rules through a duty of care lens and for requiring in **Section 13:45L-6.5** that controllers update, maintain, and document their data security measures.

[28] Press Release, Fed. Trade Comm'n, *FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches* (Oct. 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches.

[29] Cal. Priv. Protection Agency, *Initial Statement of Reasons (CPPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)* 5, (Nov. 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

With its rulemaking authority, the Division has the opportunity to set minimum standards with flexibility as to implementation that will provide the guardrails necessary to protect consumers from weak data security while allowing controllers to innovate on data security in response to evolving cyber threats. We believe the Division could provide more guidance for controllers in this Section to provide clarity on the best data security practices.

In **Section 13:45L-6.4(b),** controllers, in determining appropriate data security safeguards, "shall consider" not only the sensitivity and amount of data, source of the data, and risk of harm, but also "shall consider" industry standards. Unfortunately, "industry standards" in many sectors are simply insufficient to adequately protect consumers. For example, the Federal Communications Commission has noted that the telecommunications industry has exposed the public to an increasing number of security breaches in recent years.[30] Similarly, we are concerned that requiring a controller to consider the "nature, size, and complexity" of their organization could allow for a scenario in which a small startup handling vast amounts of sensitive data believes the Division's regime permits it to maintain sub-standard safeguards. We encourage the Division to instead outline that controllers "may consider" industry standards and the nature, size, and complexity of the controller's organization, as it has done for the burden or cost of safeguards in **Section 6.4(c).** We believe that elevating the priority of the sensitivity, volume, source, and risks of consumer data above the relevance of industry standards, business maturity, and operating costs will better underscore scenarios that merit greater cybersecurity safeguards.

In **Section 13:45L-6.4(d)(1)**, the Division rightly clarifies that "unauthorized access" (which is not defined in the statute) includes "without authorization or in excess of authorization." The Division could further clarify this rule by including examples of exceeding authorization such as social engineering or a bribed employee—as in the case of SIM swapping fraud—and/or compromised credential or credential stuffing attacks, as notably occurred with 23andMe.[31]

[30] Fed. Commc'ns Comm'n, In re Data Breach Reporting Requirements, Report and Order, WC Docket No. 22-21 at ¶ 22 (Dec. 21, 2023), https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf.

[31] Shiona McCallum & Joe Tidy, *23andMe: Profiles of 6.9 Million People Hacked*, BBC (Dec. 5, 2023), https://www.bbc.com/news/technology-67624182.

A consistent framework can help industry focus on mitigating cybersecurity threats.[32] We urge the Division to add a **new subsection (e)** to this Section to require controllers to undertake certain data security measures for which there is consensus or near-consensus across different frameworks,[33] such as:

- **Data minimization:** Data minimization is an accepted fundamental risk-reduction concept in cyber hygiene and information management. A hacker can't gain access to data that a company does not have, and companies should have strong incentives to limit the scope and nature of their collection, especially regarding sensitive data. By changing the documentation requirements in **Section 13:45L-6.3(b)** to affirmative requirements as suggested above, controllers would improve data security by minimizing the amount of personal data at risk.
- **Heightened measures for high-risk activities:** As already noted in **subsection (b)(3)**, controllers' data security practices should consider the sensitivity of personal data. Controllers must be required to exercise additional measures to ensure they implement stronger protections in higher-risk situations.
- **Governance:** Governance issues include identifying leadership accountable for implementing the program, conducting security reviews, and providing current employee training (including threat intelligence education).
- **Data mapping:** In **Section 13:45L-6.3(b)(2)**, the Division requires controllers to document their efforts to "create, establish, update, and maintain a data inventory documenting the types of data that the controller possesses, where the data is stored, and who has access to the data." An affirmative requirement to conduct such data mapping would be a strong addition to this Section.
- **Access controls:** Access controls include limiting who has access to what data within a system, as well as strong password and user authentication practices. In **Section 13:45L-6.3(b)(2)**, the Division requires that part of the data inventory include who has access to the data. The Division should require businesses to follow best practices for access control in this section. In Peter "Mudge" Zatko's whistleblower complaint filed with the Securities and Exchange Commission, he said he found "serious access control problems, with far too many staff (about half of Twitter's 10,000 employees, and growing) given access to sensitive live production systems and user data in order to do their jobs."[34] And

[32] Joseph D. Simon & Elizabeth A. Murphy, *Cybersecurity Regulation for Financial Services Companies: New York State Leads the Way*, 30 Journal of Taxation and Regulation of Fin. Insts. No. 4, at 36 (Summer 2017), https://www.civicresearchinstitute.com/online/PDF/TFI-3004-02-Cybersecurity.pdf.

[33] EPIC & Consumer Reports, Comments to the Office of the Nat'l Cyber Dir. in the Matter of Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations (Oct. 31, 2023), https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/.

[34] Peter "Mudge" Zatko, Whistleblower Aid, *Re: Protected Disclosures of Federal Trade Commission Act Violations, Material Misrepresentations and Omissions, and Fraud by Twitter, Inc.* 27–28 (July 6, 2022), https://s3.documentcloud.org/documents/22186683/twitter-whistleblower-disclosure.pdf (internal citations omitted).

this access control problem has real consequences: According to Mudge's complaint, "In 2020 alone, Twitter had more than 40 security incidents, 70% of which were access control-related. These included 20 incidents defined as breaches; all but two of which were access control related."[35]

- **Segmentation of systems:** Segmentation of systems (e.g., internal firewalls) can help to limit how much consumer harm results from a single breach by making it difficult for a threat actor infiltrating one part of the company's network to access other parts of the network.[36] The FTC has recommended this since at least as early as 2015;[37] and the White House urged companies to implement this practice "now" in June 2021.[38]
- **Vulnerability management:** Vulnerability management includes end-of-life protocols for unsupported software, devices, etc., patch management (including assessing whether a patch was effective), and penetration testing to check a security team's work. Taking precautions against known vulnerabilities, such as prompt installation of security patches and software updates, can reduce the likelihood of breach, preventing unauthorized access in the first place.
- **Threat detection:** Threat detection includes practices such as continuous traffic monitoring, which facilitates early detection of attempts at unauthorized access.
- **Incident Response:** Required incident response drills are a best practice. CISA[39] and NIST[40] have both offered guidance on incident response.
- **Business Continuity:** Disaster recovery or business continuity planning prepares an organization to maintain functionality despite an emerging cyber incident (e.g. ransomware attack locking users out). Cybersecurity insurance applications often ask about business continuity planning.

Additionally, the Division should consider requiring independent auditors for high-risk organizations. Although all organizations should do some measure of ongoing security review, for organizations possessing a large volume of data or particularly sensitive data, an independent auditor should be responsible for assessing compliance, and their assessment should be technical,

[35] *Id.* at 28.

[36] *See, e.g.*, Cybersecurity Advisory, *NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations* (Oct. 5, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a.

[37] *See* Fed. Trade Comm'n, *Start With Security: A Guide for Business* (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

[38] *See* The White House, *What We Urge You To Do To Protect Against The Threat of Ransomware* (June 2, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf.

[39] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, Incident Response Plan (IRP) Basics, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf.

[40] *See, e.g.*, Paul Chiconski, et al., Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, NIST Special Publication (SP) 800-61, Rev. 2 (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

public, use audit-like standards, and allow for external stakeholder input. High-risk organizations should not be allowed to "grade their own homework."

SUBCHAPTER 7. CONSENT

Consent required (13:45L-7.1)

As explained throughout this comment and over decades of our organizations' advocacy, notice and choice is an outdated framework that fails to meaningfully protect privacy. Instead, the concept of data minimization provides an effective framework for protecting consumers' data privacy. To that end, we strongly urge the Legislature to amend the NJDPA to include true data minimization requirements rather than mere notice requirements masquerading as "data minimization." The core of data minimization is limiting the collection and use of personal data to what is reasonably necessary and proportionate for the product or service the consumer has requested.[41] We encourage the Legislature to adopt this standard rather than allowing controllers to engage in whatever data practices they want to as long as they are disclosed to consumers.

The processing activities outlined in **Section 13:45L-7.1(a)** include many of the activities that present the greatest risks to consumers, so it is reasonable to require controllers to obtain consumers' consent before engaging in these activities. However, we would recommend adding in **Section 13:45L-7.1(a)(4)** a cross-reference to **Section 13:45L-7.5(a),** which requires controllers to wait at least 12 months after a consumer exercises their right to opt out before sending them another consent request. Without this clarification, some entities may try to take advantage of the requirement in **Section 13:45L-7.1(a)(4)** to obtain consent from consumers who have opted out before engaging in certain processing activities in order to pester consumers who have opted out. It seems that these two provisions are intended to work together, but adding an explicit reference in **Section 13:45L-7.1(a)** would ensure that consumers who have opted out of certain processing activities are not bombarded with endless consent requests from controllers wanting to engage in those activities.

We support the Division's decision in **Section 13:45L-7.1(b)** to require that controllers obtain new consent from consumers after these rules take effect, unless they have already obtained consent from consumers in a manner that complies with the requirements of these rules.

[41] Williams & Fitzgerald, *supra* note 21.

While this requirement will likely require many businesses to obtain new consent from consumers, it is the best way to ensure that consumers are meaningfully informed about what data practices businesses are seeking their consent for. Additionally, because of the clear guidelines in **Section 13:45L-7.2** that explain what qualifies as valid consent, it is likely that many consumers will benefit from a new consent request because it should be clearer and more understandable than previous requests. Businesses should not be able to rely on outdated consent if it was obtained through methods that would no longer be permissible under these rules. The benefits to consumers in terms of increased knowledge and autonomy over their own personal data outweigh the inconvenience businesses will claim they will face if this rule is adopted. For similar reasons, we also support the rule in **Section 13:45L-7.1(c)** that requires controllers to obtain new consent from consumers for previously collected personal data if those controllers want to use that data for a new processing purpose after these rules take effect. Although personal data collected before this rulemaking may have been lawfully collected at that time, the NJDPA and these rules are intended to protect consumers' personal data. Thus, it is appropriate for the Division to require that controllers follow the purpose limitation procedures outlined in **Section 13:45L-6.1** of these rules if they want to use personal data for a processing purpose that consumers were not aware of and did not consent to at the time their personal data was collected.

<u>Requirements for valid consent (13:45L-7.2)</u>

Despite our strong preference for data minimization principles over notice and choice regimes, these rules do provide good consumer protections within the confines of what a consent-based framework is able to accomplish. The rules in **Section 13:45L-7.2** require consent to be "a clear, affirmative action" that is "freely given" and "specific" and express the consumer's "unambiguous agreement." The rules set parameters for all of these consent requirements that, in combination with the rules prohibiting deceptive design in **Section 13:45L-1.5**, make consent choices more meaningful for consumers. Requiring valid consent to include these specific elements means that consumers must take a clear action to give their consent. Thus, these rules improve the status quo by prohibiting businesses from relying on neutral actions—such as accepting a long privacy policy or terms and conditions document, continuing to use a website or app, or exiting out of a banner or pop-up without making a selection—to argue that consumers have "consented."

We particularly support the clarification in **Section 13:45L-7.2(a)(2)(iii)** that the controller may not deny goods, services, discounts, or promotions to a consumer who chooses not to provide consent, unless the personal data is necessary to the provision of those goods, services, discounts, or promotions or the consent is otherwise required in connection with a consumer's voluntary participation in a loyalty program. The Division should adopt the rule we proposed in **Section 13:45L-1.5** above. As discussed in that section, businesses should not be able to force consumers into consenting to the use of their data for purposes incompatible with the context in which the personal data was collected by denying the consumer access unless they agree.

Request for consent (13:45L-7.3)

In general, we commend the Division for crafting rules that require consent requests to be accessible and understandable to consumers. In particular, **Section 13:45L-7.3(b),** which requires consent requests to be separate and distinct from other terms and conditions, makes it more likely that consumers will read and understand requests for their consent. This requirement prohibits controllers from burying consent requests inside long privacy policies or other terms and conditions documents and counting on the fact that consumers will not read, notice, or object to the requests. Requiring requests for consent to be separate and distinct gives consumers a chance to understand what data practices companies are asking them to allow and to decide whether they want to give permission for those practices. While there are still massive information and power asymmetries between companies and individual consumers that may still leave consumers with very little choice but to consent to certain data practices if they want to use the product or service, requiring standalone consent requests gives consumers a more accessible window into some of the data practices the companies with which they interact are employing.

Section 13:45L-7.3(c) furthers the goal of giving consumers clear and understandable information about their data by requiring companies to explain what consumers are being asked to consent to, what categories of their personal data is at issue, who will be handling their data, and what rights they have regarding that data. **Section 13:45L-7.3(c)(3)** requires controllers to inform consumers of the processing purpose for which they are seeking consumers' consent. Requiring controllers to specify in consent requests the particular purpose for which they want to use consumers' personal data is essential to helping consumers make an informed decision about whether to consent. It is critical to maintain the requirements in **Section 13:45L-7.2(a)(3)** that require that consumers be allowed to consent to unrelated processing purposes separately to make (c)(3) effective. This combination of rules ensures consumers will be sent notices that clearly state the specific processing purposes companies are asking them to consent to and allows consumers to choose whether to consent to each unrelated purpose individually, bolstering consumer autonomy.

Section 13:45L-7.3(c)(5) is another essential disclosure rule because it requires controllers to disclose what third parties they sell consumers' sensitive data to, which gives consumers important information about who holds their most sensitive information. However, we urge the New Jersey Legislature to amend the NJDPA to further protect the sensitive data of its residents by prohibiting the sale of sensitive data altogether. Other states have recently taken this step; Maryland prohibited the sale of all sensitive data by passing the Maryland Online Data Privacy Act in 2024,[42] and earlier this year, Oregon amended its Oregon Consumer Privacy Act to ban the sale of precise geolocation data and the data of children and teens under 16 years of age.[43]

<u>Consumers under the age of 13 (13:45L-7.4)</u>

While most of the rules in this subsection repeat the protections provided to children under 13 in the federal Children's Online Privacy Protection Act (COPPA), these rules do add a couple additional protections on top of those required by COPPA, which we urge the Division to retain. For example, **Section 13:45L-7.4(d)** requires controllers to inform parents or guardians of their right to opt out of the collection and processing of personal data on behalf of their child. This requirement ensures that parents and guardians are aware of the privacy protections that are available to children in New Jersey; COPPA requires entities to offer the ability for parents to opt out of data collection only if parents request it,[44] so this affirmative requirement serves to better protect the personal data of children under 13. Additionally, **Section 13:45L-7.4(e)** of the rules places an appropriate purpose limitation on the use of any personal data parents or guardians provide to verify their identities such that it may be used only for that specific purpose.

[42] Md. Code Ann. Com. Law § 14-4607.
[43] H.B. 2008, 83d Leg. Assemb., Reg. Sess. (Or. 2025).
[44] 15 U.S.C. § 6502(b)(1)(B)(ii), 16 C.F.R. § 312.6(a)(2).

While COPPA and its corresponding regulations do have similar restrictions on children's personal data, they do not protect the data of parents and guardians, so this subsection is an important addition.

In contrast to these heightened protections, there is one area where the intersection of these rules and COPPA's existing protections combine to result in a counterintuitive scheme for children and teens—teens aged 13-17 are more protected than children under 13. Because the NJDPA relies largely on COPPA to govern the personal data of children under 13, **Section 13:45L-7.4(a)** instructs controllers that they must obtain parental consent to collect or process the personal data of children that the controller has "actual knowledge" are under 13. This actual knowledge standard is consistent with COPPA. However, both the statute and **Section 13:45L-7.1(a)(3)** require controllers to obtain consent to process personal data if 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." This provision creates a discrepancy where controllers have a stricter duty to protect the personal data of teens 13-17 years of age than they do to protect the personal data of children under 13.

To ensure the personal data of all children and teens is adequately protected, we encourage the Division to change the knowledge standard in **Section 13:45L-7.4(a)** to "has actual knowledge, or willfully disregards" that a user is under 13. This revision would bring the personal data of children under 13 up to the same level of protection as the data of teens between 13 and 17.

Consent after opt out (13:45L-7.5)

The biggest concern around sending requests for consent after a consumer has already opted out is that it will cause consumers to experience a deluge of consent requests. Excessive requests for consent can have a countervailing effect known as consent fatigue, wherein consumers "consent" to various requests to be more efficient without paying attention to what they are consenting to. The rules in this subsection, particularly **Section 13:45L-7.5(b),** successfully outline clear rules for how businesses can interact with consumers who have opted out of various data practices while mitigating the risk of consumer consent fatigue.

Refusing or withdrawing consent (13:45L-7.6)

We commend the Division for including **Section 13:45L-7.6(c),** which protects autonomy by ensuring consumers can change their mind about whether to consent to certain data practices without suffering detrimental consequences. Importantly, **Section 13:45L-7.6(a)** requires controllers to allow consumers to withdraw consent using a method that is as easy as it was to give consent in the first place. This rule, in combination with those regarding deceptive design practices in **Section 13:45L-1.5**, is vital to protect consumer choice in a "notice-and-choice" regime.

Refreshing consent (13:45L-7.7)

We support the rules in this subsection because they ensure consumers are aware of and still consent to certain uses of their personal data, even if they have not interacted with a particular controller in a number of months or years, as **Section 13:45L-7.7(a)** contemplates. Similarly, **Section 13:45L-7.7(b)** ensures that controllers cannot change the way they use consumers' personal data without informing them of the change and obtaining new consent for the updated data practices.

SUBCHAPTER 8. DATA PROTECTION ASSESSMENTS

Minimum content (13:45L-8.1)

To make data protection assessments useful and meaningful, it's critical that the requirements are as unambiguous and specific as possible. This not only helps consumers and regulators assess the practices of systems used on them but also reduces the likelihood for regulatory circumvention. These draft rules reflect this need, and we commend the Division for the content of the current regulations.

In particular, we commend the Division's inclusion of **Section 13:45L-8.1(b)(4)(iv)**, which requires controllers to include the actual *names* of "third parties, affiliates, and processors that will have access to the personal data, the processing purpose for which the personal data will be provided to those recipients, and compliance processes that the controller uses to ensure the security of personal data shared with such recipients." Similar requirements that the assessments disclose information about security measures, types of data, and risks/harms are also important.

To strengthen the regulations further and ensure submissions are meaningful, we recommend the following improvements:

- ***Improve transparency about algorithmic systems and reduce "grading your own homework":*** Adjust **subsection (b)(10)** to include any audit conducted in relation to DPA disclosed and also require inclusion of information about the independence of the auditor and what they are assessing against (to ensure the company is not writing the rubric it is then testing itself against), in addition to the current disclosure requirements of name of auditor, name and position of those reviewing, and description of process.
- ***Clarify Section 13:45L-8.1(b)(4) with "including, but not limited to" statements to maximize actionable transparency:*** For the disclosure in the DPA about the elements of the processing activity, some statements clarifying the level of detail sought would be helpful. For example, "*sources of personal data, including but not limited to pixels, first party collection, data broker purchase, and if received from a third party the name...*" This can use the same language about personal data recipient in **Section 13:45L-8.1(b)(4)(iv)**, which is a particularly strong section as described above. Controllers should not only disclose who is *receiving* personal data from the processor, but who is *supplying* personal data to the processor.

Timing (13:45L-8.2)

We commend the clear requirement that a DPA must be conducted *before* initiating a processing activity. In the era of "move fast and break things," it's especially important to ensure entities follow the rules up front, not just ask for forgiveness later.

CONCLUSION

EPIC, CFA, NJCA, TechEquity Action, and Virginia Consumer Council applaud the Division's open and robust rulemaking process to protect consumers in accordance with the New Jersey Data Privacy Act. We will continue to be available for discussion about our recommendations and about how the Division can best protect New Jersey residents under the NJDPA, and we look forward to participating in future stages of this process.