Capitol Matrix Consulting
Analysis, Advice, Advocacy

Date: November 1, 2024

To: California Chamber of Commerce

From: Michael Genest
Brad Williams
Capitol Matrix Consulting

Subject: Comments on August 2024 CPPA SRIA

This memo is in response to your request that we review and provide to you our comments on the California Privacy Protection Agency's (CPPA) Standardized Regulatory Impact Assessment (SRIA), dated August 2024, of its proposed regulations to implement the California Consumer Privacy Act of 2018.

Key Findings

The regulation is likely to result in a substantial net loss to businesses, consumers and governments in this state, both in the near term and the long term. The SRIA's conclusion that savings from the regulation will eventually exceed its cost by a large margin is incorrect because it:

Understates the cost by:

- Underestimating external auditor and employee compensation rates;
- Excluding out-of-state businesses that sell into California markets from its economic analysis; and,
- Ignoring the massive ongoing costs and business productivity losses that would be certain to occur as a result of the regulations.

Overstates the savings by:

- Grossly overestimating baseline cybercrime losses due to an arithmetical error and other factors; and
- Overestimating savings from audits and risk assessments based on assumptions not supported by the literature.

Background

The proposed regulations would make numerous additions and changes to existing regulations related to the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). Specifically, the proposed regulations would:

- Update existing CPPA regulations.
- Clarify when insurance companies are subject to the CPPA regulations.
- Require businesses meeting specified criteria to complete annual cybersecurity audits (CSA).
- Require businesses to prepare a risk assessment (RA) prior to processing personal information for certain activities.
- Require businesses using automated decision-making technology (ADMT) to give consumers newly created rights (well beyond the scope of regulations to implement the CCPA) to opt out, and to give consumers information about how the ADMT will be used.

The SRIA concludes that the regulations would result in direct costs to California businesses of $3.5 billion in the first full year and average annual costs to businesses over the first ten years of $1.08 billion. It estimates direct benefits to California businesses and consumers of $1.58 billion in the first year, rising to $66.3 billion in 2036 due to reduced risk of cybercrimes.

The SRIA then inputs these estimated costs and savings into its economic model to calculate the broader impacts of the regulation on California employment, investment, gross domestic product, and government revenues. It concludes that the regulation will result in employment losses in early years, peaking at 126,000 in 2030, but employment gains in later years, reaching 241,000 by 2036. Similarly, it estimates annual state revenue losses peaking at $2.8 billion in 2028 but then turning positive in later years, reaching an increase over the "baseline" of $4.3 billion by 2036. In addition, the SRIA discusses unquantifiable benefits, which are characterized as "the vast majority of expected benefits."[1]

Our review finds that the SRIA substantially understates the costs and dramatically overstates the benefits of the proposed regulation. We discuss each of these findings in more detail below.

The SRIA's Understated Cost Estimates

The SRIA's $3.5 billion first-year cost estimates consist of $2.1 billion for its cybersecurity audit requirement, $0.8 billion for the ADMT pre-notification and opt-out provisions, $0.4 billion for the updated regulations, and $0.2 billion for the RA provisions. The costs in each category are solely related to employee wages and payments to contractors for programming websites, performing audits as well as other clerical and administrative tasks. The estimated costs to businesses *do not* include effects arising from actions taken by consumers or businesses in response to the regulation (discussed below).

[1] See page 9 of the Standardized Regulatory Impact Assessment: California Privacy Protection Agency.

Our Assessment

We believe that the SRIA's cost estimates are seriously understated for three main reasons:

Estimated number of businesses affected is too low. This is because the estimate, which is 52,326 covered by the proposed regulation, includes only businesses with employees in California.[2] They do not include the tens of thousands of out-of-state companies that sell into California markets. We estimate that inclusion of these businesses would raise first-year costs by potentially several billions of dollars.

The SRIA's authors acknowledge the proposed regulation's impact on out-of-state companies, but they ignore them in their cost impacts because they are not "California businesses." However, the costs imposed on out-of-state companies are relevant from the perspective of the regulation's impact on jobs and investment in California (both of which are required elements of the SRIA). Out-of-state businesses facing costly audits, ADMT opt-out provisions, and risk assessment requirements will face pressures to withdraw from California markets to avoid these costs. The withdrawal will leave consumers with fewer choices, less competition and higher prices for the goods and services they purchase over the internet.

Assumed compensation rates are too low. The SRIA's hourly rates for programming, administration, and internal audits are based on the Occupational Employment and Wage Statistics data from the Employment Development Department. While this is a reasonable approach for estimating wage rates, the estimates fail to include non-wage compensation such as employer payments for FICA, health, dental, unemployment insurance, disability insurance and pensions. The estimates also do not include supplemental over-time pay, which may be significant for companies trying to meet the additional requirements with existing staff. Combined, these expenses add 30 percent or more to the hourly wage rate. The contractor rates used (e.g., $150 per hour for an external cybersecurity audit for a company with annual sales of between $100 million and $1 billion) also appear low to us in view of recent increases in accounting rates. A 30-percent increase in compensation rates would raise the SRIA's cost estimate by over $1 billion.

The focus of the SRIA is too narrow. As significant as they are, the costs for programming, cybersecurity audits and risk assessments are only the tip of the iceberg when considering the full impact of these regulations. The primary impacts of the proposed regulations are related to their ongoing effects on business operation costs and productivity, which are admittedly more difficult to precisely quantify but are crucially important to understanding the regulation's full impacts.

This is particularly important with respect to the ADMT provisions, which have far-reaching implications. As noted earlier, the provisions require a business meeting certain thresholds to provide pre-use notices to consumers, informing them about the business's use of ADMT, and to create a new right for consumers to opt-out of the use of ADMT (subject to certain exceptions). They also allow consumers to access information about how the business used ADMT with respect to that consumer.

[2] Specifically, the CPPA applies to California businesses that (1) had revenues of more than $27,950,000.00 in the preceding calendar year, or (2) buy, sell, or share the personal information of 100,000 or more consumers or households per year, or (3) receive 50% or more of their annual revenue from selling or sharing personal information.

While the cost estimate does include up-front programming expenses for adding opt-out and related information to company websites, it does not include the much larger ongoing costs that will follow, such as:

- Added costs for intake and response to ADMT opt-out requests from consumers, as well as costs for forwarding the request to the appropriate team to administer the relevant non-automated process.

- The creation and administration of a non-automated process for each ADMT-covered decision.[3]

- The time and expense involved in responding to consumer inquiries about the purpose for which the business is using ADMT, the output of the ADMT with respect to the consumer, and how the output was used to make a decision with respect to the consumer.

- Costs to businesses of redesigning of consumer e-commerce platforms needed to accommodate consumers that opt-out of ADMT.

- Costs related to negative impact of consumer and employee opt-outs on the reliability of ADMT systems.[4]

- Other costs to businesses, including, for example, impacts arising from the suppression of behavioral ads. The proposed regulations would extend opt out rights to first-party behavioral ads,[5] which will reduce income of online publishers and raise costs for businesses to advertise to new consumers. These provisions could have substantial impacts on small businesses seeking to grow through targeted advertising campaigns.

More generally, the SRIA fails to address a key requirement set forth in California statutes for SRIAs – that they evaluate the impact of proposed regulations on "the incentives for innovation in products, materials, or processes."[6] The lack of commentary in this area is of special concern given the enormous impacts that ADMT and related AI technologies are expected to have on the global economy over the next decade. According to a recent study by Goldman Sachs, artificial intelligence could drive a 7-percent increase in global GDP and lift annual labor productivity growth by 1.5 percentage points over a 10-year period.[7] A 7- percent increase in California GDP would translate into an additional annual GDP of $400 billion by 2036. Policies that stifle even a small fraction of ADMT adoption and utilization would have impacts ranging into the tens of billions per year – amounts that would dwarf actual savings from the proposed regulations once they are adjusted for arithmetical errors and other factors (see discussion on the SRIA's savings estimates below).

The SRIA's cost estimate also does not include negative impacts that the RA- and ADMT-related provisions could have on promising research in areas such as science, health care, transportation or

[3] A single business may have multiple automated processes that are affected by the requirement. Examples include automated human resources processes for internal employees for predictive scheduling; marketing tools aimed at specific consumers, and use of ADMT for determining pricing of their products and services.
[4] The effects on reliability could be substantial if employees or consumers exercising opt-outs had undetected attributes different from the overall population of interest, thereby skewing results.
[5] First-party behavioral ads" refer to targeted advertisements by a company, delivered to users based on their actions and interactions with the company's website or other platforms, using data collected directly from that user.
[6] Government Code Section 11346.3(c).
[7] Goldman Sachs, "Generative AI Could Raise Global GDP by 7%." April 5, 2023.
https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent

climate protection. The cost-benefit calculations required before determining whether a project can move forward could thwart promising research in cases where the potential benefit from a research project may be highly uncertain and difficult to quantify (as is the case in immunotherapy and pharmaceutical research), while the risks of a data breach, though small, are quantifiable.

The SRIA acknowledges potential costs from projects not moving forward because of the RA provisions, but it asserts that the great majority of these costs should be attributed to the existing baseline because such consumer protections and requirements are implicitly required under existing federal and state law. In other words, when it is evaluating costs of the RA regulations, the SRIA claims that the regulations will result in virtually zero changes in business behavior (which raises the question of why the duplicative and complicated regulation is even being proposed in the first place). But when evaluating benefits, the SRIA contradicts their own analysis in the cost section by attributing an enormous amount of savings to the changes required by the RA and cybersecurity audits.

Lastly, the SRIA fails to include costs associated with the impacts of the regulations on out-of-state businesses, which would incur 100 percent of the costs imposed by the regulation, even though California may be only a relatively small part of their market. The questions needed to be addressed include (1) how many would withdraw from California markets to avoid these costs; and (2) what would be the costs to California consumers from business withdrawals from California markets in terms of losses of product choices, reduced competition and higher prices.

The combined impact of the factors not covered by the SRIA could easily add billions of dollars to business costs in the near term, and even more over the longer term due to the stifling impacts of the regulation on innovation, productivity, and economic growth. We acknowledge that it would be difficult to precisely quantify each of the impacts cited above. However, by downplaying or ignoring them altogether, the SRIA is omitting the largest impacts of the regulation. Combined with the underestimates of the direct costs that it did recognize, the exclusion of these ongoing impacts on business costs and productivity result in a major underestimate of the true cost of the proposed regulation.

The SRIA's Overstated Savings Estimates

Our review of the SRIA's savings estimate has identified several major issues, which taken together make the estimated savings entirely unreliable.

Arithmetical error when calculating cybercrime losses under the baseline. The first issue consists of a straightforward calculation error. The SRIA extrapolates historical increases in cybercrime losses to develop a "baseline estimate" of cybercrime-related business losses out to 2036. These projected "baseline" losses are then combined with an assumption about the *percentage reduction* in cybercrime that will result from the proposed regulation to arrive at a projected dollar amount of savings that will result from the regulation. The problem is that the SRIA dramatically overestimated the projected baseline increases due to an arithmetical error. This resulted in a comparable over-estimate of dollar savings that would result from the regulation.

The arithmetical error involves how the SRIA calculates the average annual percentage growth rate in cybercrime losses. Specifically, it uses a simple average (mean) of the annual growth rates

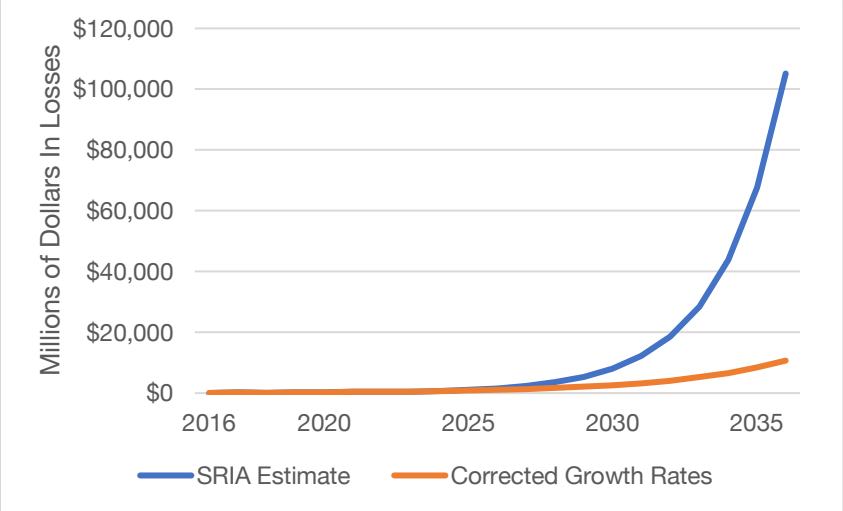
instead of the correct, geometric, average rate which accounts for compounding.[8] When we correct for the error, we get growth rates for cybercrime losses to California businesses that are only a fraction of those used in the SRIA, as shown in Figure 1.

Figure 1
Growth Rates in Monetary Losses from Cybercrimes
SRIA Calculations vs CMC Calculations

	Business Email Compromise	Corporate Data Breach	Identity Theft	SIM Swap	Ransomware	Botnet	Malware
SRIA (simple average)	44.77%	66.11%	-0.13%	19.00%	10.81%	-0.07%	-11.95%
CMC (geometric average)	24.29%	30.04%	-0.15%	19.00%	9.31%	-0.08%	-36.01%

When we apply the corrected growth rates in each area, we likewise get a substantially lower estimate of future year cybercrime losses. Specifically, using the corrected rates of growth yields an estimated loss to California businesses in 2036 of $9.2 billion compared to the $105.2 billion stated in the SRIA (see Figure 2), a reduction of over 90 percent.

Figure 2
Projected Baseline Growth in Business Losses from Cybercrimes



[8] The SRIA uses the method of first calculating the overall percentage increase in cybercrime losses between 2016 and 2023 and then dividing that by the number of years. The correct way to compute average annual growth rates is to take the Nth *root* of the overall percentage increase, where N is the number of years of growth. This is more than a technical concern because, while the SRIA uses a simple average for calculating the historical growth rate, it extrapolates the cybercrime losses into the future using compounding. This inconsistency results in a vast overestimate of future baseline losses. The SRIA Includes another error in that it uses the total number of years (i.e., 8) as the denominator in its calculations, when, in fact, in the sample of 8 years, there are only 7 years of growth (the first year being year 0, the second year being the first year of growth, etc.). We also corrected for this error, which goes in the opposite direction (i.e., it reduces the estimate of annual average increase) but has much less impact on the estimate than the failure to use a geometric average.

Other problems with the SRIA's baseline. Aside from the arithmetical error, the basic approach used in the SRIA to extrapolate future cybercrime losses under the baseline is flawed for two other reasons. First, the historical period it uses to extrapolate historical losses into the future begins in 2016. This is two years before the European Union's General Data Protection Regulation (GDPR) came into effect in May 2018, and four years before the California Consumer Privacy Act (CCPA), came into effect in January 2020. As a result, the extrapolation is based on loss-trends that were established before existing regulations were put in place, and thus it is not reflective of a true current-law baseline. At a minimum the SRIA should include a discussion about how these regulations have impacted the baseline.

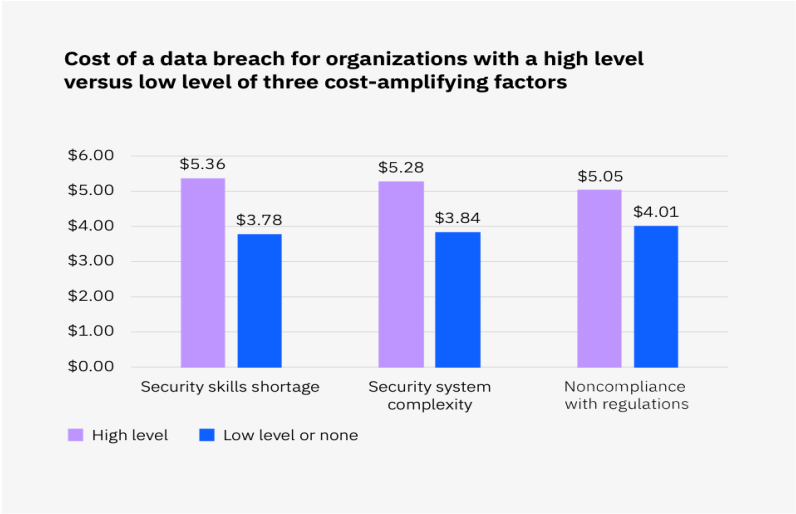
Second, the baseline fails to consider how soaring business losses from data breaches would affect business behavior absent any new regulations. The implied level of cybercrime losses under the SRIA's baseline would be $523 billion annually by 2036. To provide some perspective, a loss of this magnitude would be roughly equal to the current GDP of California's enormous business and professional services sector, 25 percent larger than its manufacturing sector, and more than double its retail trade sector. Quite simply, businesses would not be able to survive these levels of losses, and they would have enormous incentives to control cybercrime – with or without these regulations. Yet, the savings estimate is based on the premise that businesses would simply watch loss grow to these enormous levels and do nothing about them.[9]

Adjustment for unreported cybercrime unsupported by the data. The SRIA then assumes that their estimated losses represent only 20 percent of the total monetary value of cybercrime losses. This assumption is based on an FBI study that found that only 20 percent of ransomware crimes are reported. Yet, ransomware is only one of the seven types of cybercrime considered in the SRIA and the total losses from it make up only 1 percent of the total losses in 2023. In addition, the 20-percent figure reflects crimes reported, not the dollar value of those crimes. This would be an important distinction if, as we suspect, the majority of unreported crimes are of low value.[10] We conclude that the large multiplier used by the authors of the SRIA is highly questionable, and likely overstates the dollar value of unreported cybercrimes.

Unsupported savings rate assumption. The SRIA asserts that the proposed regulations would reduce cybercrime losses by 12.6 percent. According to the SRIA, "this is based on the 2023 IBM Data Breach Report."[11] However, the IBM report develops this savings estimate by comparing organizations with respect to three categories of "cost-amplifying" factors" – namely, security skills shortage, security system complexity, and noncompliance with regulations (see Figure 3, next page, which is reproduced directly from the IBM report).

[9] In addition to the obvious and growing financial and reputational incentives for firms to reduce cybercrime, there are significant incentives for firms to avoid lawsuits under California law, which creates a private right of action that allows victims of data breaches to sue companies for failing to adopt adequate security measures. Cal. Civ. Code § 1798.150.
[10] We also note that the tendency for victim underreporting may be greater for ransomware than other cybercrimes. This is because the FBI strongly discourages ransom payments, whereas some companies may find it is in their financial interest to pay the ransom and move on.
[11] Cost of a Data Breach, 2023. IBM https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf

Figure 3
Impact of Key Factors on the Cost of a Data Breach
(From "Cost of a Data Breach, 2023," IBM)
($ Millions)



There is no clear relationship between these three categories and the proposed regulations. Specifically, the regulations do not address security staffing or training in any direct way, nor do they mandate simpler security systems. Finally, it is obvious that enacting more regulations does not in any sense create more regulatory compliance with existing regulations.

In defense of this assumption, the SRIA states that "Steinbart et al (2018) is an empirical study finding a relationship between CSAs (Cybersecurity Audits) and actual cybersecurity outcomes."[12] However, our review finds that study does not directly measure impacts of cybersecurity audit quality on company outcomes. Rather, its focus is on the impact on information security outcomes of (1) the relationship between internal audit and information security divisions of companies; and (2) the level of top management support for information security on information security outcomes. In fact, the study acknowledges that one of its key limitations is that "we were not able to collect information about various measures of internal audit quality, such as auditor independence, qualifications, knowledge, and skills." Another study included in the SRIA's bibliography (Slapnicar et al, 2022) found no evidence that strong cybersecurity auditing processes resulted in fewer successful cyberattacks.[13]

The SRIA contains a bibliography listing 59 articles. Our review found that only two of the articles listed report on the relationship between any of the concepts addressed in the proposed regulation and a potential to reduce successful cybercrime attacks. Those two are the ones mentioned above (Steinbart and Slapnicar), both of which contradict the assertions made in the SRIA. We also conducted several internet searches in an attempt to find other academic articles that might support the effectiveness of the proposed regulations. We found none.

[12] P. Steinart, R. Raschke, G Gal, and W. Dilla, "The Influence of a Good Relationship Between the Internal Audit and Information Security Functions on Information Security Outcomes." Elsevier. April 2018.
[13] S. Slapnicaar, T Vuko, M Drascek, "Effectiveness of Cybersecurity Audit. Elsevier. March 2022.

Conclusion regarding savings estimate. We conclude that the savings estimates presented in the SRIA are not reliable and are grossly overstated. For example, the SRIA estimates that the regulations will result in savings of $66.3 billion in 2036, the final year of its projections. If we simply correct for the arithmetical error in estimating baseline future losses and accept – for a moment – both the SRIA's assumption of a 12.6-percent savings rate and that reported losses reflect only 20 percent of the total losses, we get an estimate of 2036 savings of only $6.7 billion – or about 11 percent of the SRIA's estimate. Given the lack of support in the literature for the 12.6-percent savings estimate used by the SRIA and the uncertainties regarding SRIA's assertion that reported losses for cybercrimes are only 20-percent, actual savings may well be only a fraction of the $6.7 billion. In fact, there is no reason, based on the available literature to date, to have confidence that the specific regulation will create any savings at all.

SRIA's Impacts on California Jobs and State Revenues

The SRIA's underestimate of costs and overestimate of benefits has major implications for its estimates of the proposed regulation's impact on California jobs and government revenues. The higher direct costs we identify would translate into reductions in jobs and revenues that are at least double the SRIA estimates. Just as importantly, it is highly unlikely that the longer-term net economic gains claimed in the SRIA will occur. This is because (1) many of costs not identified in the SRIA are ongoing (e.g., the regulation's stifling effects on innovation and ongoing costs and productivity losses resulting from opt-outs); and (2) the SRIA's estimates of cybercrime reductions due to the regulation are entirely unreliable. Contrary to the SRIA's assertion, the near-term negative impact of the regulation on the economy and state government revenues will likely grow in the future.

Summary and Conclusion

The SRIA understates the cost of the proposed regulation by underestimating external auditor and employee compensation rates paid by businesses; excluding out-of-state businesses that sell into California markets; and, most importantly, ignoring the massive costs resulting from behavioral changes by consumers and businesses following adoption of the regulation. Its savings estimate is based on a baseline that dramatically overstates cybercrime losses that would occur under current law. It also assumes substantial savings from audits and risk assessments that are not supported by the literature. We conclude that the regulation is much more likely to result in a net loss to businesses, consumers and governments in this state.