November 8, 2021

Attn: Debra Castanon
California Privacy Protection Agency
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Dear California Privacy Protection Agency,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA").

Overview of the NAI

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to the NAI's FIPPs-based,[1] privacy-protective Code of Conduct (the "NAI Code"), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.[2] Member compliance with the NAI Code is promoted by a strong accountability program. It includes a comprehensive annual review by the NAI staff of each member company's adherence to the NAI Code, advising companies about how to best comply with the Code and guidance and implement privacy-first practices, penalties for material violations, and potential referral to the Federal Trade Commission (FTC). Annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

Several key features of the NAI Code align closely with the underlying goals and principles of the CPRA. For example, the NAI Code requires members to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising,[3] and requires members to disclose to consumers the

---

[1] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[2] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter NAI CODE OF CONDUCT], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[3] *See, e.g., id.* § II.C.1.a. The NAI Code of Conduct defines Tailored Advertising as "the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and

kinds of information they collect for Tailored Advertising, and how such information is used.[4] The NAI Code's strong privacy protections also go further than the CPRA in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for Tailored Advertising for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out of Tailored Advertising.[5]

I. Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses

The NAI supports the requirement for businesses that process personal information to conduct regular cybersecurity audits and data risk assessments. These risk assessments are also required by new privacy laws in Virginia and Colorado—referred to as Data Protection Assessments ("DPAs")—and are essential for responsible data processing that minimizes risk posed by the collection and processing of personal information.

The NAI's long-standing Code and self-regulatory program predate both these legal requirements and those established in Europe under Article 35 of the European General Data Protection Regulation ("GDPR"). The Code is in essence a program to identify and minimize privacy risks surrounding the collection and use of consumer data for digital advertising purposes. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.[6] In response to the new state law legal requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

New requirements for risk assessments will ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. However, a set of disparate requirements across multiple states threatens to create an environment where businesses are overwhelmed in their efforts to comply, with no discernable privacy benefit to consumers. The CPRA generally recognizes this by directing the California Privacy Protection Agency ("Agency") to cooperate with other states and countries "to ensure consistent application of privacy protections."[7]

Therefore, the NAI urges the Agency to develop and implement regulations that seek to harmonize to the greatest extent possible with the other state laws. We also offer the following recommendations regarding data risk assessments and cybersecurity audits.

Reporting, including frequency capping or sequencing of advertising creatives." *Id.* § I.Q. Capitalized terms used but not defined herein have the meanings assigned to them by the NAI Code of Conduct. *See generally id.* § I.

[4] *Id.* § II.B.

[5] *Id.* § II.D.2.

[6] *See* NETWORK ADVERTISING INITIATIVE, 2020 ANNUAL REPORT (2020), https://www.networkadvertising.org/sites/default/files/nai_annualreport-20_nolivetype_final.pdf; NETWORK ADVERTISING INITIATIVE, 2019 ANNUAL REPORT (2019), https://www.networkadvertising.org/sites/default/files/nai_annualreport_19_no-live_type_final.pdf.

[7] *See* CAL. CIV. CODE § 1798.199.40(i).

Data Risk Assessments

First, in seeking to harmonize risk assessment requirements with other state laws, the Agency should identify a consistent set of criteria for assessments to provide for the performance of a single assessment by businesses. The Agency should maintain a clear emphasis on processing that presents a heightened risk of harm to consumers. The new laws in Colorado and Virginia are largely consistent in their identification of activities requiring the performance of a risk assessment, so aligning with these two laws would not only be a practical step, but also a relatively efficient process. Similarly, Europe's GDPR requires the performance of data protection impact assessments (DPIAs) for data processing that "is likely to result in a high risk to the rights and freedoms of natural persons."[8] The law sets out three categories in which DPIAs are always required: systematic and extensive profiling with significant effects, processing of sensitive data on a large scale, and systematic monitoring of public areas on a large scale.[9]

Second, while the CPRA makes references to submission of risk assessments on a regular basis, the NAI recommends that the Agency clarify the requirement for performance of annual risk assessments, and allow the Agency to request risk assessments when they are relevant to an investigation or inquiry. This approach would conform with Virginia's privacy law, which provides for submission to the Attorney General upon request when there is an ongoing investigation of a business, and the assessment is relevant to that investigation.[10] This is also consistent with the approach taken under the GDPR, where businesses are required to conduct data impact assessments and to make these records available to a European data protection authority in the event of an audit or investigation arising from the controller's use of the data.[11] Importantly, it helps the Agency balance its resources more effectively by not creating an unnecessary overburden through an automatic production without cause.

Third, while the CPRA appropriately requires businesses to conduct risk assessments only after the law comes into effect on July 1, 2023, the Act does not explicitly clarify that data in a businesses' possession *prior* to the effective date would also not be subject to risk assessments moving forward. We therefore ask that the CPRA regulations clarify by adopting language consistent with the Colorado Privacy Act ("CPA"), which explicitly clarifies the application of the requirement to personal data that a business "*acquired on or after"* the CPA's effective date.[12] This approach is clear and efficient, providing

---

[8] "Art. 35 GDPR - Data Protection Impact Assessment." GDPR.eu, 23 July 2020, https://gdpr.eu/article-35-impact-assessment/.

[9] "When Is a Data Protection Impact Assessment (DPIA) Required?" European Commission - European Commission, 18 Dec. 2019, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en.

[10] *See* VA. CODE ANN. § 59.1-576 (2021). "The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-574." *Id.*

[11] GOV'T OF IR., GUIDANCE NOTE: GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS (DPIAS) (2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf at 17.

[12] COLO. REV. STAT. § 6-1-1309 (2021).

businesses the opportunity to establish forward-looking assessments and have greater confidence in their compliance efforts.

Finally, the assessments should be confidential, and the rules should recognize that privileged information or trade secrets will be redacted. This presents a practical approach to help companies maintain confidentiality of business practices.

Cybersecurity Audits

The CPRA implementing regulations should clarify that businesses are required to conduct cybersecurity audits on an annual basis, and they should establish clear requirements for retention of audit records. The requirement for cybersecurity audits should maintain a risk-based approach, where businesses can certify that they have implemented and adhere to policies and procedures designed to identify types of personal information and processing practices that present the greatest risk for the consumer's privacy or security. It should be a priority for the Agency to maintain consistency with existing security requirements and practices in California law,[13] as well as those promoted by the FTC, and requirements recently enacted in other state privacy laws.

The NAI recommends that the regulations align with current California law, enabling business to utilize existing certifications, such as the ISO 27000 series certification and those that leverage the NIST Cybersecurity Framework. Companies should retain the ability to develop and conduct their own internal cybersecurity program and engage third-party auditors. The Agency can also look to the programs established in cases where audits are required pursuant to consent decrees established by the FTC. Finally, businesses should retain the ability to either select independent third-party auditors of their choice in accordance with a set of qualifications established by the Agency or to conduct internal audits provided there are policies and other safeguards in place to ensure independence. On the latter point, California law already contemplates the ability of companies to conduct independent yet internal audits in the insurance context.[14]

II. Audits Performed by the Agency

The CPRA grants audit authority to the Agency, but it does not provide significant direction regarding the performance of audits. The NAI encourages the Agency to develop implementing regulations that provide an audit performed by the Agency must be triggered by evidence that a business has violated substantive provisions of the CPRA, creating either harm or a substantial risk of harm to consumers. The Agency should also confirm that its audit authority is separate and distinct from its enforcement authority for CPRA enforcement actions. Finally, the regulations should also require a majority of Agency members to vote in favor of an audit and to issue a resolution that cites the relevant evidence and defines the scope of the audit. The scope should be limited to addressing practices directly related to the misuse of personal information that necessitated the audit. Alternatively, the Agency might follow the lead of the Federal Trade Commission and require audits to be performed after an enforcement action against a business has been completed. The NAI urges the Agency to ensure that any audits required under the law are protected by strict confidentiality provisions that prevent disclosure to or use by third parties.

[13] *See* CAL. CIV. CODE § 1798.81.5 (2021).

[14] *See* CAL. INS. CODE § 900.3 (2021).

III. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

The NAI has a long history of promoting consumers' ability to exercise choice over uses of their data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use choice mechanisms is a foundational element of tailored advertising that we have championed for decades.

In crafting the provision regarding opt-out preference signals, the authors of the CPRA provided explicitly the option for businesses to have a choice whether to honor these signals, or to instead offer consumers the ability to opt-out through a link on their website or digital property.[15] In the case of relying on links to opt out, consumers determine on a case-by-case basis which businesses they will allow to sell or share their personal information. In the case of opt-out preference signals, users can set their preference to be applied across all businesses they interact with, for instance through a browser signal transmitting a consumer's preference across all websites that they don't want their personal information to be shared or sold.

Despite this flexibility created by the CPRA, we expect that many companies will elect to honor both approaches to maximize consumer choices about their data, and to minimize confusion for consumers who elect to activate opt-out preference signals. However, if technology companies who serve as intermediaries through which consumers access internet-based products and services seek to make decisions about selling and sharing personal information on behalf of consumers by using default-on settings, businesses will doubt the integrity of these signals as an expression of a genuine consumer choice. The regulations can play a valuable role in encouraging businesses to honor opt-out preference signals by ensuring that they reflect actual consumer choices.

To that end, the CPRA places specific parameters around the Agency's promulgation of such rules. Namely, the opt-out signal or mechanism must "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal **cannot unfairly disadvantage another business**."[16] According to the CPRA, the Agency must also ensure such opt-out preference signals or controls "clearly represent a consumer's intent and [are] **free of defaults constraining or presupposing such intent**."[17]

We urge the Agency to develop regulations that reflect these important priorities established by the CPRA to ensure consumer choices are genuine, that opt-out preference signal regulations do not favor certain businesses over others, remove businesses' ability to communicate the consequences of opt out choices to consumers, or stand in the way of true and informed consumer choices. Also, the regulations should recognize that in many cases, an opt-out preference signal should only apply to a specific

---

[15] According to the CPRA, businesses "**may elect**" to either "(a)… [p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information… through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]" The CPRA makes this business choice explicitly clear by stating: "**A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or (b).**" *Id.* § 1798.135(a)-(b) (emphasis added).

[16] *Id*. at § 1798.185(19)(A)(i) (emphasis added).

[17] *Id*. at § 1798.185(19)(A)(iii) (emphasis added).

browser, device or platform from which the signal is sent. This would be applicable in cases where the entity sending the signal is not known by the business receiving the signal, rather only a pseudonymous identifier is used by the business to identify a consumer, and the business does not take steps to associate that identifier with the specific consumer. Finally, the regulations should recognize that opt-out preference signals will in some cases present conflicting preferences by a consumer who has otherwise agreed to the business selling or sharing their data, and they should provide guidance that retains flexibility for businesses to resolve these discrepancies.

IV. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

For many years, the NAI has set the highest industry standard for defining sensitive data categories, and for requiring opt-in consent for the use of such data for advertising and marketing purposes. For instance, our definition has long included mental health and sexual orientation, even before European policymakers adopted a broad definition of sensitive personal information--referred to as special category data--under the GDPR. We recently further expanded the scope of sensitive data with the adoption of our 2020 Code of Conduct to also include new types of data that are increasingly being collected through mobile phones and connected devices, such as sensor data, and personal directory data that consumers enter or compile on their own devices. For all of this data, NAI member companies and their partners are required to obtain opt-in consent with clear and conspicuous notice about the sharing and use of this data for advertising and marketing purposes.

While the NAI definition of sensitive data closely aligns with the definition established by the CPRA, there are some categories of data where we diverge, notably regarding the inclusion of data that reveals a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership. We recognize and agree that many consumers have increased sensitivity around these data types, and that they present an increased likelihood of leading to disparate outcomes, particularly when processed for eligibility determinations. For that reason, the NAI prohibits the use of any data collected for advertising and marketing to be used for eligibility determinations. This approach preserves the ability of companies to tailor advertising based on these categories, but it mitigates the potential for harmful outcomes through these practices.

Indeed, there are many cases where these data types are utilized to reach at-risk communities and promote products and services that are beneficial to these populations. Most recently, tailored advertising was effectively deployed by health organizations to reach at-risk populations and educate them about the value of COVID vaccines.[18] Advertising for educational institutions and services is another key area where identification of these data types can have beneficial outcomes, such as promoting racial or ethnic diversity.

The NAI strongly shares the objectives of the CPRA to increase consumers' control over the use of their sensitive data, and more importantly to mitigate harmful outcomes around the processing of these data types. However, we encourage the Agency to also be mindful of the beneficial uses of this data, and to craft rules that do not unnecessarily limit opportunities presented by tailored advertising. As currently drafted, the CPRA definition of sensitive personal information is unclear as to the application of inferences. The NAI believes that this category should include data which is used to make such specific

[18] Dan Diamond, *It's Up to You: Ad Campaign to Encourage Coronavirus Vaccinations Get Underway*, THE WASHINGTON POST, (Feb. 25, 2021), https://www.washingtonpost.com/health/2021/02/25/covid-vaccine-ad-council/.

inferences, not that which merely *could* be used. This latter approach would encompass a much broader set of data, and it would alter the objectives and construct of the bill, which appropriately provides for different treatment of a narrower set of data categories.

With respect to the treatment of inferences, the guidance provided by the UK Information Commissioner's Office (ICO) regarding special category data, as defined consistently under the GDPR, establishes the following intent standard that could be applied effectively for the CPRA.

> "It may be possible to infer or guess details about someone which fall within the special categories of data. Whether or not this counts as special category data … depends on how certain that inference is, and whether you are deliberately drawing *that* inference."[19]

Advertising and marketing to individuals who have similar shopping and lifestyle interests could reveal, for instance, a similar race or ethnicity, but if those are neither declared by a user, nor intentionally inferred by a business to reach members of the population, the data should not be treated as sensitive data. The same guidance contains an example referring to collection of surnames and images relating to inferences and educated guesses based on those data categories, noting that if used for profiling it would likely constitute special category data.[20] Therefore, a practical interpretation for the CPRA would be to require opt-outs of selling and sharing sensitive personal information to profiling and targeted advertising practices that deliberately seek to target sensitive information categories, rather than merely those that could have the effect of disproportionately reaching individuals in these categories unknowingly. After all, large data sets can be processed in different ways, either seeking to reveal or target certain categories of individuals, to avoid drawing those specific inferences, or even with the goal of avoiding unintended disparate outcomes of the data processing. The regulations should therefore clarify this distinction, with the goal of incentivizing processing that avoids the use of sensitive data or making inferences about sensitive data categories, while still enabling uses of the data that can be beneficial to consumers and to businesses.

For example, in our *Guidance for NAI Members: Health Audience Segments*, the NAI distinguished between companies inferring that a consumer may have a certain health condition, a practice which requires a consumer's express consent, and generalized demographic targeting based on such demographic factors as age and gender to select the decile of the population that is most likely to be affected by a condition.[21] This approach was designed to balance the objective of reaching populations with valuable advertising and information, against potential privacy risks.

Taken in the context of the CPRA, the law's various provisions combine to enable privacy risk analysis and increase privacy protections for consumers, even when consumers do not exercise their right to limit the use and disclosure of their sensitive personal information. That is, the requirements for businesses to conduct data privacy risk assessments is crucial in helping to identify cases of processing personal information, even in the absence of sensitive personal information, that pose a heightened risk

---

[19] *What is special category data?*, INFORMATION COMMISSIONER'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION, (emphasis added) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7.

[20] *Id.*

[21] *See generally Guidance for NAI Members: Health Segment Audiences*, NETWORK ADVERTISING INITIATIVE (2020), https://thenai.org/wp-content/uploads/2021/07/nai_healthtargeting2020.pdf.

of harm to a consumer, and to identify whether the risks to privacy of the consumer outweigh the benefits.

V. Regulation and Enforcement of Dark Patterns

The vast majority of websites, apps and digital media services leverage data-driven advertising in order to maximize ad revenue. Indeed, data driven advertising is the leading driver of free and low-cost content across the digital ecosystem. These businesses therefore have an incentive to inform consumers about these practices, and to encourage them to share their data. At the same time, consumers have long expressed support for ad-supported content that is made available for free or low cost.[22] Ultimately, the interests of consumers and businesses are often aligned in this regard, and consumers are well served by websites and apps that engage tailored advertising and employ responsible data practices—this scenario is a win-win for consumers and business, and worth preserving.

The NAI's industry-leading self-regulatory program was founded with the mission to promote transparency around these mechanisms, and choice for consumers about the use of their data, as well as establishing use limitations to protect consumers from unexpected and harmful outcomes. The NAI has long promoted—and even required through our Code and self-regulatory program—notice and choice interfaces that are presented to consumers regarding their data collection should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain elections. Most recently, with the introduction of our 2020 Code of conduct, the NAI developed industry leading requirement, along with detailed guidance, that directs companies seeking the collection of consumer location data and other sensitive data to present clear and meaningful disclosures about the sharing and uses of the data for advertising and marketing purposes in conjunction with obtaining a user's consent.[23]

The concept of dark patterns was first identified in 2010, defined broadly as "tricks used in websites and apps that make users do things they otherwise would not necessarily do, such as buying or signing up for something."[24] These practices, which span much more broadly than the collection of consumers' personal information, have received well deserved attention and enforcement as policymakers at various levels seek to discourage and enforce against them. Thus far, most cases where the FTC has brought enforcement actions, have been focused on business practices that lead to upselling consumers on services and subscriptions such as the enforcement case against Age of Learning, Inc. that involved misrepresentation with respect to membership cancellation leading many to renew their membership without clear consent.[25]

---

[22] NAI's 2019 consumer survey revealed that nearly 60% of respondents prefer their online content to be paid for by advertising, while another question sought feedback from consumers on how much they currently pay for online content and how much they would be willing to pay. Nearly 90% said they are unwilling to pay a significant amount of money to continue receiving apps and online content that they currently receive for free. The survey provided a strong affirmation that the ad-supported content model is ideal for most consumers. *See* Network Advertising Initiative, *NAI Consumer Survey on Privacy and Digital Advertising*, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/.

[23] *See Guidance for NAI Members: Opt-In Consent*, NETWORK ADVERTISING INITIATIVE (2019), https://thenai.org/wp-content/uploads/2021/07/nai_optinconsent-guidance19.pdf.

[24] DARK PATTERNS, http://www.darkpatterns.org

[25] *Fed. Trade Comm'n. v. Age of Learning, Inc.*, No. 2:20-cv-7996 (C.D. Cal. Sept. 8, 2020), https://www.ftc.gov/enforcement/cases-proceedings/172-3186/age-learning-inc-abcmouse

Despite the leadership of the NAI and other self-regulatory efforts across the digital advertising industry, consumers are all too often subject to deceptive and unfair practices around data collection. As a result, we are currently placing even greater emphasis on our efforts to educate businesses and discourage these practices. To that end, we are developing more detailed recommendations that draw from the ongoing discussions at the FTC, as well as CCPA and CPRA requirements, and perspectives from other key stakeholders.

At the same time, California regulators and other policymakers are right to focus specifically on enforcing against deceptive and unfair practices associated with consumer data collection. The CPRA, and the preceding regulations pursuant to the CCPA, define dark patterns as a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.[26] With respect to consumer requests to opt out of the sale of their personal information as authorized under California law, the California Office of the Attorney General ("OAG") has directed through regulations that businesses must make the process easy for consumers to execute and must follow a minimal number of steps.[27] Moreover, a business must not use a method "designed with the purpose or [having] the substantial effect of subverting or impairing" the consumer's choice.[28]

The NAI concurs with the scoping of this definition, and we share the goal of maintaining user autonomy over their own decisions about the use of their data, in this case pertaining to the sale or sharing of their data by each business with which they interact. Notices and choice interfaces that are presented to consumers should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain decisions. At the same time, businesses should retain the flexibility to present user information, choices, and notices to consumers in ways that are practical for each particular business, and the consumer, to facilitate informed choices about whether their data may be sold by a business, as long as these practices don't amount to deception or tricks, and that user autonomy is not undermined. To achieve this important balance, the NAI offers the following recommendations for the Agency.

The Agency should clarify current CCPA regulations to ensure that businesses can perform consumer education and communicate effectively with their consumers.

Under the current proposed regulations, a business may not require consumers to click through or listen to reasons why they should not submit a request to opt out before confirming their request.[29] The NAI concurs with the objectives of this regulation: a consumer should not be forced to unreasonably click through a lengthy list of reasons that unnecessarily hinders their ability to submit their request to opt out. However, this should not prohibit businesses from providing concise meaningful and truthful notices or disclosures that inform users about their decisions, including informing users about the potential harms related to an opt out, as long as these are truthful and do not obstruct a consumer's intentions to opt out. Additionally, as various states enact differing opt-out requirements, it could be a necessary service to consumers for businesses to explain differences in these requirements.

For example, prior to the delivery of a privacy-related permission request, a business could reasonably provide a concise explanation of the types of sales or sharing that it engages in, and notify its consumers that it relies on the use of this data to monetize free or low-cost products and services. As long as this is

[26] CAL. CIV. CODE § 1798.140(l) (2021).

[27] CAL. CODE REGS. tit. 11, § 999.315(h) (2021).

[28] *Id.*

[29] CAL. CODE REGS. tit. 11, § 999.315(h)(3) (2021).

not done in a way that impairs or unnecessarily delays the consumer's decision to opt-out of the sale or sharing of their information, this does not undermine a consumer's ability to easily make an informed choice. Ensuring the regulations strike this balance is important for the Agency to tailor the regulations to avoid a conflict with First Amendment free speech principles.

The Agency should avoid developing technical specifications or specific user interfaces that prescribe how choices should be offered.

The Agency's proposed regulations include a non-exhaustive list of examples of dark patterns.[30] These examples involve overly complicated or lengthy processes for opting out of selling personal information, confusing or misleading language, and requiring consumers to click through a list of reasons to not opt out.[31] Taking this totality-of-the-circumstances approach, rather than seeking to develop or prohibit specific user interfaces, is the right approach. Ultimately, what could constitute a dark pattern in one circumstance, such as a multi-click interface on a website, could actually serve consumers more effectively if offered on small screen devices that ease consumer choice through clear interfaces.

The Agency should be mindful of so-called "light patterns" or "bright patterns."

In contrast to dark patterns, "light patterns" or "bright patterns" have been referred to as practices that make it easy for consumers to navigate, read, and follow directions or make choices in general. Alternatively, it could be described as a practice that makes a proactive choice on behalf of consumers, with their best intentions in mind.[32] These "best intentions" are not uniform across the consumer experience, and therefore these practices should be approached carefully. For example, according to a 2019 NAI survey, 60 percent of consumers prefer to have online content sponsored by advertising, rather than paying subscription fees for individual websites and apps.[33] A user interface that assumes data-driven advertising is not in the best interest of consumers fails to contemplate negative market externalities to those consumers, such as an increase in fees and subscription-based digital content.

The Agency should be guided by the findings, recommendations, and enforcement activities of the Federal Trade Commission.

As the federal administrative body that oversees consumer protection throughout the FTC has produced a body of opinions and rulemakings that should guide the Agency in how it defines and regulates dark patterns. In particular, the Agency should be mindful of the FTC's regulations regarding deceptive acts or practices, and whether any omissions or misrepresentations are material. Under well-established FTC standards, an act or practice is deceptive if it (1) is *likely* to mislead the consumer; (2) is one a *reasonable* consumer would consider misleading; and (3) is a *material* misrepresentation.[34] For a

---

[30] CAL. CODE REGS. tit. 11, § 999.315(h)(1)-(5) (2021).

[31] *Id.*

[32] *See, e.g.,* Coleman, Aidan*, Light and Dark UX Patterns,* Medium*, Prototypr,* 26 May 2019, blog.prototypr.io/light-anddark- ux-patterns-19ffcaa50e9a.

[33] Network Advertising Initiative, *NAI Consumer Survey on Privacy and Digital Advertising*, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/.

[34] Letter from James C. Miller, Chairman, Federal Trade Commission, to the Hon. John D. Dingell, Member of Congress (Oct. 14, 1983) (https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

misrepresentation to be material, it must be one that is likely to affect a consumer's choice or conduct regarding a product.[35]

These are practices and regulations businesses in California—and the entire United States—have been adhering to for decades. Businesses are familiar with the requirements and have modeled their best practices around them. Importantly, in recent years the FTC has considered dark patterns to be an example of a deceptive act or practice and have been pursuing enforcement actions accordingly.[36] By following the FTC's standards, the Agency can ensure its regulations are consistent with federal law.

VI. Updates or additions, if any, that should be made to the categories of "personal information" given in the law.

There is broad agreement around the inclusion of an internet protocol address (IP address) as a data type that could be considered personal information. The CPRA definition of personal information includes persistent identifies such as an IP address, but only if it "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This definition aligns generally with the conclusion reached by the FTC dating back to their 2012 Privacy Report, which also focused on the ability to link these to specific individuals.

While it is true that in many cases businesses can and do associate IP addresses with specific individuals or households, many fundamental uses of IP are not related to identifying a specific individual or household, such as monitoring website traffic, identifying a general location of a consumer, such as the state in which they live, and even deterring malicious activity. Additionally, many IP addresses do not function at a personal or household level, rather they are associated with businesses or even communities, such as in the case of public Wifi networks. IP addresses can therefore be used for many practical purposes without creating privacy risks, particularly when combined with additional privacy-protective tools and policies, such as anonymization, encryption, and restricted forms of access. In recognition of this, the February 2020 modified proposed regulations, the California Attorney General added an example stating that "if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be 'personal information.'"[37]

Unfortunately, the final CCPA regulation removed this helpful language. The NAI recommends that the Agency restore the example and clarify that IP addresses, when used with appropriate practices and controls, cannot be reasonably linked to a particular consumer or household.

---

[35] *Id.*

[36] *See, e.g., In re Zoom, Inc.*, F.T.C. No. C-4731 (2021) (complaint).

[37] CAL. CODE REGS. tit. 11, § 999.302(a) (2021).

VII. Agency Enforcement

The NAI offers the following recommendations regarding the Agency's enforcement of the CPRA.

Delay enforcement sufficient to provide business compliance following adoption of final regulations

The CPRA empowers the agency to begin enforcement in January 2023, a date that is now less than 14 months away. While it was the goal of the CPRA for enforcement to begin on this date, the legislation underestimated the task of establishing a new Agency, and the process for development and finalization of implementing regulations. The NAI recognizes the need for timely enforcement, but it is also imperative that businesses be given sufficient time to update their policies and practices to comply with the regulation. We therefore request that the Agency provide a delay in enforcement as necessary, or exercise leniency in enforcement for an appropriate period of time to provide for a reasonable duration for businesses to come into compliance.

Maintain 30-day cure period for businesses first offense when demonstrating reasonable efforts to comply

The CPRA presents many significant updates and changes from the CCPA, and pending regulations are expected to also provide new direction for businesses across a wide range of processing consumers' personal information. The mandatory cure period established by the CCPA was removed from the statute to address concerns that companies would wait to comply with key requirements of the CCPA until they received a warning, and to take the opportunity to comply only after being called out by Californian regulators. While the NAI concurs that this is an outcome that should be discouraged, a cure period provides a valuable tool for companies seeking to comply, enabling well-intentioned companies from being penalized.

Although the CPRA removes the requirement for a "30-day cure period," the Agency maintains the ability to utilize its discretion to apply this approach in cases it deems appropriate, such as cases where companies are demonstrating a good-faith effort to comply with the law, and where reasonable measures could bring that company into compliance quickly. The goal of the CPRA, and all data privacy and security laws and regulations, is to enhance privacy and security for consumers. The NAI therefore recommends that the Agency retain the use of a 30-day cure period for first-time enforcement with a particular business, particularly in cases where the business has demonstrated a reasonable attempt to comply with the CPRA and implementing regulations and is not a repeat offender.

VIII. Conclusion

Again, the NAI appreciates the opportunity to submit preliminary comments to the Agency on the rulemaking process for the CPRA. We look forward to reviewing a draft of the regulations and providing specific comments at a later date. In the meantime, if we can provide any additional information, or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact me at leigh@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

*****

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)