March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834
Via email: regulations@cppa.ca.gov

Re: PR 02-2023

Dear California Privacy Protection Agency:

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit comments on proposed rulemaking around cybersecurity audits, risk assessments, and automated decisionmaking (ADM).

Background on SIIA

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies, many based in California or primarily serving California residents. Our members include a range of broad and diverse digital content providers and users in specialized content industries, academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. On behalf of our members' wide interests and services, SIIA has long advocated for privacy protections.

I. Cybersecurity Audits

Question I.3. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits, assessments, or evaluations comply with CCPA's cybersecurity audit requirements?

Response to Question I.3.

We recommend that the Agency allow businesses to comply with cybersecurity audit requirements by submitting self-certifications required by other laws and/or certifications that indicate compliance with industry standards. Cybersecurity audits are necessarily dependent on the nature of the business being audited, and it is important that the requirements are tailored to the types of information systems used by businesses in different sectors. There is a risk that audit requirements that are not sufficiently tailored

will create enormous compliance costs for businesses that are not tailored to achieve the desired objectives.

Question I.4. With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the Agency consider to ensure that cybersecurity audits will be thorough and independent?

Response to Question I.4.

We recommend that the Agency allow businesses to rely on industry standards for cybersecurity audits, assessments, and evaluations. The Agency could promote best practices to ensure that audits are undertaken in an independent manner.

II. Risk Assessments

Question II.1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?

Response to Question II.1.

Privacy risk assessments have become increasingly common in jurisdictions with privacy laws and we encourage the Agency to align California's rules to those already in place that cover substantially similar data processing activities. We would recommend the Agency look to existing obligations under Virginia and Connecticut law as models for risk assessment requirements.[1] These jurisdictions have taken care to implement risk assessment requirements that meet the needs of consumers. We would urge caution in expanding the scope of risk assessments that businesses are already conducting unless there is a clear indication that those existing legal frameworks are inadequate to the purpose (and we are aware of none).

In addition, we recommend that risk assessments should be limited to processing of personal data that may have a legal or similarly significant effect on the individual consumer, such as processing that affects access to employment, educational opportunities, housing, and access to financial services. Expanding the scope of risk assessments to cover all processing of personal data will have significant downstream effects that would likely undermine consumer welfare and present compliance challenges to businesses that will especially hurt small- and medium-sized enterprises.

[1] https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/; https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF.

While we recognize that the GDPR requires risk assessments, we would caution the Agency against adopting the GDPR approach as it currently stands. The GDPR requirements remain subject to development, compliance hurdles, and legal challenges, and are not adaptable to the U.S. landscape without careful finetuning. We recommend looking to other U.S. jurisdictions as guideposts on what may be appropriate for risk assessment requirements.

III. Automated Decisionmaking

Question III.1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

Response to Question III.1.

On November 8, 2021, SIIA provided the Agency with recommendations to guide rulemaking around ADM technology. We recommended that the Agency look to develop a risk-based framework for assessing such technology and focus on decisions that have a direct effect on the legal rights of the natural person subject to ADM (rather than the technology itself).[2] We continue to recommend this approach as the Agency develops regulations and supplement our prior recommendations as follows.

First, the Agency should develop a robust record regarding the benefits and myriad uses of ADM technologies for consumers. With respect to the internet ecosystem, ADM technologies are used in many ways to provide services that consumers rely on and expect. This includes using ADM technologies to personalize services, filter content (such as movie and music recommendations), improve the user experience, and assist organizations (including non-profits and government agencies) in finding the leads and information they need to execute their operations more effectively. The vast majority of these uses do not have legal or similarly significant effects on consumers and should be considered "low risk" and not subject to further regulation.

Second, the Agency should focus ADM rulemaking on high-risk decisions. We recommend that the Agency focus rulemaking on those decisions that have "legal or similarly significant effects" on individual consumers that are rendered through fully automated processes, and represent final decisions. As we noted, this approach would align with that of the GDPR, which in Article 22 protects consumers from decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[3]

This approach would also align with laws enacted in other states. Among the laws that require access and/or opt-out rights in the context of automated decision-making are privacy laws enacted in other states. For example, state privacy laws in Colorado, Connecticut, and Virginia permit opt out for high-risk

[2] https://www.siia.net/wp-content/uploads/2021/11/CPRA-Comments.pdf
[3] https://gdpr-info.eu/art-22-gdpr/

decisions – those that, in the case of Colorado and Virginia, have "legal or similarly significant effects" and, in Connecticut, are "solely" automated decisions.[4] The approach taken in Virginia's Consumer Data Protection Act (VCDPA) provides a good model for the Agency's rulemaking. Under the VCDPA, "[d]ecisions that produce legal or similarly significant effects concerning a consumer" is defined to mean "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."[5]

We strongly recommend that California adopt the same approach, focusing on high-risk decisions rendered by ADM technologies – rather than the technologies themselves – and limit any rulemaking to those decisions reached through fully automated processes. Regulatory interoperability should be a guiding principle for the Agency. Consumers should have uniform expectations regarding access to important technologies and personalization, and a patchwork approach at the state level will invariably lead to increased compliance costs for businesses that will be passed on to consumers and create barriers for small- and medium-sized enterprises to provide services to California residents.

Question III.2. What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

Response to Question III.2.

Many of SIIA's member companies have implemented robust frameworks to advance responsible AI in ways that mitigate potential unintended bias from algorithms and datasets, to advance transparency and explainability, and to mitigate safety, security, and reliability concerns. The need to augment these frameworks to provide for access and/or opt-out rights is minimal with respect to common, everyday uses of ADM – such as those ADM engines that generate recommendations for entertainment, provide automated spellcheck or word suggestions, and so on. These "low-risk ADM" technologies do not generate legal or similarly significant effects on consumers and do not require regulation. Regulating low-risk ADM technologies would have a negative impact on consumer welfare and also impede business innovation in ways that benefit consumers.

As noted above, we strongly recommend that the Agency focus any rulemaking on "high-risk ADM." In advancing rules to ensure the safety, security, and unintended bias of high-risk ADM, we recommend that the Agency align any rulemaking to expert-driven efforts that are currently underway in the United States and internationally. The National Institute of Standards and Technology (NIST) in January 2023

[4] https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf; https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF; https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

[5] https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

released detailed guidance for assessing and mitigating risks associated with AI.[6] The NIST AI Risk Management Framework is a good touchpoint for companies of all sizes to assess the risks associated with their use of ADM technologies. We recommend the Agency refer to the Framework as a key element of best practices for companies.

Question III.3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2: a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not? b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the processes and goals articulated in Civ. Code § 1798.185(a)(16)? c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements? d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers? e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers? **f.** Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?

Response to Question III.3.

The Agency should endeavor to align its definition of key terms such as ADM and ADM technology with how those terms are understood and used in existing legal regimes. We recommend that California align its rules with those of the VDCPA and, further, define ADM as "final decisions made through fully automated processes that employ artificial intelligence technology and result in a legal or similarly significant effect concerning an individual." We further recommend that California provide a clear definition of AI that aligns with the definition in the NIST AI Risk Management Framework.

Question III.4. How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

Response to Question III.4.

ADM technologies, including algorithms, have been used for decades by businesses in virtually every sector. These technologies provide ways to streamline operations, provide customized consumer experiences, improve products and services, and address consumer needs. Most uses of AI do not rise to

[6] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

the level of high-risk as we describe in this submission and do not generate decisions that have legal or similarly significant effects on consumers.

Question III.7. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Response to Question III.7.

Algorithmic discrimination, which refers, under one definition, to "unjustified different treatment or impacts disfavoring people based on" their identification in various protected classes, as a result of automated systems,[7] is a significant issue that must be addressed in the design, development, and deployment of ADM technologies. While we encourage the development of guardrails to protect against algorithmic discrimination, we would caution against using access and opt-out rights as appropriate tools to mitigate unintended bias in ADM systems. Instead, we would recommend that the Agency consider rules (such as safe harbors) that recognize the need to collect – rather than restrict collection of – data that relates to identification with protected classes, at least in the context of high-risk ADM, with the consumers' consent. Having additional information about individuals may be critical to ensuring that datasets that inform ADM systems are sufficiently robust to anticipate and prevent unintended bias with respect to critical, high-risk decisions.

Question III.8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

Response to Question III.8.

Access and opt-out rights, if appropriate, should be tailored by sector and usage. Even with respect to high-risk ADM, the requirements will differ depending on context. We recommend deference to sector-specific approaches and frameworks, such as in the employment context, where there are already robust efforts underway to craft regulatory approaches.

In addition, there are situations in which access and/or opt-out rights would be harmful to the consumers who may benefit from ADM technology, even in high-risk scenarios. The Agency should take care to identify scenarios in which consumers could be harmed by having access or opt-out rights. In situations where ADM technologies are used to detect fraud, to facilitate medical care and emergency treatment, and others, permitting access or opt-out could undermine the efficacy and effectiveness of

[7] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

those ADM-driven services and cause harm to consumers who rely, directly or indirectly, on those services.

Question III.9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer?

Response to Question III.9.

Regulations that require detailed information on specific decisions and the processes that lead to those decisions and processes run the risk of revealing trade secrets, which will have downstream effects on consumers and serve as a barrier to innovation. We believe the meaningful information can be provided to consumers and the broader public through general descriptions of how the high-risk ADM systems work and how those systems are used. We would caution the Agency against requiring detailed disclosures of algorithms or datasets and encourage the Agency to exempt disclosure of information that would reveal trade secrets or proprietary information.

Question III.10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

Response to Question III.10.

We recommend that the Agency avoid creating new access or opt-out requirements without a fulsome understanding of the unintended consequences and, to the extent the Agency moves ahead with access or opt-out requirements, they should apply only to high-risk decisions. A broad approach to regulating in the ADM space will have a negative impact on consumer expectations and experiences, and could raise safety and security risks - including by limiting the ability of businesses to protect individuals from harmful content and cybersecurity risks.

In addition, we recommend that the Agency include critical exceptions to any access or opt-out rights to avoid consequences that may result from individuals (including bad actors) who seek to undermine processes that are in place to protect consumers. For example, access and opt-out rights could be abused by individuals to circumvent detection of fraudulent and malicious activity, undermine processes designed to buttress the safety and security of online platforms, assist government agencies in criminal, regulatory, and other matters, and more.