Computer & Communications Industry Association
Tech Advocacy Since 1972

Statement of

Alyssa Doom
State Policy Director
Computer & Communications Industry Association

Regarding

Pre-Rulemaking Stakeholder Sessions
California Privacy Protection Agency

May 4, 2022

Chair Urban and Members of the California Privacy Protection Agency:

Thank you for the opportunity to provide input on the upcoming rulemaking under the California Privacy Rights Act, or "CPRA". My name is Alyssa Doom and I am speaking today on behalf of the Computer and Communications Industry Association, or "CCIA". CCIA is a nonprofit, nonpartisan trade association that for 50 years has represented a broad cross section of small, medium, and large communications and technology firms. Our members place high value on the protection of individual privacy and support the important principles that underpin the CPRA, including transparency, accountability, and consumer control over how their data is processed and used.

CCIA has long supported enactment of comprehensive federal baseline privacy legislation to avoid the creation of a divergent set of state privacy laws that could result in a confusing and burdensome regulatory patchwork. However, we understand that in the absence of a federal regime, state lawmakers have a continued interest in enacting local privacy policies to protect consumers. As such, the Association has proposed a set of state privacy principles to inform legislators as local legislation is considered. Among these is the need to adopt a risk-based approach to privacy protections. My brief comments will focus on the importance of adopting a risk-based model for regulating the use of automated decision-making tools.

CCIA recommends that rules concerning automated decision-making focus on securing protections for consumers with respect to decisions that are *fully automated* and that may have *legal or similarly significant effects*. The rules should not create unnecessary restrictions for low-risk systems and tools that support ordinary business operations and transactions. We advise that regulations involving automated decision-making reflect the following principles governing regulatory terminology, access to meaningful information, and consumer opt-outs.

1. **Regulatory Terminology**

I will first focus on regulatory terminology. The regulation of "automated decision-making" is an emerging concept in privacy law and, as such, the term lacks clear, universally accepted legal definitions. Under the CPRA, the term "automated decision-making" could be interpreted so broadly as to encompass a range of low-risk processing activities and basic tools that have proven beneficial for both businesses and consumers, such as spreadsheets or spell-checkers. The term could even reach the automated tools Internet companies rely on to responsibly moderate their services and keep their users safe, such as chat, spam, and abuse filters. The adoption of overly inclusive regulatory terminology could impede the use of such widely accepted tools. Therefore, we recommend that the regulations ensure that businesses shall only be obligated to implement access or opt-out requests with respect to fully automated decisions involving personal information having legal or similarly significant effects, such as processing that impacts access to medical treatment, public assistance, or credit decisions.

2. **Access to Information About Automated Decisions**

Next, I will turn to potential regulations governing consumers' access to information about automated decision-making. Again, CCIA recommends that the forthcoming regulations focus on high-risk automated decision-making processing. Here, the Agency should provide guidance on how to develop notices that contain clear information regarding the purpose of the high-risk automated processing and the source, categories, and relevance of the processed information. Companies should be able to make these disclosures through existing websites and transparency notices. Explanations should be straightforward, allowing users to understand the impacts of the automated decision-making on their lives. Importantly, the degree to which businesses will be required to disclose this information should be proportionate to the level of risk associated with the automated decisions and should not implicate trade secrets or business sensitive information. Disclosures should only be required in connection with automated decisions that produce legal or similarly significant effects for consumers. An obligation to provide disclosures for each type of low-risk automated decision would overwhelm businesses and have no clear benefit to consumers. In addition, and equally important, regulations should not require businesses to disclose trade secrets or proprietary information such as algorithms or source code. These types of disclosures are unlikely to provide meaningful protections against risk, are of little practical use to consumers, and can severely chill not only the provision of good customer service but also innovation and speech.

3. ***Opt-Out Rights With Respect to Automated Decisions***

Finally, consistent with emerging U.S. privacy regimes, only fully automated decisions that produce legal or similarly significant effects should be subject to rules establishing consumer opt-out rights. To provide greater legal certainty, regulations should specify the categories of use cases that would be implicated here – such as decisions that result in the provision or denial of financial or lending services or access to essential goods or services. Broader applicability to low-risk decisions would impede ordinary business activity and diminish the availability and functionality of personalized consumer services. Lastly, in instances where high-risk automated decision-making processing is essential to provide certain services or where a core function of the service is its

automation, businesses should be able to demonstrate to consumers supplemental precautions taken instead of offering opt-out options.

***

In sum, requiring prescriptive, one-size fits all privacy controls that cover the processing of non-sensitive or de-identified data would be inconsistent with consumer expectations, degrade user experience, and hinder legitimate business practices. We believe the Agency can mitigate these pitfalls, while upholding privacy protections, by promulgating regulations with these principles in mind.

CCIA welcomes the thoughtful and deliberative approach taken by the Agency in considering the key operational and enforcement issues introduced or modified by the CPRA. I will also be submitting these remarks in a written format alongside CCIA's State Privacy Principles and invite Members to contact me following the hearing should questions arise.

Computer & Communications Industry Association
Tech Advocacy Since 1972

Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices

As the economy becomes increasingly data-focused, it is important for the U.S. to have a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights, transparent data processing, and organizational accountability. The digital economy is not constrained by state borders, and consumer interests and economic competitiveness will be best served by the development of baseline, federal privacy legislation. However, in the absence of a nation-wide framework, many lawmakers are debating whether to enact state-level consumer privacy rules. Though the adoption of divergent state privacy laws risks the emergence of a confusing and burdensome regulatory patchwork, carefully drafted state-level privacy legislation can also advance consumer protection while promoting the responsible processing of information that leads to data-enabled innovation and new technologies benefiting U.S. consumers and businesses. Therefore, CCIA presents these privacy principles to help inform stakeholders considering local privacy legislation.

Scope and Definitions

Effective consumer privacy legislation should clearly articulate what entities are subject to the law and to which types of data protections apply. Where practicable, policymakers should make an effort to align key definitions with consensus consumer privacy standards in both law and practice in order to promote regulatory interoperability and mitigate unnecessary compliance burdens.

- **Covered Organizations**: Legislation should extend to all private organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold. Legislation should apply regardless of a business's sector or whether it collects information in an online or offline context. While some state privacy laws have excluded small businesses, policymakers should consider that potential risks resulting from the processing of personal data are not necessarily mitigated by the size of the data controller.

- **Personal Data**: Legislation should apply to information that is linked or reasonably linkable to a particular individual. While different types of personal data can vary in sensitivity depending on the context, some personal data is almost always sensitive and may warrant heightened protections under the law.[1] Furthermore, consumer privacy legislation should exclude publicly available information, as well as information that has been collected in an employment or business-to-business communications context, including as a job applicant

[1] U.S. state privacy laws have recognized certain discrete categories of "sensitive" personal data including: (1) information revealing racial or ethnic origin, religious beliefs, mental or physical health information, sexual orientation, and citizenship or immigration status; (2) biometric data processed for the purpose of uniquely identifying a natural person; and (3) data collected from a known child.

or as a beneficiary of someone acting in an employment context. Finally, in order to incentivize more protective data processing and storage, privacy laws should include carve-outs for information that is maintained in a de-identified or pseudonymous format.

- **Controllers and Processors:** Legislation should include a role-based distinction between "data controllers" that typically have a first-party relationship with data subjects and determine the collection and use of personal information and "data processors" that perform services on behalf of a controller. Data controllers are better situated to receive and implement the exercise of consumer rights while data processors should meet certain contractual obligations to support lawful and protective data use.

- **Exceptions:** Legislation should incorporate common sense exceptions to clarify requirements for covered organizations and to promote uniformity with international and domestic laws. Common exceptions include those for existing federal privacy regimes such as HIPAA, or exceptions for covered entities related to disclosure of trade secrets.

Consumer Rights

Consumers should feel confident they have control over their personal data, which will promote trust and participation in the digital economy. Privacy law should establish baseline rights for consumers over their personal information, no matter where it is collected or for what commercial purposes it is used.

- **Choice**: Legislation should empower consumers with greater choice over the use of their personal information. Leading jurisdictions have created **opt-out rights** for data processing for the purposes of sale to third parties, cross-platform targeted advertising, and profiling in furtherance of decisions with legal or similarly significant effects. For data processing that presents particular risks, policymakers should consider requirements that controllers obtain affirmative **consent** prior to the collection of sensitive data. Importantly, privacy law should align with the reasonable expectations of consumers, and avoid creating unnecessary friction that can result in "consent fatigue" or degrade user experiences.

- **Control**: Consumers should have the rights to reasonably **access**, **correct**, and **delete** personal information held by a covered organization. Furthermore, consumers should have the right to acquire data they have provided to a controller in a machine-readable, **portable** format when technically feasible. To protect against fraudulent requests, data controllers should be required to comply only with requests that are authenticated through commercially reasonable efforts. Controllers should not be empowered to require that consumers create new accounts to exercise requests, but should be able to require that consumers exercise requests via existing accounts.

- **No Retaliation:** Consumers should be protected from retribution from companies for exercising their privacy rights. However, this right should account for the fact that certain data processing is necessary for providing a requested product or service and include

exceptions for data processing that is relevant to participation in bona fide loyalty or other rewards programs.

- **Appeals:** Privacy legislation should require covered organizations to establish mechanisms for consumers to contest the denial of a consumer right under the law and to provide information for a consumer to contact the regulator to submit a complaint.

Responsibilities for Covered Organizations

In addition to empowering consumers with new rights, privacy legislation should require that covered organizations meet baseline standards for the safe and ethical use of personal data. Policymakers should consider the following threshold requirements applicable to organizations collecting, holding, and processing personal information.

- **Transparency:** Covered organizations should provide clear and accessible notices about the types of personal information that they are collecting and how they may use it. Effective notices should also state what categories of third parties personal information may be transferred to, and what choices and controls individuals have with respect to their personal information. Covered organizations should limit their collection of data to what is reasonably necessary for their clearly disclosed purposes.

- **Data Security:** Covered organizations should maintain a security program and follow reasonable measures to protect the confidentiality, integrity, and accessibility of personal information.

- **Risk Assessments:** Covered organizations that collect sensitive data or engage in processing that presents a heightened risk of harm to consumers should conduct and document a risk assessment that weighs the benefits and risks of data processing and applicable safeguards. Risk assessments should be producible to regulators conducting an investigation but should be otherwise exempt from public disclosure. Regulators should also accept risk assessments conducted pursuant to comparable legal regimes.

Ensure Practicable Compliance

The enactment of new consumer privacy legislation can be challenging and costly from a compliance perspective, and carries the risk of disproportionately impacting small and medium-sized organizations. To ensure that covered organizations have predictability in meeting their compliance obligations by the time a law becomes effective, privacy legislation should adhere to the following principles.

- **Technology Neutral:** Legislation should be principles-based, and afford differently situated organizations flexibility to meet legal standards by avoiding specific technological mandates.

- **Effective Date:** Complying with a new privacy law frequently requires covered organizations to engage in lengthy processes such as reviewing and potentially reconfiguring IT systems and renegotiating contracts with vendors and service providers. Legislation should allow covered organizations sufficient time for compliance, typically at least 18 months after a law's enactment.

- **Voluntary Consensus Standards**: Legislation should promote interoperable compliance across jurisdictions by recognizing and incentivizing participation in designated safe harbor programs and adherence to codes of conduct representing industry best practices for privacy and security.

- **Rulemaking:** Legislation should avoid sprawling rulemaking processes that could have the effect of turning a legal statute into a "moving target" and disincentivize early investment in compliance. Any rulemaking should be narrowly focused on specific implementation issues or enabling the law to be updated in light of changes in technology and business practices.

Enforcement

Privacy legislation should provide adequate funding for enforcement through the Attorney General or other comparable state consumer protection offices. Privacy laws should not include private rights of action, which have been shown to have the impact of attracting nuisance suits and distorting incentives away from risk-based compliance. Finally, in order to enable organizations acting in good faith to rapidly bring their data practices into compliance, legislation should include an **opportunity to cure** allegations of defective conduct prior to a formal enforcement action.