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

March 27, 2023

Re: PR 02-2023

Mr. Sabo:

The Insights Association ("Insights") submits the following comments on proposed rulemaking related to cybersecurity audits, risk assessments, and automated decision making, per the invitation of the California Privacy Protection Agency (the "Agency").

Representing more than 900 individuals and companies in California and more than 7,200 across the United States, Insights is the leading nonprofit trade association for the market research[1] and data analytics industry. We are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The California Privacy Rights Act ("CPRA") is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 ("CCPA"). Accordingly, and on behalf of our members, we commend your decision to seek input and are grateful for the opportunity to comment.

1. In determining what processing presents a "significant risk" to consumers' privacy or security, use a clearer, more concise approach than the European Data Protection Board's Guidelines on Data Protection Impact Assessment (the "Guidelines").

On page 5 of the Agency's invitation for comments, the Agency asks about the benefits and drawbacks of following the Guidelines.

[1] Market research, as defined in model federal privacy legislation from Privacy for America, is "the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (ii) used to advertise or market to any particular individual or device." See Part I, Section 1, R: https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/

The Guidelines include nine different criteria for determining what processing operations are "likely to result in a high risk"; namely, (1) evaluation or scoring, (2) automated decision-making, (3) systematic monitoring, (4) sensitive data, (5) data processed on a large scale, (6) matching or combining datasets, (7) data concerning vulnerable data subjects, (8) innovative use or new technological or organizational solutions, and (9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

We respectfully suggest that the Agency's adoption of a similar approach entailing the application of so many different factors will result in an overly nebulous and at any rate unhelpful analysis that will create more problems than it solves.

The Guidelines stipulate that "[i]n most cases, a data controller can consider that a processing meeting two criteria would require a data protection impact assessment (DPIA) to be carried out," and that "[i]n some cases," a single criteria will be sufficient. It is not clear, however, how much weight should be given to each criteria, or whether there are any meaningful thresholds for individual criteria. Is the processing of a hundred records of sensitive data enough to qualify under criteria #4? A thousand? Ten thousand? How many data sets have to be matched or combined to trigger criteria #6? How much data concerning vulnerable data subjects is sufficient under criteria #7? These are the types of questions the Guidelines do not answer.

While the Guidelines do include some "examples of processing" purporting to illustrate the application of possible relevant criteria, these examples do not make the analysis any clearer. Accordingly, we strongly urge the Agency to implement clearer, more concise standards for what constitutes "significant risk" so that businesses have more meaningful guidance about whether they are subject to the cybersecurity audit and risk assessment requirements.

2. Limit the cybersecurity audit and risk assessment requirements to firms that meet one of the first two prongs of the CCPA's "business" definition.

On pages 4 and 8 of the Agency's invitation for comments, the Agency asks "What else should the Agency consider to define the scope of cybersecurity audits?" and "What else should the Agency consider in drafting its regulations for risk assessments?"

As the Agency is aware, there are three different ways for an organization to be defined as a "business" under CCPA: (1) annual gross revenues in excess of $25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms like this who are subject to CCPA solely on the basis of this third prong should be exempt from costly cybersecurity audits and risk assessments.

To comply with these requirements, small businesses will likely have to hire outside expertise and expend considerable expense relative to the size of their enterprise. Because the cybersecurity audits and risk assessments are already premised on processing that presents a "significant risk" to consumers' privacy or security, we believe limiting these requirements as we propose would allow the Agency to balance the interests of small businesses without hampering the opt-out right of California consumers.

Alternatively, the Agency could limit the cybersecurity audit and risk assessment requirements based on smaller limits than those in the CCPA's "business" definition (e.g., firms that do $15 million in revenue

or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

3. Limit processing which presents a "significant risk" to processing which occurs on a regular basis or a minimum number of times per year

In addition to limiting "significant risk" scenarios as described above, the Agency could also clarify that such processing must occur on a regular basis, or at least with some minimal frequency, to trigger the auditing and risk assessment requirements. It does not meaningfully further the spirit of the CCPA, and imposes particularly unnecessary burdens on small businesses, to require an audit and security assessment solely on the basis of one, two, or a handful of isolated instances of processing deemed to present a "significant risk" in a given year.

4. Limit processing which presents a "significant risk" to processing of at least 100,000 records

Alternatively, we suggest the Agency could incorporate some numerical trigger into what constitutes "significant risk" processing. For example, this number could track the figure in the CCPA's "business" definition of 100,000 records, or the Agency could select some lower number. In any case, the underlying statutory language of the CCPA counsels in favor of some such numerical limit. The statute contemplates "significant risk to consumers' privacy or security," language which connotes larger concerns of aggregate risk, not every isolated presentation of risk to any individual consumer or small group of consumers.

Conclusion

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

Again, we appreciate the opportunity to comment.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association