California Privacy Protection Agency

Standardized Regulatory Impact Assessment: California Privacy Protection Agency

October 2024

Prepared by:

Berkeley Economic Advising and Research

Drew Behnke, PhD
Jonathan Chang, MPP
Safa Faki, MPP
Samuel Neal, PhD
David Roland-Holst, PhD

California State University, Sacramento

Raul Tadle, PhD
Yan Zhou, PhD

For more information, please contact the California Privacy Protection Agency at pierre.du.vair@cppa.ca.gov or (916) 471-0754.

ACKNOWLEDGEMENTS

We would like to thank the Chief Economist of the California Department of Finance and her staff in the Economics Research and Major Regulations Unit for providing comments and insights in support of preparing this SRIA. Any errors implementing their inputs are the sole responsibility of the authors.

The authors and the California Privacy Protection Agency would also like to thank all of the individuals and organizations that shared their time, information, insights, and expertise to assist with the preparation of this SRIA. Your efforts are very much appreciated.

ADA COMPLIANCE

This document has been screened and modified to be compliant with the current ADA standard for Microsoft Word documents. In addition to this, a complementary support file has been provided online, making all tables and figures in this document available for use with companion readers and a variety of visual enhancement technologies. The master ADA support file can be downloaded here:

https://bearecon.com/Tools/CPPA_SRIA_ADA_Tables and Figures_BEAR 110624.xlsx

Table of Contents

Abbreviations

ADMT – Automated Decisionmaking Technology
AG – Attorney General of California
Agency – California Privacy Protection Agency
AI – Artificial Intelligence
BEA – Bureau of Economic Analysis
BEAR – Berkeley Economic Advising and Research
BEC – Business Email Compromise
CCPA – California Consumer Privacy Act of 2018
CGE – Computable General Equilibrium
CIS – Center for Internet Security
CPRA – California Privacy Rights Act of 2020
CSA – Cybersecurity Audit
DDoS – Distributed Denial-of-Service
DOF – California Department of Finance
DOJ – California Department of Justice
EDD – California Employment Development Department
EIN – Employer Identification Number
FBI – Federal Bureau of Investigation
FTE – Full-Time Equivalent
FY – Fiscal Year
GAMS – General Algebraic Modeling System
GDPR – General Data Protection Regulation
GenAI – Generative Artificial Intelligence
GDP – Gross Domestic Product
GSP – Gross State Product
HIPAA – Health Insurance Portability and Accountability Act
IBM – International Business Machines
IC3 – Internet Crime Complaint Center
IEC – International Electrotechnical Commission
IMPLAN – Impact Analysis for Planning
ISO – International Organization for Standardization
LVA – Labor Value Added
NAICS – North American Industry Classification System
NIST CSF – National Institute of Standards and Technology Cybersecurity Framework
OEWS – Occupational Employment and Wage Statistics

OOPS – Opt-Out Preference Signal
PI – Personal Information
RA – Risk Assessment
RTC – Right to Correct
RTK – Right to Know
RTL – Right to Limit
RTOO – Right to Opt-Out of Sale/Sharing
SAM – Social Accounting Matrix
SIM – Subscriber Identity Module
SOC 2 – System and Organization Controls 2
SPI – Sensitive Personal Information
SUSB – Statistics of U.S. Businesses
SRIA – Standardized Regulatory Impact Assessment
URL – Uniform Resource Locator

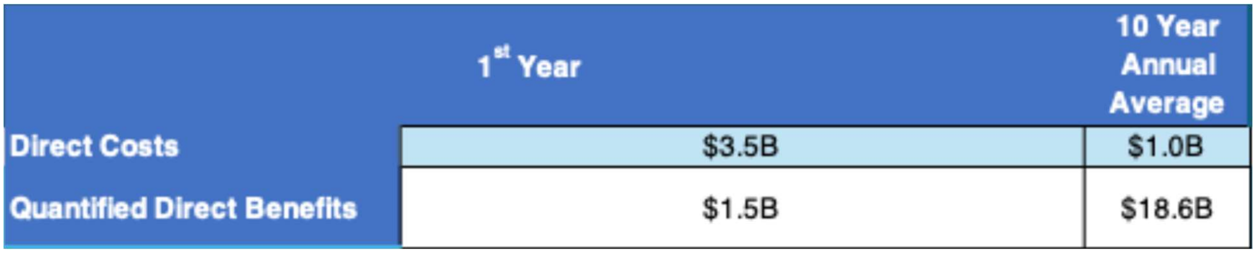
Executive Summary

The California Privacy Protection Agency ("Agency") was established to implement and enforce the California Consumer Privacy Act of 2018 ("CCPA"). The Agency is directed to adopt regulations to further the purposes of the CCPA, including 21 specific topics. The proposed regulations address the following: (1) updates to existing CCPA regulations; (2) clarify when insurance companies must comply with the CCPA; (3) establish requirements to complete a cybersecurity audit ("CSA"); (4) establish requirements to prepare a risk assessment ("RA"); and (5) operationalize consumers' rights to access and to opt-out of businesses' use of automated decisionmaking technology ("ADMT").

Direct Costs & Benefits

The Agency anticipates that the proposed regulations will generate direct costs to businesses and direct benefits to businesses and consumers. Direct costs include those costs incurred by businesses to come into compliance with new requirements and are primarily comprised of labor costs. Covered businesses are expected to strengthen their protection of consumer personal information ("PI") as well as more effectively enable consumers to exercise their privacy rights thereby generating direct benefits to businesses and consumers. The vast majority of expected benefits from the proposed regulations cannot be quantified, so this Standardized Regulatory Impact Assessment ("SRIA") contains an extensive discussion of unquantified benefits expected to accrue to both businesses and individuals. Some of these unquantified or qualitative benefits include improvements to the health, safety, welfare, and quality of life for California individuals. Direct benefits to California businesses estimated in this SRIA focus on reduced risk of cybercrimes. Total direct costs and quantified direct benefits are summarized below in Table ES-1.

Table ES-1: Summary of Estimated Direct Costs and Benefits of Proposed Regulations



	1st Year	10 Year Annual Average
Direct Costs	$3.5B	$1.0B
Quantified Direct Benefits	$1.5B	$18.6B

Note: All figures in 2022 $

Fiscal Impacts

This proposed rulemaking package contains multiple requirements for California businesses that will create a new workload for staff at the Agency. New workload results from implementation of proposed regulations and can be separated into two categories:

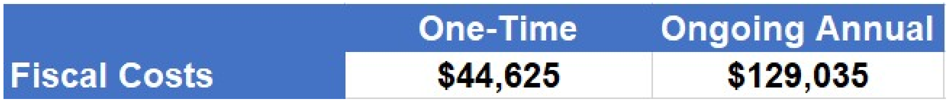
1) one-time staff work to build the frameworks necessary to receive multiple required documents from more than 52,000 California businesses and letters of complaint from an uncertain number of California consumers; and 2) ongoing staff workload to review submitted documents and respond to submittals on a case-by-case basis.

The proposed regulations require covered California businesses to submit documents to the Agency. The frequency of document submittals will be annual or intermittently, when businesses have a material change that requires a revision or addition to their existing document submissions.

The Agency's Information Technology Division will need to develop web portals to accept the documents referenced above. The Agency estimates this would require a one-time fiscal impact of $44,625. We estimate the fiscal impact of this ongoing workload scenario to be 50 percent time of an Associate Governmental Program Analyst, at an annual cost of $63,000. We estimate addressing consumer complaint letters will require an ongoing fiscal impact of $66,035.

Based on these additional workloads, total fiscal impacts are shown in Table ES-2.

Table ES-2: Summary of Fiscal Impacts



	One-Time	Ongoing Annual
Fiscal Costs	$44,625	$129,035

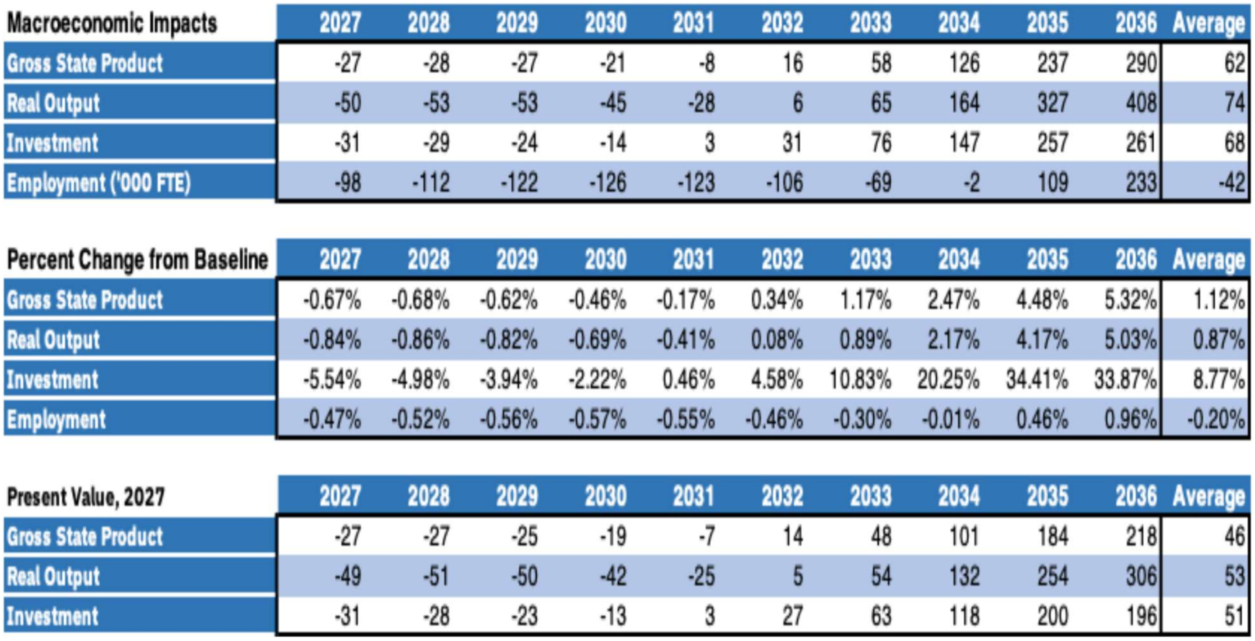
Note: All figures in 2024 $

California Economywide Impacts

The economy-wide impacts of the Agency's proposed regulations have been evaluated using the BEAR forecasting model. The BEAR Model is a dynamic computable general equilibrium ("CGE") model of the California economy. The Model simulates detailed patterns of demand, supply, and resource allocation across the state, estimating economic outcomes over the period 2027-2036.

The salient feature of the proposed regulations is a reversing trend in economic growth, from net reductions to net increases with respect to the Baseline. This can be seen as a lagged response to the reversal of net direct costs from positive to negative. Simply put, the proposed regulations have high upfront costs, but low ongoing costs, and this shows up in early years as a net cost to the economy. The benefits of stronger protections for consumers' privacy far outweigh these costs in the long run, improving the investment climate and overcoming cumulative adjustment costs incurred by California businesses required to comply with the proposed regulations, their workers, and their supply chain partners. The driver of the investment reversal in these results is enhanced private net income and savings from reductions in cybercrimes. If we could include such behavioral adaptations and direct beneficial qualitative impacts, the macroeconomic benefits would be far more dramatic.

Table ES-3: Estimated Macroeconomic Impacts



Macroeconomic Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-28	-27	-21	-8	16	58	126	237	290	62
Real Output	-50	-53	-53	-45	-28	6	65	164	327	408	74
Investment	-31	-29	-24	-14	3	31	76	147	257	261	68
Employment ('000 FTE)	-98	-112	-122	-126	-123	-106	-69	-2	109	233	-42

Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-0.67%	-0.68%	-0.62%	-0.46%	-0.17%	0.34%	1.17%	2.47%	4.48%	5.32%	1.12%
Real Output	-0.84%	-0.86%	-0.82%	-0.69%	-0.41%	0.08%	0.89%	2.17%	4.17%	5.03%	0.87%
Investment	-5.54%	-4.98%	-3.94%	-2.22%	0.46%	4.58%	10.83%	20.25%	34.41%	33.87%	8.77%
Employment	-0.47%	-0.52%	-0.56%	-0.57%	-0.55%	-0.46%	-0.30%	-0.01%	0.46%	0.96%	-0.20%

Present Value, 2027	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-27	-25	-19	-7	14	48	101	184	218	46
Real Output	-49	-51	-50	-42	-25	5	54	132	254	306	53
Investment	-31	-28	-23	-13	3	27	63	118	200	196	51

Notes: All figures in 2022 $ billions. Employment in full-time equivalent (FTE) thousands.

This direct impact is composed of a $3.5 billion direct cost to businesses subject to the CCPA, resulting in a much larger adverse impact on investment (-$31 billion) because it directly impacts cost and profit margins. The investment shortfall reduces current output (-$50 billion), employment (-98,000 FTE), and gross state product or GSP (-$27 billion). From this point, the trend moderates and then reverses as the limited set of quantified benefits consistently exceed costs. Note that the first year of compliance is by far the most adverse shock; incremental costs after that are modest in the next few years until the quantified direct benefits of proposed regulations overcomes them and becomes growth positive for the California economy.

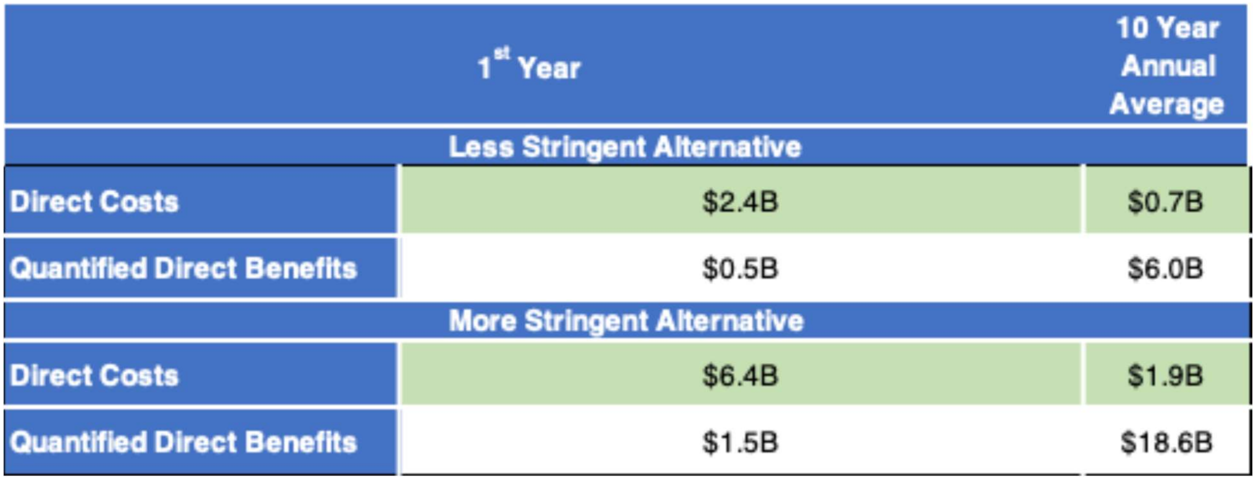
In terms of economywide impacts, three salient findings deserve emphasis. First, when net direct costs are positive, the regulation is understandably adverse to Baseline or "Business as Usual" economic activity in California's PI dependent sectors. This translates to lower profit, investment, output, and employment for established enterprises and allied activities. Second, cumulative impacts are much stronger than direct ones because the investment is reacting to the marginal change in profit, which is initially much higher than the marginal revenue effect. Finally, despite the investment shock combined direct, indirect, and induced effects are still a small percentage of California Baseline levels.

Alternative Regulatory Scenarios

In addition to the Baseline and proposed regulations, the Agency considered a package of less stringent and more stringent alternatives. The less stringent alternatives would reduce the number of covered California businesses for CSA, RA, and ADMT requirements, while the more stringent alternative would increase both coverage and extend additional compliance requirements.

Direct costs of the less stringent package are estimated to be approximately 31% lower than the proposed regulations, while direct costs of the more stringent package are estimated to be 83% more than the costs of proposed regulations.

Table ES-4: Direct Costs and Benefits Under Regulatory Alternative



	1st Year	10 Year Annual Average
	Less Stringent Alternative	
Direct Costs	$2.4B	$0.7B
Quantified Direct Benefits	$0.5B	$6.0B
	More Stringent Alternative	
Direct Costs	$6.4B	$1.9B
Quantified Direct Benefits	$1.5B	$18.6B

Note: All figures in 2022 $

Economywide comparisons of the more and less stringent alternatives suggest that the proposed regulations strike a good balance between the desire to strengthen consumer privacy and recognition of the importance of the information technology sector to the statewide economy. As PI protective practices and technologies proliferate, this adaptation can help reconcile higher levels of security and economic opportunity.

1 Introduction

In November 2020, voters approved the California Privacy Rights Act of 2020 (“CPRA“), amending and building on the California Consumer Privacy Act of 2018 (“CCPA”). The CPRA established a new agency, the California Privacy Protection Agency (“Agency”), to implement and enforce the CCPA. (Civ. Code, § 1798.199.10.) The Agency is directed to adopt regulations to further the purposes of the Act, including promulgating regulations on 21 specific topics. (Civ. Code § 1798.185.) The proposed regulations do the following things: (1) update existing CCPA regulations; (2) clarify when insurance companies must comply with the CCPA; (3) operationalize requirements to complete an annual cybersecurity audit (“CSA”); (4) operationalize requirements to conduct a risk assessment (“RA”); and (5) operationalize consumers’ rights to access and to opt-out of businesses’ use of automated decisionmaking technology (“ADMT”).

This document provides an economic impact assessment of the costs and benefits of the proposed regulations and the regulatory alternatives. The methodological approach is in compliance with Department of Finance (“DOF”) baseline calibration standards. All data are from the latest available official and industry sources except where otherwise noted.

1.1 Background and Summary of Proposed Regulations

As noted above, the proposed regulations do the following things: (1) update existing CCPA regulations; (2) clarify when insurance companies must comply with the CCPA; (3) operationalize requirements to complete a CSA; (4) operationalize requirements to conduct an RA; and (5) operationalize consumers’ rights to access and to opt-out of businesses’ use of ADMT.

For the CSA and RA requirements, respectively, a business subject to them has 24 months from the effective date of these regulations to complete its first cybersecurity audit and to submit its first risk-assessment materials to the Agency. The proposed regulations will be fully implemented two years after the effective date.

More specifically, the proposed regulations:

1. **Update Regulations:** Update existing CCPA regulations to improve the ease by which consumers can access information about their CCPA rights and exercise those rights. They also clarify for businesses their obligations regarding what information they must provide regarding their information practices, how to offer methods for submitting CCPA rights, and how they are to process requests from consumers exercising those rights. (Civ. Code § 1798.185, subd. (a).)

   More specifically, the proposed regulations: (1) add an additional category to the definition of sensitive personal information (“SPI”); (2) provide more guidance regarding how to design and implement methods for submitting CCPA requests and obtaining consent; (3) update rules and procedures for submitting requests to know, requests to opt-out of sale/sharing, and requests to limit; (4) clarify requirements for the processing of requests to delete and requests to correct; (5) update rules and procedures for denying CCPA requests, including informing consumers of their ability to submit a complaint with the Agency and Attorney General's ("AG") office, and their ability to require businesses to note internally and with those they sell or share PI that they contest its accuracy; and (6) require businesses to display the status of the consumer's choice regarding the sale and sharing of their PI, and the use of their SPI.

2. **Insurance:** Clarify the circumstances under which insurance companies are to comply with the CCPA. (Civ. Code § 1798.185, subd. (a)(20).)

3. **Cybersecurity Audit**: Establish when businesses are to perform a CSA, the scope of the audit, and the process to ensure that audits are thorough and independent. (Civ. Code § 1798.185, subd. (a)(14)(A).) Specifically, the proposed regulations require businesses that must comply with the CCPA and that meet either of the following two criteria in the preceding calendar year to complete an annual CSA:

   (1) The business made 50% or more of its annual revenue from selling or sharing consumers' PI; or

   (2) The business made over $28 million[1] in annual gross revenue and (A) processed the PI of 250,000 or more consumers or households or (B) processed the SPI of 50,000 or more consumers.

   The proposed regulations require a business to select an auditor, provide all information the auditor asks for and not hide important facts from them, present the audit results to the most senior individuals in the business responsible for its cybersecurity program, and submit a certification of completion to the Agency.

   The proposed regulations also require the auditor to be qualified, unbiased, and independent, and use professional auditing procedures and standards. The auditor can be someone working in the business or outside of the business. If an auditor is internal, they must report to the business's board, governing body, or highest-ranking executive who does not have direct responsibility for the cybersecurity program. Whether working in the business or not, the auditor has to determine which systems need to be audited and how they will be assessed; independently review documents, conduct tests, and interview people to support audit findings; and certify that they completed an independent and unbiased audit.

   The proposed regulations require the audit to include a description of the systems being audited; the information the auditor used to make decisions and why it

[1] Original CCPA figure is $25 million. AB 3286 (July 2024) provides for a two-year look back to adjust for inflation. Based upon recent DIR CPI figures, and in line with the assumption of a 11.8% increase for purposes of this SRIA, the adjusted annual gross revenue threshold is $27,950,000.

supported their findings; an assessment of how the business protected PI through its cybersecurity program (e.g., through multifactor authentication, encryption, account management and access controls, inventorying and managing PI and the business's information system, cybersecurity training, and incident-response); a description of how the business followed its own cybersecurity policies and procedures; a description of the gaps and weaknesses of the cybersecurity program and how the business plans to address them; a description or sample copy of data-breach notifications that were sent to consumers or agencies, and related information and fixes; the dates that the cybersecurity program was reviewed and presented to the most senior individuals in the business responsible for the business's cybersecurity program; and a certification that the business did not influence the auditor's decisions or assessments, and that the business reviewed and understood the audit findings.

The proposed regulations provide that a business would have 24 months to complete its first CSA and submit its certification of completion to the Agency and would then complete its CSA and submit a certification each following year.

Lastly, the proposed regulations clarify that if a business completed a CSA or assessment for another purpose or had a cybersecurity certification, the business would not have to redo the same CSA. However, if the audit, assessment, or certification did not meet all of the requirements in the proposed regulations, the business would have to add to it as needed.

4. **Risk Assessment**: Establish when businesses are to conduct an RA with respect to their processing of PI, what must be included in the RA, the consequence of the RA, and how RAs are to be submitted to the Agency. (Civ. Code § 1798.185, subd. (a)(14)(B).) Specifically, the proposed regulations require businesses that must comply with the CCPA to conduct an RA before it does any of the following:

   (1) Sells or shares consumers' PI;

   (2) Processes consumers' SPI;

   (3) Uses ADMT for a "significant decision" (a decision that has an important consequence for consumers, such as a decision to provide or deny financial services, housing, insurance, educational or employment opportunities, healthcare services, or essential goods or services like groceries, medicine, or fuel) or for "extensive profiling" (includes analyzing consumers' personality, interests, behavior, or location in their workplace, at school, or in public places (e.g., using facial-recognition technology in a store to identify potential shoplifters), or to target ads to them); or

   (4) Uses PI to train ADMT or artificial intelligence ("AI") that could be used to identify people (e.g., facial-recognition technology), for physical or biological identification or profiling (e.g., analyzing people's facial expressions or gestures to infer their emotional state), to make significant decisions, to

generate deepfakes (e.g., fake images of real people that are presented as truthful or authentic), or to operate generative models.

The proposed regulations require RAs to include why the business needs to engage in the processing activity; the types of PI the business would process to engage in the activity; how the business would engage in the activity (e.g., how many consumers would be affected, what the business would tell them about its use of their PI, who else might be involved, which technology it plans to use; and, for certain uses of ADMT, how the business would use the ADMT to make decisions); the benefits (including benefits to the business, consumers, other stakeholders, and the public) and consequences to consumers associated with the activity (e.g., unauthorized access to their PI, discrimination on the basis of protected characteristics (e.g., race or gender), not providing enough information to consumers so that they understand how their PI would be used, or creating additional costs for consumers), and protections the business plans to put in place (e.g., encryption and privacy-enhancing technologies. A business using ADMT for a significant decision or extensive profiling would also have to identify whether it evaluated the ADMT to ensure it worked as intended and did not discriminate, and which accuracy and nondiscrimination safeguards it planned to put in place); the people at the business who contributed to, reviewed, and approved the RA; and whether the business will initiate the activity.

The proposed regulations clarify that a business would not be permitted to engage in an activity if the risks to consumers' privacy outweighed the benefits of the activity.

The proposed regulations clarify that a business would have to conduct an RA before it initiated any of the activities listed above; and would have to review (and update if needed) its RAs at least once every three years to make sure they remained correct. If something important changed about how the business engages in the activity (e.g., if it needed to collect more SPI), the business would have to immediately update its RA.

The proposed regulations also clarify that the business would have 24 months to submit to the Agency: (1) a certification that it conducted its RAs as set forth in the proposed regulations; and (2) abridged RAs (a shorter version of the full RA, which would include the activity that triggered the RA; why the business needed to engage in that activity; the types of PI needed for the activity and whether they included SPI; and the protections put in place). After its first submission, the business would submit its certification and any new or updated abridged RAs annually. Lastly, if the Agency or the AG requests a business's unabridged RA, the business would have 10 business days to provide it.

Finally, the proposed regulations clarify that if a business conducted an RA for the same activity to comply with another law, the business would not have to redo the same RA. However, if the RA did not meet all of the requirements in the proposed regulations, the business would have to add to it as needed.

5. **ADMT**: Govern access and opt-out rights with respect to businesses' use of ADMT. (Civ. Code § 1798.185, subd. (a)(15).) Specifically, the proposed regulations define ADMT and require businesses that must comply with the CCPA and do any of the following to comply with the proposed regulations' ADMT requirements:

   (1) Use ADMT to make a "significant decision" about a consumer;

   (2) Use ADMT for "extensive profiling"; or

   (3) Process PI to train ADMT that could be used to identify people (e.g., facial-recognition technology); for physical or biological identification or profiling (e.g., analyzing people's facial expressions or gestures to infer their emotional state); to make significant decisions; or to generate deepfakes (e.g., fake images of real people that are presented as truthful or authentic) ("training ADMT").

   The proposed regulations require such a business to provide a consumer with a Pre-use Notice about its use of ADMT. The Pre-use Notice has to include why the business wants to use the ADMT; how the ADMT would work, such as the key factors that affect its output and how the business would use the output to make a decision about the consumer; and that the consumer has CCPA rights (to opt-out of ADMT and to access information about the ADMT), how they could exercise them, and that the business cannot retaliate against them for exercising those rights.

   The proposed regulations also require such a business to provide an easy way for the consumer to opt-out of the business's use of ADMT, unless an exception applies. If the consumer does not opt out and chooses to exercise their right to access ADMT, the business must give the consumer an easy way to access information about how the business used the ADMT with respect to the consumer, though this requirement does not apply to a business's use of PI for training ADMT.

   The proposed regulations require a business's response to a consumer's access request to include why the business used the ADMT; how the ADMT worked with respect to that consumer, such as the key factors that affected the ADMT's output, what the output was, and how the business used the output to make a decision about that consumer; how the consumer could exercise their other CCPA rights (e.g., their right to correct inaccurate information); and that the business cannot retaliate against them for exercising their rights.

   When a consumer opts out of ADMT, the proposed regulations prohibit a business from processing consumer's PI using that ADMT. However, the proposed regulations include exceptions to providing opt-outs from ADMT:

(1) If the business uses the ADMT solely for necessary security, fraud prevention, or safety. (This exception would apply only to a business's use of ADMT for two kinds of extensive profiling: work/educational profiling and public profiling);

(2) If the business gives consumers the ability to appeal the significant decision to a qualified human decisionmaker. (This exception would apply only to a business's use of ADMT for significant decisions); and

(3) If the business evaluated the ADMT to ensure it worked as intended and was not discriminatory, and the business implemented safeguards to ensure that the ADMT worked as intended and was not discriminatory. (This exception would apply only to a business's use of ADMT for certain kinds of significant decisions (admission/acceptance/hiring and allocation/assignment of work); or work/educational profiling.)

Lastly, the proposed regulations clarify that the exceptions do not apply to the use of ADMT for profiling for behavioral advertising, nor to the use of consumers' PI for training ADMT.

1.2 Major Regulation Determination

A proposed regulatory package is determined to be a major regulation if the estimated economic impact of the regulation (including both direct costs and direct benefits) is expected to exceed $50 million over a 12-month period, once fully implemented. The direct compliance costs and direct benefits of the proposed regulations are expected to exceed this threshold.

Based on a preliminary assessment using conservative approaches to assessment of combined direct economic costs and benefits, the regulatory impacts are estimated to exceed $4 billion in the first year of implementation. Thus, it is our determination that the proposed regulations will exceed the $50 million threshold and thus the Agency's continued implementation of the CCPA qualifies as a major regulation and requires preparation of a Standardized Regulatory Impact Assessment.

1.3 Public Outreach and Input

Since the fall of 2021, the Agency has engaged in extensive public outreach and solicited broad public input relating to the proposed updates to the existing CCPA regulations, the clarification regarding when insurance companies must comply with the CCPA, and new proposed regulations on CSAs, RAs, and ADMTs.

In the fall of 2021, the Agency issued an invitation for written comment, which was open from September 22 through November 8, 2021.[2] The Agency received over 75 public comments, totaling over 850 pages.[3]

In the spring of 2022, the Agency hosted two days of instructive informational sessions by academics, officials from the California Office of the Attorney General, the Agency, and the European Data Protection Board on March 29 and 30, 2022. The Agency then hosted three days of stakeholder sessions, from May 4 through 6, 2022, providing an opportunity for members of the public to speak.[4] The sessions were collectively attended by many members of the public; and the Agency received approximately 100 comments, across all three sessions.[5]

On February 10, 2023, the Agency solicited additional preliminary written public comment in a submission period that ended on March 27, 2023.[6] The Agency received over 50 public comments, totaling over 1,000 pages, during and immediately following that comment period.[7]

The Agency again held three pre-rulemaking stakeholder sessions on May 13, 15, and 22, 2024 to receive feedback on the proposed CSA, RA, and ADMT regulations.[8] The sessions were collectively attended by nearly 400 members of the public; and the Agency received close to 50 comments across all three sessions.

In addition, the Agency has held seven Board meetings at which these topics have been discussed, and every meeting included the opportunity for members of the public to comment.

1.4 Baseline and Incremental Impacts of Proposed Regulations

California law requires that prior to undertaking a major rulemaking action the agency conducts an analysis "assessing and determining the benefits and costs of the proposed

[2] Cal. Priv. Prot. Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020* (Proceeding No. 01-21) (Sept. 22, 2021), ***available at*** https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

[3] Public comments received in response to the Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) are available at https://cppa.ca.gov/regulations/pre_rulemaking_activities.html.

[4] *California Consumer Privacy Act Regulations, Pre-Rulemaking Stakeholder Sessions,* CAL. PRIV. PROT. AGENCY (May 4–6, 2022), ***available at*** https://cppa.ca.gov/meetings/materials/20220504_06.html.

[5] Public comments received during Pre-Rulemaking Stakeholder Sessions are available at https://cppa.ca.gov/meetings/materials/20220504_06.html.

[6] Cal. Priv. Prot. Agency, Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (Feb. 10, 2023), available at https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html.

[7] Public comments received in response to the Agency's Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking are available at https://cppa.ca.gov/regulations/pre_rulemaking_activities_pr_02-2023.html.

[8] *California Consumer Privacy Act Regulations, Pre-Rulemaking Stakeholder Sessions,* CAL. PRIV. PROT. AGENCY (May 13, 2024), ***available at*** https://cppa.ca.gov/meetings/materials/20240513.html; *California Consumer Privacy Act Regulations, Pre-Rulemaking Stakeholder Sessions,* CAL. PRIV. PROT. AGENCY (May 15, 2024), ***available at*** https://cppa.ca.gov/meetings/materials/20240515.html; *California Consumer Privacy Act Regulations, Pre-Rulemaking Stakeholder Sessions,* CAL. PRIV. PROT. AGENCY (May 22, 2024), ***available at*** https://cppa.ca.gov/meetings/materials/20240522.html.

regulation" (Gov. Code § 11346.36). We interpret "benefits and costs of the proposed regulation" to mean the agency is tasked with evaluating the costs and benefits of the marginal changes proposed beyond existing law or regulation. In the present case, while the CCPA as amended by the CPRA has impacts in its own right, we aim to evaluate only the costs and benefits of the proposed regulations insofar as they define new obligations, either through the creation of new requirements or the new interpretation of existing requirements beyond what is required by current laws and regulations.

The counterfactual scenario without the proposed regulations is referred to as the regulatory baseline. For this SRIA, it is assumed that the overall California economy will grow according to the macroeconomic projections of the California Department of Finance (DOF).[9,10,11] As a condition for implementation in SRIA analysis, economy-wide models must provide accurate reference baselines for comparison to their own SRIA regulatory scenarios, as well as other state economic assessment[12] according to trajectories forecast by DOF in its regular forward projections, published twice per year.

There are three fundamental macroeconomic series or factors of importance for baseline calibration: Population, Employment, and Personal Income. Because population is an exogenous input to the BEAR Model, DOF projections are incorporated directly. In the case of Personal Income, DOF forecasts extend to 2027, but the BEAR Model tracks these exactly through a built-in calibration mechanism and extrapolates them to 2033.[13]

For the industry itself, several categories of economic statistics have been assembled from official and industry sources and, in some cases, estimates have been made to compensate for gaps in reporting.

Lastly, baseline conditions do not account for future legislation that may be implemented prior to implementation of the proposed regulations. We assume full compliance with existing legal requirements such that any new costs attributable to the proposed regulations are only associated with requirements that extend beyond those that already exist.

We label the difference between requirements associated with the proposed regulations and requirements associated with existing legal requirements as the "regulatory delta." As discussed in the previous section, in some cases, the proposed regulations clarify existing statutory or regulatory requirements (e.g., in the CCPA and existing CCPA

[9] California Code of Regulations, title 1, section 2003(b).

[10] http://www.dof.ca.gov/Forecasting/Demographics/.

[11] https://dof.ca.gov/forecasting/economics/economic-forecasts-u-s-and-california/.

[12] We would like to express our thanks to the DOF Chief Economist and staff for their cooperation and data sharing to support this calibration exercise. Any errors implementing these inputs are solely the responsibility of the authors. This version of the SRIA implements the latest DOF economic forecasts (as of 7/15/24) and last year's population projections. Although they were available this time last year, the latest estimates for population will not be available in time for completion of this SRIA.

[13] Full technical documentation of the BEAR Model, including its DOF conforming baseline calibration, is available upon request to admin@bearecon.com

regulations). In other cases, the proposed regulations articulate privacy protections that are already required by other laws (e.g., California and federal laws that broadly prohibit unfair or deceptive acts or practices).

In addition, many businesses that are subject to the CCPA are also subject to other states' privacy laws and the European Union's General Data Protection Regulation ("GDPR"); and the proposed regulations' requirements are largely consistent with those laws' requirements. Insofar as the proposed regulations' clarifications and articulations do not create new requirements for businesses, we consider any associated impacts to be statutory or part of the baseline, and we intentionally exclude them from the assessment.

In the following subsections, we discuss the elements of the proposed regulations that we considered as potentially constituting a "regulatory delta."

1.4.1 Changes to Insurance Code

The proposed insurance regulations do not have an economic impact because they articulate existing requirements for insurance companies. They do not introduce new laws nor amend existing legal rights or requirements. Rather, they acknowledge that the CCPA and Insurance Code may overlap in their jurisdiction and delineate the boundary between the two legal frameworks. Accordingly, any impacts associated with them would be attributed to the statutes or within the baseline and not the updates to existing CCPA regulations.

1.4.2 Proposed Updates to Existing CCPA Regulations

As discussed above, the proposed revisions to the CCPA regulations include several changes. However, only a subset of the changes constitutes regulatory deltas, and only a subset of the regulatory deltas has associated economic costs.

The following changes were assessed to have substantive economic costs attributable to the proposed regulations:

- 7003(d) – While mobile apps are already required to have a conspicuous link in the privacy policy associated, the proposed regulation adds the requirement that a link must be accessible *within the app itself*.
- 7011(d) – Makes mandatory the requirement that a mobile app's setting has a link to the company's privacy policy.
- 7014(e)(3) - Mirrors the requirements for Notice of Right to Opt-Out ("RTOO") of Sale/Sharing for the Notice of the Right to Limit ("RTL").
- 7020(e) - Consumers are entitled to obtain all their PI collected by the business after January 1, 2022, but there is nothing in the statute or previous round of rulemaking that requires businesses to alert consumers of this right. This allows a

type of loophole where consumers are entitled to all their PI, but likely have no way of knowing this without reading the statute. This rule addresses this issue by requiring businesses give consumers the option to request more than just 12 months of their PI.

- 7022(g)(5), 7023(f)(6), 7024(e), 7026(e), 7027(f) – This group of rules introduces required language informing consumers that they can file a complaint with the Agency and AG's office if a CCPA request is denied. This rule covers requests pertaining to requests to delete, request to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.
- 7023(f)(3) – Creates a requirement that the business inform the consumer that, upon the consumer's request, it will note both internally and to any person/business with whom it discloses, shares, or sells PI that the PI is contested by the consumer.
- 7023(f)(4) – Mirrors 7023(f)(3) but pertains to PI concerning a consumer's health. The consumer may provide a written statement to be included with the PI and made part of the consumer's record and this rule requires that, upon request, the business will make the written statement available to anyone who it shares the contested PI with.
- 7023(i) – Requires businesses to share the source of incorrect contested PI when they are not the source of the information.
- 7023(j), 7024(d) – 7023(j) concerns the ability of a consumer to check that specific pieces of inaccurate SPI have been corrected and requires that businesses not disclose the information but do allow consumers to confirm that the SPI it maintains is accurate. 7024(d) effectively mirrors 7023(j) but instead of concerning a Right to Correct ("RTC"), it is focused on a Right to Know ("RTK").
- 7025(c)(3), (4), (6) – Requires a business to display whether it has processed the consumer's opt-out preference signal ("OOPS").
- 7026(g) – Requires businesses display that a consumer's request to opt-out of sale/sharing has been processed.
- 7027(h) – Requires businesses provide a way to confirm requests to limit SPI have been honored.
- 7028(a)(c) – Extends to businesses that use SPI for purposes other than those set forth in 7027(m) the requirement that opting in after opting out of right to limit be a two-step process.

Changes described in 7001, 7002, 7004, 7005, 7013, 7050, 7051, 7053, 7060, 7063, 7300, and 7302 were determined to not have an economic impact because they simply clarify the existing statute, do not constitute substantive changes to existing requirements, or because they removed an existing obligation.

1.4.3 Proposed Cybersecurity Audits (CSA), Automated Decisionmaking Technology (ADMT), and Risk Assessment (RA) Regulations

Unlike the proposed updates to the existing CCPA regulations, the proposed CSA, ADMT, and RA regulations are new. Therefore, we consider most of these proposed regulations' requirements to constitute the "regulatory delta." However, the new requirements being proposed do overlap with certain existing CCPA and other laws' and regulations' requirements. Because we assume full compliance with existing laws and regulations, this means that compliance costs for the areas of overlapping requirements will be lower relative to a scenario where the other laws' and regulations' requirements were not already in place. The details of the overlapping requirements and how cost mitigation is modeled for each element of the proposed regulations are described below in Section 2.

2 Costs

This section describes the incremental compliance cost estimates used in this SRIA, representing each of several categories of incremental changes identified in Section 1.4.

The SRIA directive requires that prior to any major rulemaking package the agency conduct an economic assessment of the proposed regulation’s impacts on California business enterprises (Gov. Code § 11346.3(a)).

There are different ways that business units can be defined. We assess “California business enterprises” at the firm-level rather than the establishment-level according to definitions used by the US Census’s Statistics of US Businesses (SUSB).[14] For single-establishment firms there is no difference because a single-establishment business is equivalent to a firm (76% of firms in the US are single-establishment firms). However, for multi-establishment firms we count each multi-establishment firm as a single business rather than separate businesses. We do this because we assume in most cases CCPA compliance will be done at the firm-level rather than separately by each establishment within a firm. We rely on the SUSB methodology for defining firms which is based on Employer Identification Number (EIN) where multi-establishment firms are defined as businesses with multiple clustered EINs.

We interpret California business enterprises to mean firms with a physical presence in California according to the California Employment Development Department methodology (EDD).[15] This means that while many foreign businesses and businesses from other states without a physical presence in California will be impacted by the proposed regulations, they are purposefully excluded from our analysis because we recognize these impacts to be outside the scope of the SRIA.

2.1 How Many California Businesses are Impacted by the Proposed Regulations?

This section describes estimates for the number of businesses required to comply with each element of the proposed regulation. These estimates are then combined with estimated compliance costs per business in the subsequent section to characterize total compliance costs.

[14] See SUSB definition of firms: https://www.census.gov/programs-surveys/susb/technical-documentation/methodology.html.

[15] https://labormarketinfo.edd.ca.gov/LMID/Size_of_Business_Report_Terms.html.

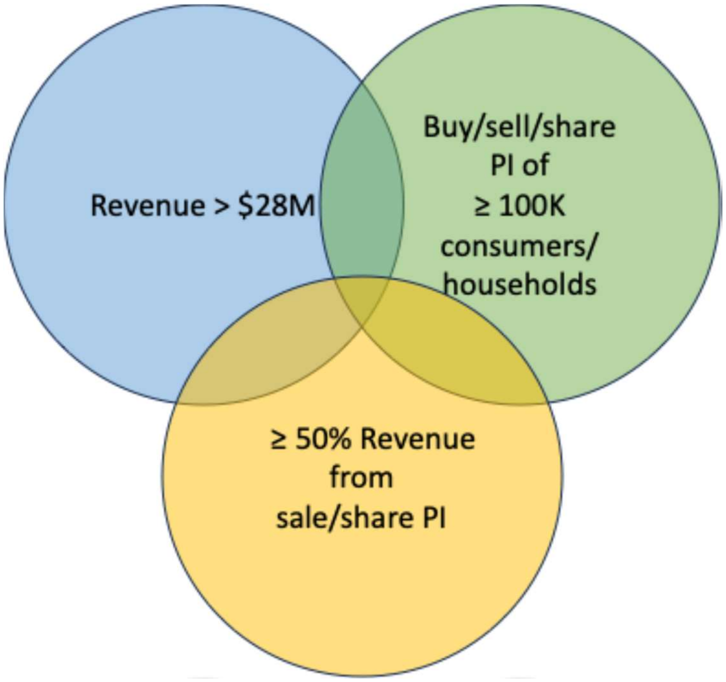
2.1.1 Businesses Required to Comply with Proposed Updates to CCPA Regulations

Businesses are required to comply with the CCPA if they meet any of the following three criteria, as well as other criteria set by statute (e.g., they determine the purposes and means of processing consumers' PI):

1. Annual revenue exceeds $27,950,000.00 in the preceding calendar year[16] OR;
2. Buy, sell, or share the PI of 100,000 or more consumers or households per year OR;
3. Receive 50% or more of their annual revenue from selling or sharing PI.

Because meeting any of the three criteria necessitates compliance with the CCPA, covered businesses can meet any combination of the three criteria (Figure 2-1).

Figure 2-1: California Businesses Required to Comply with the CCPA


Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

There is no readily available database that tracks the number of "California businesses" subject to the CCPA. Therefore, we must estimate how many California businesses meet at least one of the criteria shown in Figure 2-1. We first focus on estimating the number of businesses with annual revenue greater than $28M before estimating how many businesses would meet either of the PI related criteria.

[16] Original CCPA figure is $25 million. AB 3286 (July 2024) provides for a two-year look back to adjust for inflation. Based upon recent DIR CPI figures, we assume 11.8% increase for purposes of this SRIA.

The following section describes each step in detail.

1. **Did the business's annual revenue exceed $28M in the preceding calendar year?**

Outside of publicly traded companies, business revenue is not typically publicly reported. We therefore use publicly available aggregate data to estimate the number of California businesses with annual revenue >$28M by sector.

The Bureau of Economic Analysis (BEA) publishes firm population by North American Industry Classification System (NAICS) code[17], and BLS publishes total payrolls for the same industry codes. Estimates of average firm revenue per employee were combined with EDD data on the count of firms and number of firm employees, with all three series disaggregated by industry code. Firms are identified by level of annual revenue in the following steps.

We first collect EDD estimates by 2-3 digit NAICS codes for California payrolls and number of firms in each of the following workforce size buckets: 0-4, 5-9, 10-19, 20-49, 50-99, 100-249, 250-499, 500-999, 1000+. We utilize the most current data available from first quarter of 2022, when detailed analysis for this SRIA began in August of 2023.[18] We combine this information with EDD estimates of number of firms in each workforce size category. Together, the two yields average number of workers per firm in each workforce size bucket.

Next, we use the BEA Input-output table for California, a detailed accounting for interindustry transfers and value-added, and final demand, to extract shares of Labor Value Added (LVA) in Gross Output (GO) for each sector. By assuming LVA corresponds to Payrolls and GO to revenue, we can calculate revenue for all the NAICS sectors by dividing Payroll (EDD Table 2A) by LVA share.

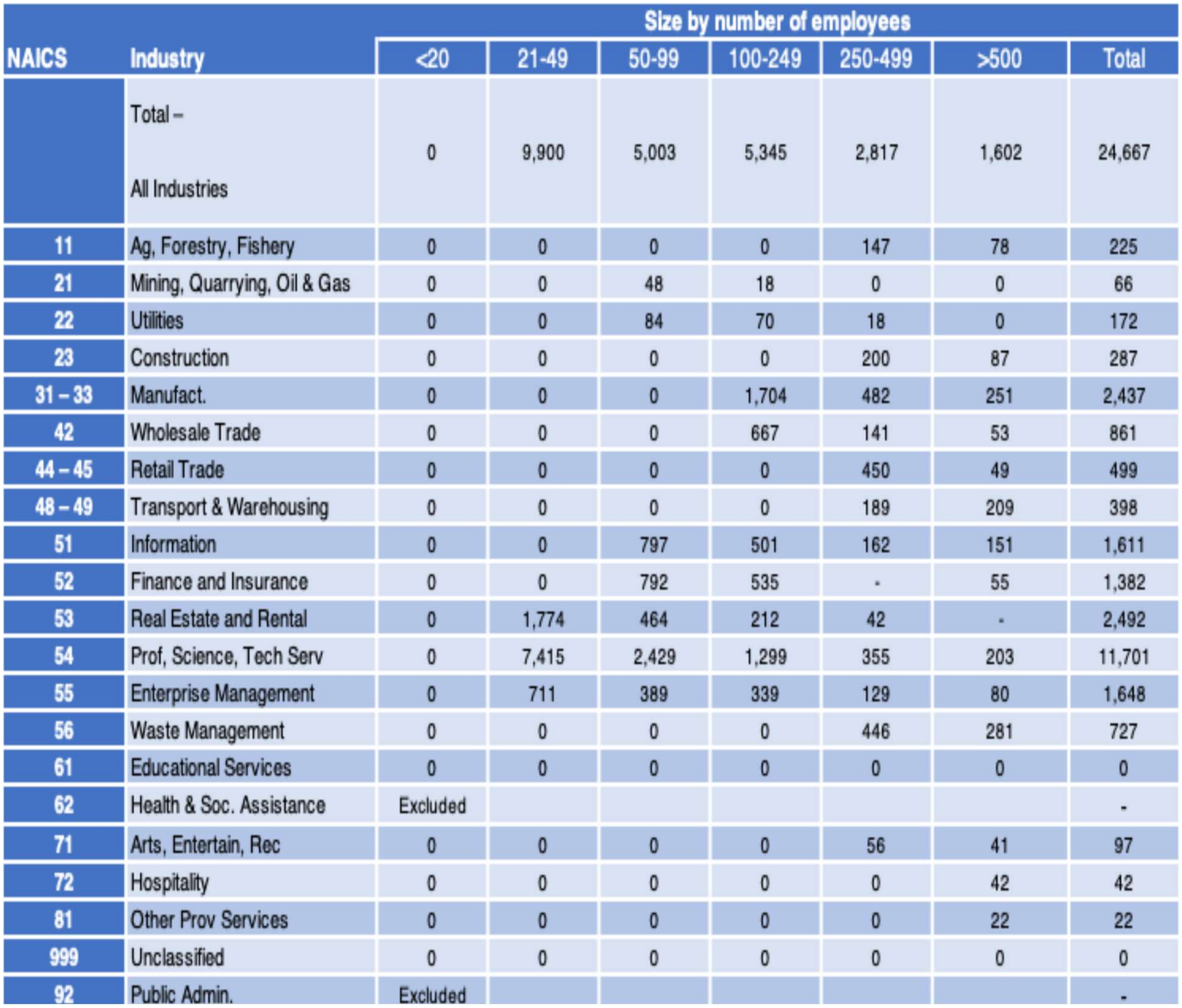
Combining these outputs, we calculate average revenue per worker for every NAICS sector and workforce size bucket, then convert to NAICS and firm revenue size buckets using the EDD workforce sizes. This calculation makes the assumption that average employee salaries in the same industry are the same across firms of different sizes. Given the potential underlying heterogeneity in salaries by firm size, this assumption may understate larger firms' revenues and/or overstate smaller firms' revenues. To the extent that 60% of California businesses subject to the proposed regulations have less than 100 employees and 40% have more, use of an average salary within an industry could provide a conservatively high estimate of the number of firms subject to an annual revenue threshold.

[17] We use 2017 NAICS codes rather than the 2022 update to correspond to the NAICS codes classification used in the most recent available SUSB data (https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html).

[18] https://labormarketinfo.edd.ca.gov/file/indsize/2A-22-1-FINAL.xlsx

Combined, this enables identification of the number of firms with average revenue of at least $28M. Estimated number of California firms to have annual revenue >$28M are shown by industry in Table 2-1.

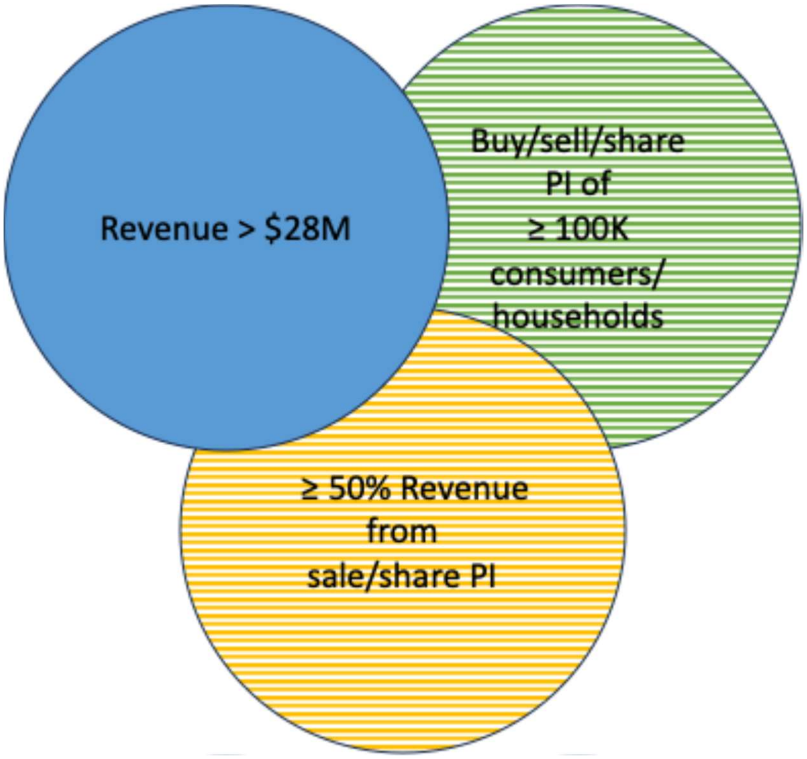
Table 2-1: Number of California Businesses with Average Revenue > $28M



NAICS	Industry	Size by number of employees						
		<20	21-49	50-99	100-249	250-499	>500	Total
	Total – All Industries	0	9,900	5,003	5,345	2,817	1,602	24,667
11	Ag, Forestry, Fishery	0	0	0	0	147	78	225
21	Mining, Quarrying, Oil & Gas	0	0	48	18	0	0	66
22	Utilities	0	0	84	70	18	0	172
23	Construction	0	0	0	0	200	87	287
31 – 33	Manufact.	0	0	0	1,704	482	251	2,437
42	Wholesale Trade	0	0	0	667	141	53	861
44 – 45	Retail Trade	0	0	0	0	450	49	499
48 – 49	Transport & Warehousing	0	0	0	0	189	209	398
51	Information	0	0	797	501	162	151	1,611
52	Finance and Insurance	0	0	792	535	-	55	1,382
53	Real Estate and Rental	0	1,774	464	212	42	-	2,492
54	Prof, Science, Tech Serv	0	7,415	2,429	1,299	355	203	11,701
55	Enterprise Management	0	711	389	339	129	80	1,648
56	Waste Management	0	0	0	0	446	281	727
61	Educational Services	0	0	0	0	0	0	0
62	Health & Soc. Assistance	Excluded						-
71	Arts, Entertain, Rec	0	0	0	0	56	41	97
72	Hospitality	0	0	0	0	0	42	42
81	Other Prov Services	0	0	0	0	0	22	22
999	Unclassified	0	0	0	0	0	0	0
92	Public Admin.	Excluded						-

In total, we estimate 24,667 California businesses are covered by the CCPA because their annual revenue exceeds $28M. This estimate reflects all businesses in this revenue range regardless of whether they buy/sell/share PI of 100,000 consumers or households or receive more than 50% of their revenue from sale/share of PI (Figure 2-2). In subsequent steps, we first subset to the number of businesses *with annual revenue <$28M* before estimating the subset of those that buy, sell, or share PI for 100,000 or more consumers or households or those that make 50% or more of their annual revenue from selling or sharing PI.

Figure 2-2: California Businesses with Annual Revenue >$28M


Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

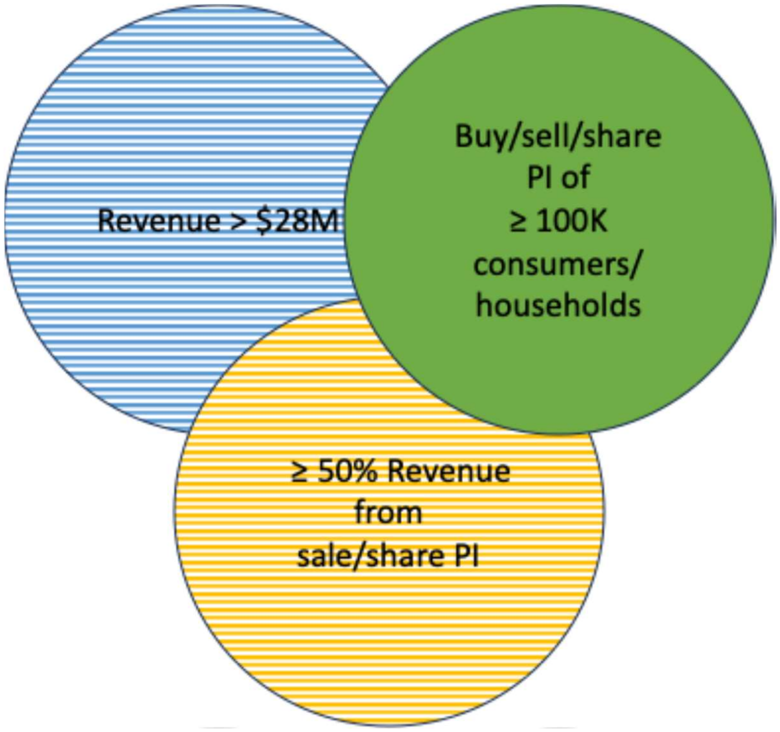
Caption: *We first identify all businesses in California with annual revenue >$28M regardless of whether they meet the other criteria (Blue visible).*

2. **For businesses with annual revenue <$28M, did the business buy, sell, or share the PI of 100,000 or more consumers or households?**

The 24,667 California businesses estimated to have annual revenue >$28M have already been addressed. Next, for each 6-digit NAICS code, we assess whether a firm with annual revenue below $28M could plausibly buy, sell, or share the PI of 100K or more consumers or households per year. The selected NAICS codes and descriptions are included in Appendix 1.

To set an upper bound for economic impacts, we assume that 100% of California businesses with less than $28M in annual revenue from any of our identified 6-digit NAICS codes buy/sell/share the PI of 100K or more consumers or households per year. The total number of businesses included in this exercise reflects the shaded area in Figure 2-3, businesses with annual revenue <$28M but that may buy/sell/share PI of 100K or more consumers or households per year.

Figure 2-3: California Businesses with Annual Revenue <$28M that Buy/Sell/Share PI of ≥ 100K Consumers or Households


Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

Caption: *Because we already accounted for all businesses with annual revenue >$28M, in this step we focus on businesses with annual revenue <$28M but that do buy/sell/share the PI of 100K or more consumers or households (Green visible).*

The number of California businesses grouped by number of employees and detailed sector (6-digit NAICS) is available from SUSB.[19] It should be noted that the most recently released SUSB data is from 2021. It's plausible that utilizing 2021 data could lead to an underestimate of covered firms if anomalous economic conditions associated with the COVID-19 Pandemic caused the number of California firms to decrease. However, EDD data[20] indicate that there was never a contraction in the total number of California firms but just marginally slower than average growth. As such, we believe the highly detailed SUSB data from 2021 which are available by employee count and 6-digit NAICS, are a suitable data source the use of which produces a fair approximation of current conditions. Given the slow growth in total firms in recent years, alternative data sources, which are primarily available at the 4-digit NAICS level, are likely to lead to similar estimates.

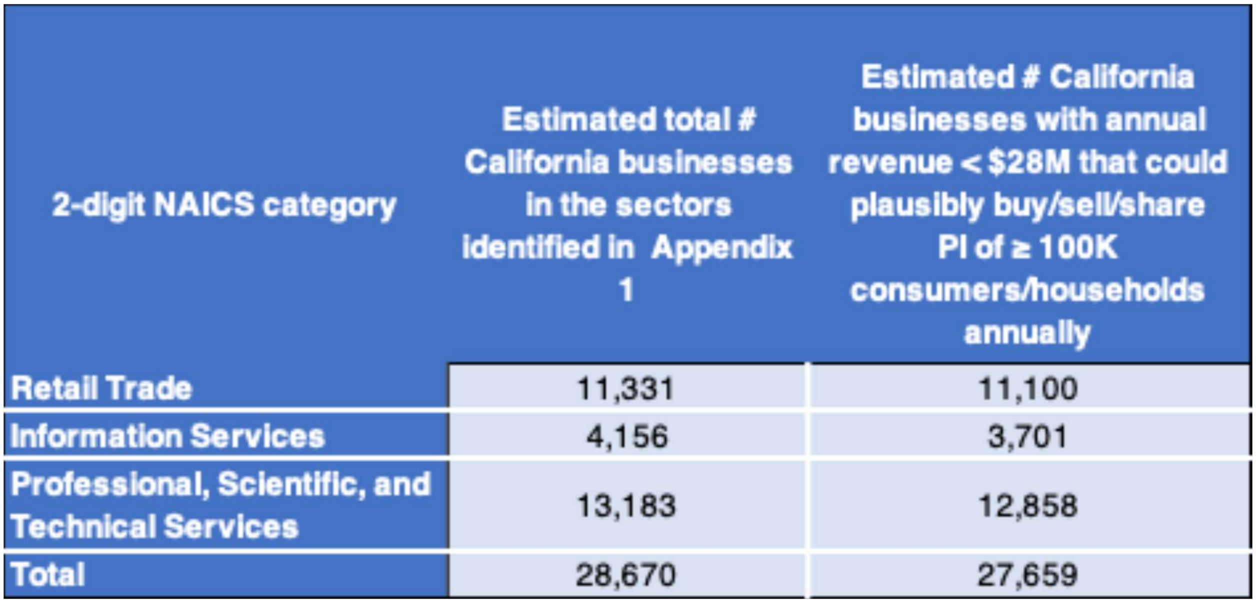
We do not observe firm revenue by 6-digit NAICS code in the SUSB data. Therefore, to identify the subset of businesses in each sector that have annual revenue <$28M we

[19] https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html

[20] https://labormarketinfo.edd.ca.gov/LMID/Size_of_Business_Data.html

follow previous work and assume a fixed revenue per employee such that businesses with less than 100 employees are assumed to have annual revenue less than $28M. The total number of businesses in the sectors identified are shown in Table 2-2. The 6-digit NAICS codes which correspond to these estimates are shown in Appendix 1.

Table 2-2: Estimated Number of California Businesses by NAICS Code



2-digit NAICS category	Estimated total # California businesses in the sectors identified in Appendix 1	Estimated # California businesses with annual revenue < $28M that could plausibly buy/sell/share PI of ≥ 100K consumers/households annually
Retail Trade	11,331	11,100
Information Services	4,156	3,701
Professional, Scientific, and Technical Services	13,183	12,858
Total	28,670	27,659

3. Did the business receive 50% or more of their annual revenue from sale/share of PI?

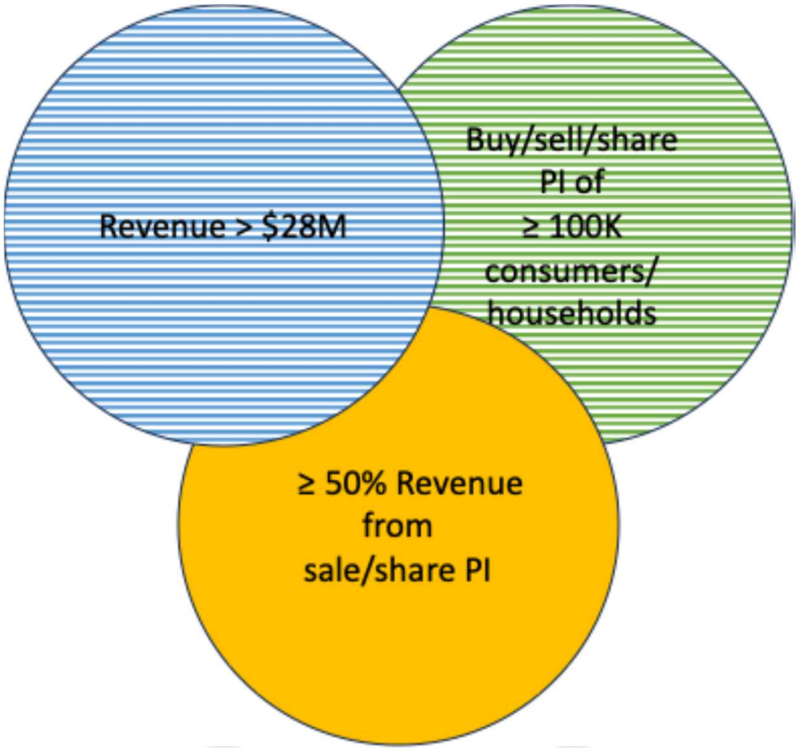
Finally, we turn to businesses that receive 50% or more of their annual revenue from the sale/share of PI. We do not have a reliable way to estimate the share of revenue that businesses receive from PI. Instead, we assume that data brokers, businesses whose primary business activity is working with data, are the sole group that receives 50% or more of their revenue from sale/share PI. The Agency maintains a list of registered data brokers that operate in California which includes 500 businesses.[21] While some data brokers may meet the annual revenue criteria, we expect that most will not. However, many data brokers are likely to buy/sell/share PI of 100K or more consumers or households. Therefore, we assume data brokers constitute the overlapping areas between those businesses that receive 50% or more of their revenue from PI and those businesses that buy/sell/share PI of 100K or more consumers or households (Figure 2-4).

To account for the area of overlap highlighted in Figure 2-4 and avoid double counting, we assume data brokers are a subset of the businesses identified in the previous step and prior to adding the total number of covered businesses we subtract data brokers from

[21] https://cppa.ca.gov/data_broker_registry/

our estimated number of businesses that buy/sell/share PI of ≥ 100,000 consumers or households. In other words, while we estimated 27,659 businesses in the previous step, we subtract off 500 (the number of registered data brokers) prior to adding all businesses together.

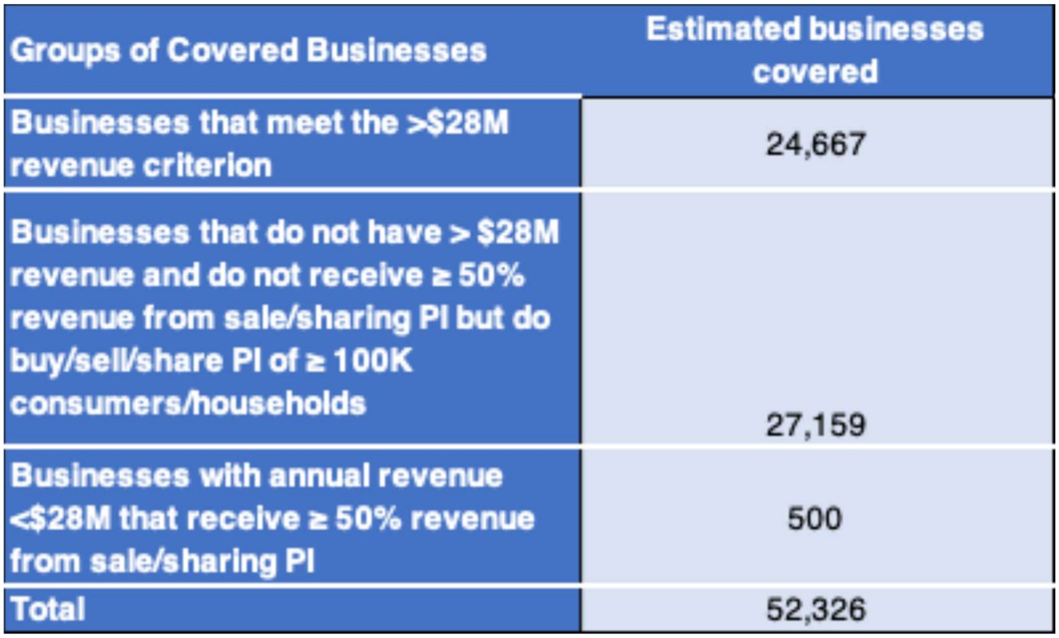
Figure 2-4: Data Brokers are Assumed to Receive Large Shares of Revenue from Sale/Share PI and to Buy/Sell/Share High Volumes of PI


Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

Caption: *Data Brokers are assumed to receive ≥ 50% of revenue from sale/share PI and to buy/sell/share PI of ≥100K consumers or households but to not generate annual revenue >$28M (Yellow visible).*

Combining the calculations yields the following total count of businesses as shown in Table 2-3:

Table 2-3: Estimated Total Counts of Businesses Covered by the Proposed Updates to the CCPA Regulations



Groups of Covered Businesses	Estimated businesses covered
Businesses that meet the >$28M revenue criterion	24,667
Businesses that do not have > $28M revenue and do not receive ≥ 50% revenue from sale/sharing PI but do buy/sell/share PI of ≥ 100K consumers/households	27,159
Businesses with annual revenue <$28M that receive ≥ 50% revenue from sale/sharing PI	500
Total	52,326

The approach used here to estimate the number of California businesses covered by the CCPA likely leads to an overestimate. The assumption that all 27,159 businesses from the 6-digit NAICS code sectors described in Appendix 1 buy/sell/share the PI of ≥ 100K consumers or households per year is likely to substantially overstate the number of businesses covered by the CCPA. Realistically, only a subset of these businesses will buy/sell/share the PI of ≥ 100K consumers or households per year and therefore be covered by the CCPA. For example, if we assume that businesses with less than 5 employees never buy/sell/share the PI of ≥100K consumers or households per year then the total number of firms estimated to have annual revenue < $28M but that buy/sell/share PI of ≥ 100K consumers/households gets reduced from 26,974 to 5,541. Nonetheless, for our estimation procedure we maintain the more conservative assumption that all businesses in these NAICS codes buy/sell/share PI of ≥ 100K consumers/households.

2.1.2 Businesses Required to Comply with Proposed CSA Regulations

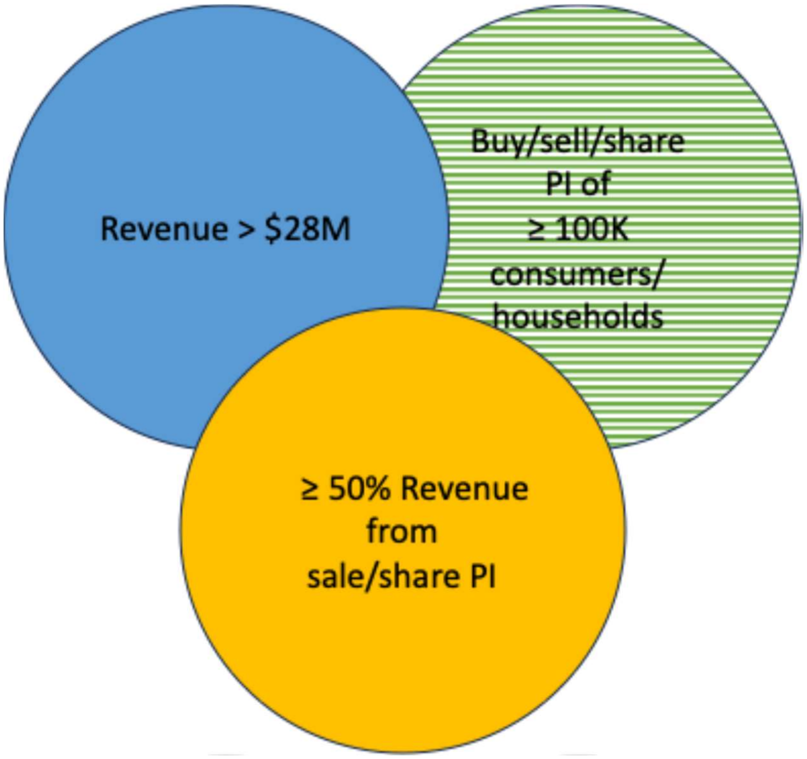
Businesses are required to comply with the proposed CSA regulations if they meet *any of the following criteria* in the preceding calendar year:

1. Derived 50% or more of their annual revenue from selling or sharing PI; OR
2. Had annual revenue >$28M and processed the PI of 250,000 or more consumers or households; OR

3. Had annual revenue >$28M and processed the SPI of 50,000 or more consumers.

The subset of businesses covered by the CCPA that will be obligated to conduct CSAs are those that receive ≥ 50% revenue from selling or sharing PI (regardless of total annual revenue or PI volume processed) as well as those that generate >$28M in annual revenue and processed the PI of ≥ 250,000 consumers or households or the SPI of ≥ 50,000 consumers or households in the preceding calendar year (Figure 2-5).

Figure 2-5: Subset of CCPA Covered Businesses that will be Required to Comply with Proposed CSA Regulations

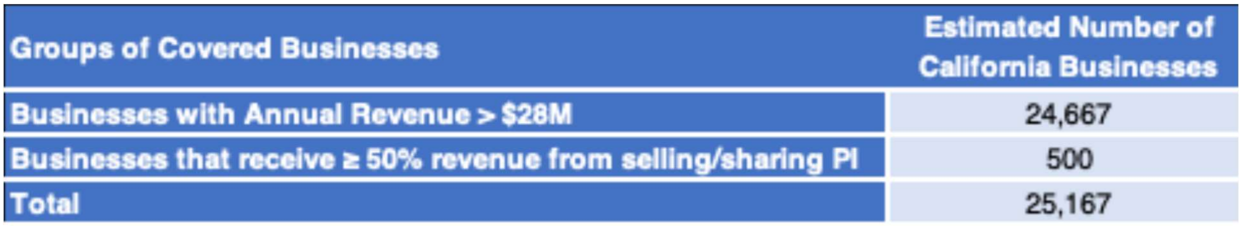

Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

Caption: *Businesses that will be required to comply include all those that make ≥ 50% revenue from selling/sharing PI, as well as a subset of those with >$28M revenue (Blue or Yellow visible). We assume all businesses that had annual revenue > $28M process the PI of ≥ 250,000 consumers or households or process the SPI of ≥ 50,000 consumers (hashed area Figure 2-5). To estimate the number of businesses that receive ≥ 50% of revenue from sale/share PI we utilize the Agency's database of registered data brokers and we again assume that all data brokers have annual revenue <$28M.*

If any businesses that had annual revenue >$28M did not process sufficiently high levels of PI or SPI to be covered by the proposed CSA regulations then our estimate for the number of businesses required to conduct CSAs would be an overestimate.

Applying this approach to the total number of California businesses in each sector we estimate there are a total of 25,167 California businesses that will be required to comply with the proposed CSA regulations (Table 2-4).

Table 2-4: Estimated Number of California Businesses Required to Comply with Proposed CSA Regulations



Groups of Covered Businesses	Estimated Number of California Businesses
Businesses with Annual Revenue > $28M	24,667
Businesses that receive ≥ 50% revenue from selling/sharing PI	500
Total	25,167

2.1.3 Businesses Required to Comply with Proposed ADMT Regulations

Businesses that are covered by the CCPA are required to comply with the proposed ADMT regulations if they meet any of the following criteria:

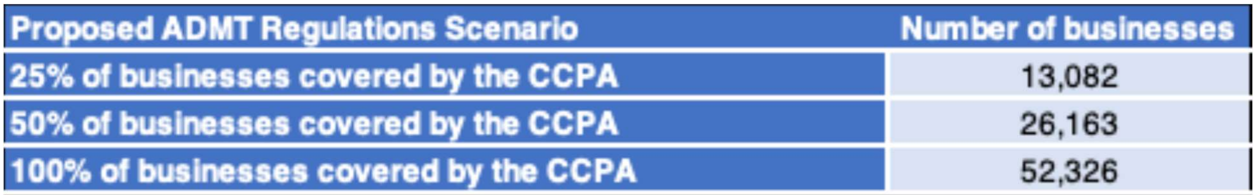
1. Use ADMT to make a significant decision; OR
2. Use ADMT for extensive profiling; OR
3. Process PI to train ADMT that could be used in certain ways outlined by the regulation.

The group of California businesses required to comply with the proposed ADMT regulations is therefore the subset of all businesses covered by the CCPA that use ADMT for one or more of the purposes outlined in the proposed regulations.

Data identifying the number of California businesses covered by the CCPA that use ADMT for any of the three highlighted reasons is not available. We therefore estimate costs of the proposed ADMT regulations using a scenario analysis with high, medium, and low proportions of CCPA covered businesses meeting the requirements to be covered by the proposed ADMT rules: 25%, 50%, and 100%.

The number of California businesses estimated to be covered by the proposed ADMT regulations under the three scenarios described above range from 13,082 to 52,326 (Table 2-5).

Table 2-5: Estimated Number of California Businesses Required to Comply with the Proposed ADMT Regulation



Proposed ADMT Regulations Scenario	Number of businesses
25% of businesses covered by the CCPA	13,082
50% of businesses covered by the CCPA	26,163
100% of businesses covered by the CCPA	52,326

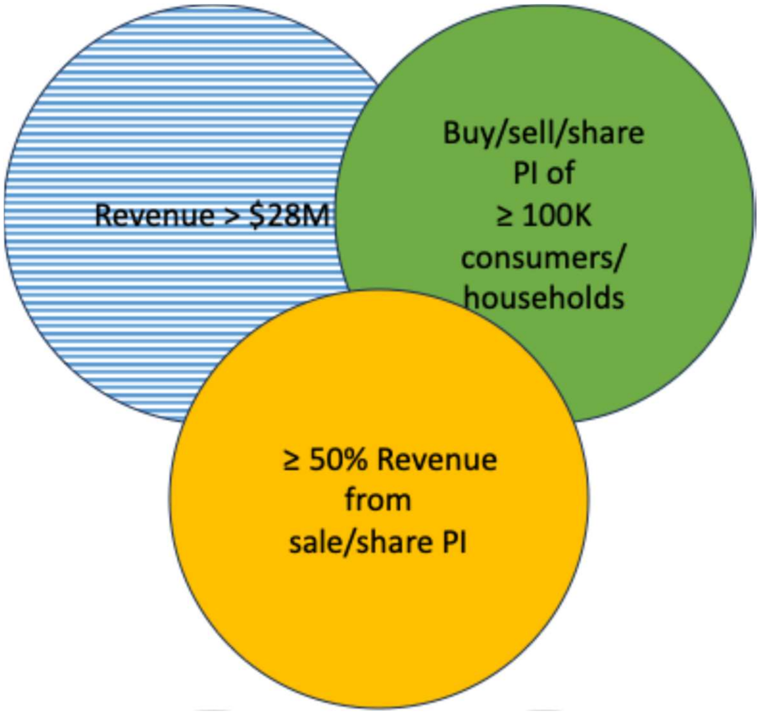
2.1.4 Businesses Required to Comply with Proposed RA Regulations

Businesses that are covered by the CCPA are required to carry out an RA under the proposed regulations if they meet any of the following criteria:

1. Sells or shares consumers' PI; OR
2. Collects, uses, discloses, or otherwise processes consumer's SPI; OR
3. Uses ADMT for a "significant decision" or "extensive profiling"; OR
4. Processes PI to train ADMT or AI that could be used in certain ways outlined by the regulation.

While the type of RA required will depend on the specific business activities, nearly all businesses covered by the CCPA will meet at least one of the criteria that requires an RA (Figure 2-6). For example, any business that receives >50% of revenue from sale/sharing of PI will be required to conduct an RA for its sale/sharing of PI. Additionally, any business that sells/shares PI of >100K consumers or households would also be required to conduct an RA for its sale/sharing. While this would initially suggest that all of the 27,659 businesses we identified previously as meeting the buy/sell/share PI of ≥100K consumers or households would be subject to the proposed RA requirements, some portion of these businesses buy PI and do not sell/share. We have no way of estimating what percent of businesses buy versus sell/share PI. Therefore, there is still some uncertainty in what portion of CCPA covered businesses will be required to conduct an RA.

Figure 2-6: California Businesses Covered by Proposed RA Regulation


Revenue > $28M
Buy/sell/share PI of ≥ 100K consumers/ households
≥ 50% Revenue from sale/share PI

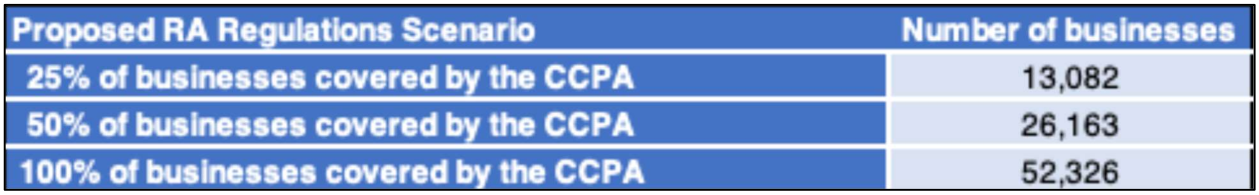
***Caption:** Businesses that buy/sell/share PI of more than 100,000 consumers/households or receive more than 50% of revenue from sale/share of PI will be required to conduct RAs (Green or Yellow solid). Whether the other group of businesses covered by the CCPA (businesses with annual revenue >$28M that receive <50% of revenue from PI and do not buy/sell/share PI of 100,000 consumers/households may or may not be covered depending on the types of PI related business activities conducted (hashed area).*

In theory, it is also possible that a business that is covered by the CCPA because it had annual revenue > $28M but that does not sell or share PI, does not process SPI, does not use ADMT for a significant decision or extensive profiling, and does not use PI to train ADMT or AI in the ways outlined in the proposed regulations would not be required to comply with the proposed RA regulations. While we believe this to be a small number of businesses overall, there is a still a level of uncertainty.

Given the uncertainty, a scenario analysis is appropriate here. We use a similar scenario analysis as the ADMT regulation with high, medium, and low proportions of CCPA covered businesses meeting the requirements to be covered by the proposed ADMT rules: 25%, 50%, and 100%.

The number of California businesses estimated to be covered by the proposed RA regulations under the three scenarios described above range from 13,082 to 52,326 (Table 2-6).

Table 2-6: Number of California Businesses Required to Comply with the Proposed RA Regulations



Proposed RA Regulations Scenario	Number of businesses
25% of businesses covered by the CCPA	13,082
50% of businesses covered by the CCPA	26,163
100% of businesses covered by the CCPA	52,326

2.2 Direct Costs

This section describes the estimated direct costs associated with each of the proposed regulations.

2.2.1 Proposed Updates to Existing CCPA Regulations

Before discussing the number of affected businesses and costs to firms, we must clearly define how the proposed rulemaking goes beyond existing law or previous rounds of rulemaking to establish new requirements. This distinction, which we label the regulatory "delta," is crucial as it identifies which elements of rulemaking are novel and beyond existing law. It is only for these regulatory deltas that costs (or benefits) can be attributed to the proposed regulation.

For the proposed changes to the CCPA regulations there are several regulatory deltas. In this analysis, we highlight the relevant sections where deltas are identified and discuss the cost estimation strategy for that specific section.

Number of Affected Businesses

We estimate that 52,326 businesses are subject to the CCPA and therefore would be impacted by this proposed rulemaking.

Direct Costs of Proposed Updates to Existing CCPA Regulations

7003(d)

The regulatory delta associated with 7003(d) is nuanced. Current requirements state “For mobile applications, a conspicuous link shall be included in the business’s privacy policy, which must be accessible through the mobile application’s platform page or download page.” Therefore, mobile apps are already required to have a conspicuous link in the privacy policy associated with the mobile app and any costs of developing that are attributable to the existing requirements. The proposed regulation adds the requirement that a link must be accessible *within the app itself*.

The only cost directly attributable to the proposed regulation is to companies that have apps that must insert the link in their app. The initial development of a link is attributed to the baseline, so the only additional cost is the time for a developer to add the existing link to a mobile app. We conservatively estimate the work time for this to be completed to be 0.5 hours. Wage data comes from the Occupational Employment and Wage Statistics (OEWS) program of the EDD. OEWS estimates an hourly wage of $91.14 for a software developer in Q1 2023.

Additionally, in the last round of rulemaking this feature was suggested but not required. The proposed regulation alters the language from the suggestion that businesses “may” have a link within the app to the requirement that businesses “shall” have a link. Therefore, to the extent that companies have already voluntarily adopted this feature, not all businesses with mobile apps will incur new costs.

Approximate costs are:

Costs = [# of businesses subject to CCPA with mobile apps that do not already have link to privacy policy from within app] * [cost of altering mobile app to have privacy policy link]

Costs = (52,326 *0.43*0.65) * 45.57 = **$666,467**

Calculation inputs:

1. # businesses subject to CCPA [52,326]
2. Subset of (1) that have mobile apps [43%]
3. Subset of (2) that don't already have link to privacy policy in mobile app [65%]
4. Cost of developer time adding link to app [0.5 hour of developer time at $91.14 hour]

7011(d)

Although there is a regulatory delta here, businesses complying with 7003(d) have already borne this cost. Section 7003(d) says that the privacy policy must be accessible through a link within the application such as the settings menu. We assume developers will place the link in the settings menu to comply with both sections of the regulation. Therefore, to avoid double counting costs we only estimate the cost of compliance associated with 7003(d) but do not estimate additional costs associated with 7011(d).

7014(e)(3)

This element of the proposed regulation has to do with notice of the RTL SPI and mirrors what already exists in the regulations for the RTOO (7013(e)(3)). Specifically, this subsection adds language that companies must include the notice of the RTL in the same manner that SPI that it uses or discloses for purposes other than those specified in section 7027(m) is collected.

A similar logic applies as in the analysis from section 7023(d) in the last round of rulemaking where the structure has already been established and an employee would just need to provide an additional prompt.[22] Given that businesses must already provide this notice for the RTOO, the system has been established and only additional text is needed to notify consumers that this extends to the RTL.

Furthermore, the proposed regulation is only extended to SPI. Therefore, the only companies that will have a cost are those that collect SPI for purposes other than those specified in section 7027(m) and that interact with consumers in ways outside of websites. We are unable to reliably estimate what portion of businesses would collect SPI outside of websites so as an upper bound we include all companies subject to the CCPA.

Since the existing structure is attributed to the baseline, we conservatively estimate adding the appropriate RTL language will be 0.5 hours' worth of employee time. Some updated language will be done in offline situations, while others will require updates on a web-based interface. We have no way of estimating wage rates for each affected industry, so we use the average wage rate across two groups of workers: office and admin support

[22] See "Notes on Economic Impact Estimates for Form 399 (2023)."

($25.91) and software developers ($91.14). This gives an approximate estimated wage rate of $58.525/hour.

Approximate costs are:

Costs = [# of businesses subject to CCPA] * [cost to add RTL link on platform]

Costs = 52,326 * 29.2625 = **$1,531,190**

Calculation inputs:

1. # of businesses subject to CCPA [52,326]
2. average cost of adding RTL link to RTOO infrastructure including non-web platforms [0.5 hours * $58.525]

7020(e)

Consumers are entitled to obtain all their PI collected by the business after January 1, 2022, but there is nothing in the statute or previous round of rulemaking that requires businesses to alert consumers of this right. This allows a type of loophole where consumers are entitled to all their PI, but likely have no way of knowing this without reading the statute. This rule intends to address this shortcoming.

While there is a regulatory delta here, it is minimal as it builds on the existing baseline. Businesses must already provide a method for consumers to request their PI collected by the business for the 12 months preceding the consumer's request. This new rule adds that businesses must provide a method for obtaining PI beyond 12 months. Therefore, the existing structure is already in place and what must be amended is a line of text inserted in the same structure. The statute provides consumers with the right to obtain their PI, so any cost associated with providing the additional data is attributed to the statute. The only cost associated with the proposed regulation is the cost of informing consumers they are entitled to PI beyond the 12 months preceding the consumer's request.

To perfectly estimate costs, we would need to know the number of firms subject to CCPA that maintain PI more than 12 months. There is no way to reliably estimate that number so as an upper bound estimate we assume all firms subject to CCPA will be subject to this cost.

We would also need to know the hourly wage rate for each employee who is responsible for adding the additional line of text. There will certainly be some non-web-based interfaces where this occurs, but we are unable to estimate this portion and instead use the blended wage rate between clerical and software developers. Since the underlying structure already exists from the baseline, we conservatively estimate the time needed to be 0.5 hours.

Approximate costs are therefore:

Costs = [# businesses subject to CCPA] * [average cost to inform consumers all PI is available]

Costs = 52,326 * 29.2625 = **$1,531,190**

Calculation inputs:

1. # businesses subject to CCPA [52,326]
2. Cost of adding text informing all PI available regardless of timing [0.5 hours at $58.525 hour]

7022(g)(5), 7023(f)(6), 7024(e), 7026(e), 7027(f)

The proposed updated regulation introduces language informing consumers that they can file a complaint with the Agency and AG's office if a CCPA request is denied. This applies to all CCPA requests—requests to delete (7022(g)(5)), requests to correct (7023(f)(6)), requests to know (7024(e)), requests to opt-out of sale/sharing (7026(e)), and requests to limit (7027(f)).

Although these proposed updated regulations are similar, each will incur a separate cost (and benefit) as they pertain to different requests for PI. That being said, the structure of the costs is the same in each case and they are: (1) added cost of language to business's response letters/communications; (2) added cost in number of complaints for the Agency and AG.

The first cost is minimal as it is just adding language to the business's existing response letters. Consumers will already be notified of the denial, but now additional language is required to inform consumers of their right to file a complaint. The language is the same across all denials and example text is included in the proposed regulation. There is some cost here but depending on the estimated length of time to insert the notification into the text, the costs are likely small.

The second cost is fiscal and will be estimated in consultation with the Agency as part of the broader fiscal cost analysis. Again, as a conservative upper bound estimate, we assume it will take an employee 0.5 hours to amend the response letters. This time considers the response letters for each section. Updates to the language will likely be performed by a range of workers from clerical to software developers so we use the average wage rate of $58.53.

Costs are approximately:

Costs = [# businesses subject to CCPA] * [cost of adding 1-2 sentences of text including a link to response letters].

Costs = 52,326 * 29.2625 = **$1,531,190**

Calculation inputs:

1. # businesses covered by CCPA [52,326]
2. Cost of adding sentences to letter [0.5 hour of employee time at $58.525 hour]

7023(f)(3)

If a business denies a consumer's request to correct (RTC) this subsection requires businesses to note that the accuracy of the PI has been contested. Businesses must note this internally, as well as any others to whom it discloses, shares, or sells the PI. Businesses must also inform the consumer of this right.

There are two costs associated with this subsection. The first is minimal which is informing the consumer of their right for the PI contention to be passed downstream. Businesses will already be notifying consumers whether they have complied with their request, so this cost is just an additional line of text explaining the additional right.

The second cost category is more involved as it requires businesses to insert some type of notification or tag with the PI to inform others who use it that the PI has been contested. The cost should be relatively small because this proposed regulation applies on a going-forward basis, and so the PI in question can simply be amended to include the notification of contestation. We assume it will take a software developer 10 hours to create a toggle that employees can tag when PI has had a contested RTC but has been denied.

Finally, in principle there could be lost value to PI that is tagged as contested. However, since the request was denied, we assume the PI remains accurate and thus the full value of the PI is retained.

The universe of affected companies is less than every company subject to CCPA because only companies that have denied a consumer's RTC are affected. To be able to deny a request also requires a consumer to submit a request to correct in the first place. Knowing what percent of companies receive consumers RTC and then what portion of those are denied would identify the relevant number of affected companies. This estimation is likely not feasible, however. As an upper bound we could assume that every company subject to the CCPA will receive a request to correct in the course of the year after the proposed regulation is introduced and will deny a request at some point. Furthermore, we should assume that every company must be prepared for this scenario. Thus, the relevant number of companies would be every company subject to the CCPA.

Costs are approximately:

Costs = [# of businesses covered by CCPA] * [employee time to insert language to existing response letters + employee time to insert a tag that the PI has been contested]

Costs = 52,326 * (45.57+ 911.40) = 52,326 * ($956.97) = **$50,074,412**

Calculation inputs:

(1) # businesses covered by CCPA [52,326]

(2) cost of updating consumer notification [0.5 hour of software developer time at $91.14/hour]

(3) cost of tagging PI that has been contested for forward uses [10 hours of software developer time at $91.14 hour]

7023(f)(4)

The regulatory delta here is very similar to 7023(f)(3) but extends only to PI concerning a consumer's health. The consumer may provide a written statement to be included with the PI and made part of the consumer's record. The proposed updated regulation requires that upon request, the business will make the written statement available to anyone who it shares the contested PI with.

Thus, the cost mechanism is quite similar to 7023(f)(3). There is no specific mention in the proposed regulation that the business must inform the consumer of this right, but we assume this to be the case and thus there will be updated language required. Only future sharing of PI will be affected, requiring the consumer's statement to be included with any future disclosure, sharing, or selling of PI.

Since the consumer will be providing the actual written statement, there is no cost to the business other than tagging it to the relevant piece of PI and making sure it is included downstream. We assume that the business will leverage the systems developed in 7023(f)(3) and will include the mechanism to insert the written statement when developing those systems. We anticipate this taking an additional hour of work. We anticipate the system to be fully automated so there will not be ongoing costs. Instead, consumers will provide the written statement, and this will be included automatically with the contested PI.

The universe of affected companies is smaller as this proposed regulation is only concerned with companies that use PI related to health that are not covered by the Health Insurance Portability and Accountability Act (HIPAA). This is a small subset of total companies that are not in the healthcare industry but instead might have health data. For example, companies that have apps related to exercise, diet, or menstrual cycle tracking. As an upper bound estimate, we include all companies from three 6-digit NAICS sectors in California that might plausibly have health PI not covered by HIPAA. These include: 541511 - Custom Computer Programming Services, 713940 - Fitness and Recreational Sports Centers, and 812191 - Diet and Weight Reducing Centers. Additionally, we only include companies with >5 employees as we assume any below this level will not be subject to the CCPA requirements. This approach estimates 4,941 eligible companies.

Costs are approximately:

Costs = [# non-HIPAA businesses under CCPA with health PI] * [cost of adding text on existing response letters to inform consumer option of this option + cost of adding infrastructure to connect downstream data users with consumers 250-word statement]

Costs = 4,941 * (45.57 + 91.14) = 4,941 * (136.71) = **$675,484**

Calculation inputs:

(1) # non-HIPAA businesses under CCPA with health PI [4,941]

(2) cost of updating consumer notification [0.5 hour of software developer time at $91.14/hour]

(3) cost of adding infrastructure to connect downstream data users with consumers 250-word statement levering existing system [1 hour of software developer time at $91.14 hour]

7023(i)

This subsection requires businesses to share the source of incorrect contested PI when they are not the source of the information. Businesses can alternatively inform the source that the information is incorrect and must be corrected. The subsection changes the language from the suggestive “may” to the required “shall.” Total costs can be mitigated with credible evidence of how many companies have already voluntarily adopted these features based on suggestive language.

The proposed regulations will require businesses to track where the PI they use is coming from (assuming they do not collect it themselves). Many businesses might already do this, but for those that assemble different sources and make a unique database this will require updating their systems to flag where PI comes from in the event they need to share their source (or contact the source). With regard to cost, the primary cost will come from identifying the source of the PI. Once the source is identified, the cost of either sharing the source or contacting the source directly is similar and trivial in relation. Again, it is likely that many businesses already know this, but as an upper bound estimate we assume it will take a software developer 40 hours to amend a PI database to include sources of PI.

In addition to identifying where PI comes from, businesses will need to update their communications. However, this cost is likely minimal. This section of the regulatory text already requires businesses to communicate with consumers about their decision to correct PI. Thus, all that will change will be an additional line of text in their communication informing consumers of their source. Businesses can also elect to notify the source of the PI. We assume either process will be automated and will require a software developer an additional hour to develop the system.

Some businesses might never receive PI from other sources and thus would not be affected by this proposed regulation. However, it is difficult to estimate what percent of CCPA businesses do not receive PI from other sources, and thus, as an upper bound estimate we use all businesses covered by CCPA. For purposes of calculating costs, we estimate approximately 35% of businesses are already meeting the proposed regulatory requirements.

Costs are approximately:

Costs = [# businesses covered by CCPA not currently meeting proposed requirements] * [employee time to insert language to existing response letters or communicate to source of PI + cost of internal tracking].

Costs = (52,326 * 0.65) * (91.14 + 3,645.60) =34,011.90* 3,736.74 = **$127,093,627**

Calculation inputs:

(1) # businesses covered by CCPA [52,326]

(2) Subset of (1) that are not currently meeting the proposed regulation [65%]

(3) Update communication structure to consumer or source of PI [1 hour of software developer time at $91.14/hour]

(4) employee time to develop system that tracks source of PI [40 hours of software developer time at $91.14/hour

7023(j), 7024(d)

7023(j) concerns the ability of a consumer to check that specific pieces of inaccurate SPI have been corrected. Businesses shall not disclose the information but should allow consumers to confirm that the SPI it maintains is accurate. The updated regulation moves the language from the suggestive “may” to the required “shall.” In practice, this could look like a form or box on a web interface where a consumer can enter the correct SPI they want to amend, and the business can confirm that is what they have on file. In a non-web-based context, consumers could call the business and the business could respond with either affirmation or denial. In both examples, the business shall not disclose the information but instead only confirm information the consumer has provided.

7024(d) effectively mirrors 7023(j) but instead of concerning a RTC, it is focused on an RTK. Thus, the cost structure to businesses is largely the same. To estimate costs, we must first separate the businesses that have voluntarily become compliant with 7023(j) from the suggestive language. For these businesses, there will only be a small additional cost to become compliant with 7024(d) as they can leverage the system used for 7023(j). For businesses who are not compliant with 7023(j) there will be a larger cost to become compliant with both 7023(j) and 7024(d). We assume these systems will be developed concurrently.

There will be two types of costs associated with this subsection. The first is updating existing communication structures to inform consumers of their new right. Once again, this will be a few lines of text which we anticipate will take a software developer 0.5 hours. The second cost will be creating the mechanism where consumers can ensure the SPI on file is corrected or is the same as what the consumer believes it should be. We anticipate this will take a software developer 40 hours of working time if no system is currently in place. If a RTC system exists, we assume it will take 4 hours to amend the system for RTK.

Only businesses with SPI will be affected by this regulation. However, we are unable to reliably estimate what portion of businesses subject to the CCPA have SPI. As an upper bound estimate, we use all companies subject to the CCPA.

Costs are approximately:

Costs = [# businesses subject to CCPA that are compliant with 7023(j)] * [cost informing consumers + cost amending internal mechanism to confirm information] + [# businesses subject to CCPA that are not compliant with 7023(j)] * [cost informing consumers + cost creating internal mechanism to correct and/or confirm information].

Costs = (52,326 * 0.35) (45.57 + 364.56) + (52,326 * 0.65) (45.57 + 3,645.60) = (18,314.10* 410.13) + (34,011.90* 3,691.17) = **$133,054,867**

Calculation inputs:

(1) # businesses covered by CCPA [52,326]

(2) Subset of (1) that are compliant with 7023(j) [35%]

(3) Amount of time required to add text to website informing consumers. [0.5 hour of software developer time at $91.14/hour]

(4) Cost of generating a platform to confirm information. [40 hour of software developer time at $91.14/hour]

(5) Cost of amending platform to know information [4 hours of software developer time at $91.14/hour]

7025(c)(3), (4), (6)

These subsections require businesses to display the status of an opt-out preference signal (“OOPS”). Subsection (c)(6) sets forth the requirement of displaying the status of the OOPS changing the suggesting “may” to the mandatory “shall,” while subsections (c)(3) and (4) simply reference the requirement to clarify how it is applied in different contexts such as when the OOPS signal conflicts with previous business-specific privacy settings.

In effect, all three updates require the same thing. It would become mandatory to show that the consumer's opt-out request is honored. Businesses have two options in honoring this request. They can either develop this mechanism on their own, or they can rely on a consent management platform to meet this requirement. We assume that companies who work with consent management companies will already use this feature. Also, some portion of companies will have voluntarily adopted this based on the previous round of rulemaking.

For companies that do not provide the signal some portion will elect to use a consent management platform, while others will elect to develop it on their own. Given consent management companies provide a suite of services attributing the additional cost specifically for the opt-out signal will be a challenge. Additionally, it is unlikely companies will choose to work with a consent management company solely for the purpose of these new regulations. For those reasons we only attribute costs to developing the signal interpedently. For companies that must develop the opt-out request on their own we estimate 40 hours of software developer working time.

Costs are approximately:

Costs = [# businesses subject to CCPA who haven't already adopted these toggles] * [additional cost of independent development].

Costs = (52,326 * 0.25) * (3,645.60) = **$47,689,916**

Calculation inputs:

(1) # businesses covered by CCPA [52,326]

(2) Subset of (1) that have no consent management platform or existing toggles [25%]

(3) Cost of adding toggle without consent management platform [40 hours of software developer time at $91.14/hour].

7026(g)

This updated section now requires businesses to display that consumers' request to opt-out of sale/sharing has been processed. In effect, this can be displaying that that the consumer's opt-out request is honored. Complying with section 7025(c)(3) will satisfy this regulation (or vice versa). Thus, the costs are already established under that section.

7027(h)

This updated regulation applies to the request to limit for SPI. Here the language moves from the suggestive "may" to the mandatory "shall" and now requires businesses to provide a means in which consumers can confirm their request has been honored. Although this is similar to subsections 7025(c)(3), (4), (6) and 7026(g), this regulation concerns the RTL versus the RTOO. Therefore, we assume that companies will leverage RTOO systems and will require an additional 4 hours of software developer time.

The universe of affected companies is smaller as only businesses that use or disclose SPI for purposes other than those identified in section 7027(m) will be affected. As discussed above, we are unable to estimate what portion of firms use SPI in this manner, but we assume that firms with consent management platforms will already be compliant which reduces the number of affected businesses. Additionally, some firms may voluntarily be compliant without a consent management platform, but we are unable to separate these estimates. As we assume more businesses currently have consent management platforms than are voluntarily compliant from suggestive language, we use the more liberal assumption to reduce the number of firms.

Costs are approximately:

Costs = [# businesses subject to CCPA with no consent management platform] * [cost of amending opt-out signals to display limit requests].

Costs = (52,326 * 0.25) * (364.56) = **$4,768,992**

Calculation inputs:

(1) # businesses covered by CCPA [52,326]

(2) Subset of (1) that have no consent management platform [25%]

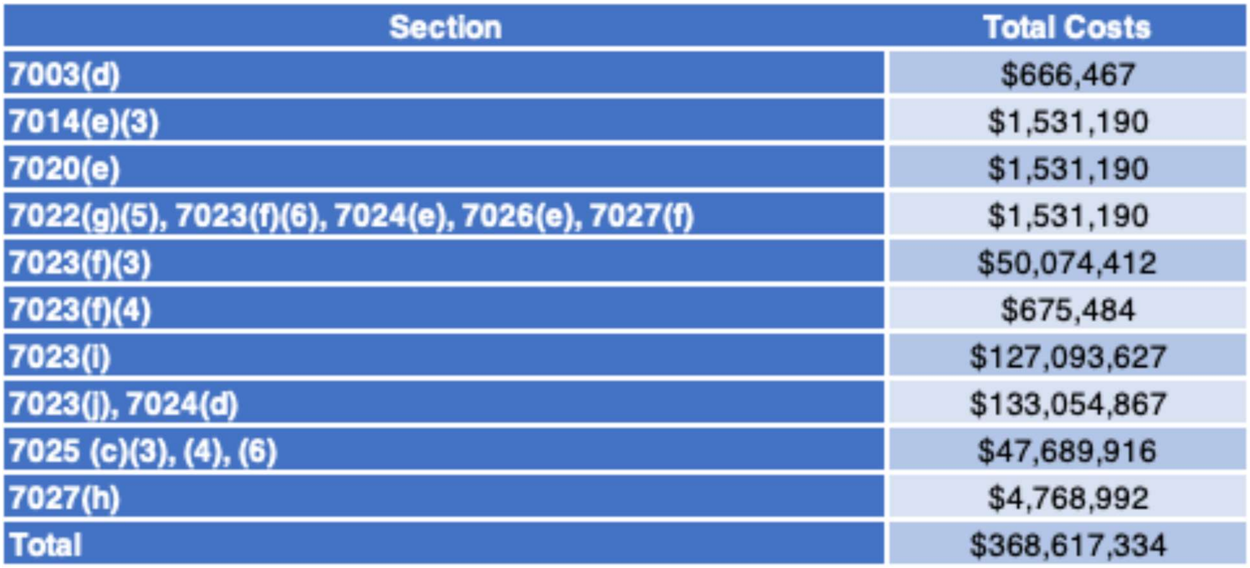
(3) Cost of adding toggle without consent management platform [4 hours of software developer time at $91.14/hour].

7028(a), (c)

This subsection concerns consumers who want to opt-in of sale/sharing of PI after opting-out and amends the regulation to apply also to the RTL. Since businesses are already required to do a two-step process for opting-in after opting-out, the overall system has already been developed and only needs to be amended to apply also to the RTL. Similarly, if a consumer has opted-out and then uses a product or service that requires opting-in, notice must be given. The only change is that this process now applies to businesses that use SPI for purposes other than those set forth in section 7027(m).

Thus, the amended regulation builds on existing systems and the principal costs will be extending the processes to include certain uses and disclosure of SPI. This is quite nuanced because SPI is a subset of PI and thus one might expect businesses who are already complying with the regulation to extend their systems to SPI. Although this updated text now makes the requirement to include SPI explicit, we assume businesses will already be doing this and thus attribute no additional costs here. Total direct year-1 costs are summarized in Table 2-7 below.

Table 2-7: Total Costs of Updates to CCPA Regulations



Section	Total Costs
7003(d)	$666,467
7014(e)(3)	$1,531,190
7020(e)	$1,531,190
7022(g)(5), 7023(f)(6), 7024(e), 7026(e), 7027(f)	$1,531,190
7023(f)(3)	$50,074,412
7023(f)(4)	$675,484
7023(i)	$127,093,627
7023(j), 7024(d)	$133,054,867
7025 (c)(3), (4), (6)	$47,689,916
7027(h)	$4,768,992
Total	$368,617,334

Note: All figures in 2022 $

2.2.2 Proposed CSA Regulations

This proposed rulemaking package contains a number of regulatory deltas. The primary cost of a CSA is having to engage an independent auditor to conduct a thorough, independent CSA. However, we attribute the majority of costs to section 7123(b)(2), which details the 18 components required for the CSA. Estimating the costs of implementing a CSA for a typical firm is challenging for many reasons. Firm size and complexity along with the utilization of existing security frameworks are expected to be primary cost drivers. The large variation in these factors across covered businesses means that CSA costs will be highly heterogeneous. For some firms, certain components listed in 7123(b)(2) will not be applicable (but if not applicable, the cybersecurity audit must document and explain why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security), or the business may already be using a cybersecurity framework to understand and assess how it protects consumers' PI.

For these firms, costs will be lower. For other firms that do not already use a cybersecurity framework to assess how they protect consumers' PI and for whom all 18 components in 7123(b)(2) apply, the costs will be higher. In order to account for these sources of heterogeneity, we first identify the number of affected firms and then define different scenarios that reflect the broad range of firms and requirements needed to comply with the proposed CSA guidelines. Given that the bulk of the costs will derive from section 7123(b)(2), we focus our estimation efforts on this subsection. Although other sections may incur additional costs, we assess these to be trivial relative to the costs associated with 7123(b)(2).

Number of Affected Businesses

To reflect the varying costs and complexities of completing the CSA, we divide businesses by average annual revenue and estimate average compliance costs separately for businesses in each revenue range. While even within revenue ranges there will be variation in costs, we assume that annual revenue is a reasonable proxy for average complexity of CSA implementation.

In total we estimate that 25,167 businesses will be subject to the CSA regulation. We further assume 100% of firms with revenue >$28M process at least 250,000 PI.[23] Taken together, we estimate the coverage by revenue range is:

- <$100M: 18,409
- $100M-1000M: 6,195
- >$1000M: 563

First-Year Direct Costs of Proposed CSA Regulations

As previously discussed, while there are several sections that may have economic costs, we focus on estimating the costs of section 7123(b)(2), which details 18 components that the CSA must identify, assess, and document. While this section outlines core components of the CSA and thus represents the bulk of costs, other sections naturally relate to this section and what is required to complete the CSA. For example, section 7122 contains auditor requirements. On their own, these sections would incur costs, but they ultimately serve to provide guidance for section 7123(b)(2). Thus, we take a holistic approach in what is needed to complete the CSA as prescribed by section 7123(b)(2) and include these additional more minor costs in our overall estimate of hours required to complete the CSA. Given that we are unable to estimate each cost by subsection for each firm in California, we take this more general approach.

Although we are unable to estimate individual firm level costs to complete a CSA, we rely on guidance from industry experts to generalize how firms of different sizes are likely to approach compliance with the proposed regulation. Depending on the firm size and complexity, firms may elect to do the CSA in-house, or they may elect to hire a third-party to complete the audit. Additionally, security frameworks such as SOC 2, ISO 27001, and NIST CSF have some overlap with the proposed CSA requirements, and thus firms that currently utilize these frameworks to assess their cybersecurity programs are expected to have lower compliance costs.

[23] This assumption is based in part on conversations with industry professionals.

To estimate costs, we separate firms by revenue size and assume firms of similar size respond similarly with respect to both how they comply and the extent to which they may already be in partial compliance. Based on discussion with industry sources, for each scenario we have identified the average labor rates and estimated hours needed to complete the 18 core components of the CSA.

Annual Revenue Range: <$100M

For firms in this range, we assume companies are more likely to conduct a CSA in-house rather than to outsource, because their in-house labor rates will be relatively cheaper. Based on conversations with industry experts, we estimate an average in-house salary for employees responsible for implementing a CSA at a firm in this revenue range is approximately $150,000 per year (or $75/hour), and it is estimated to take approximately 750 hours of labor to complete a CSA.

$75/hour x 750 hours = $56,250 per firm to conduct a CSA.

Annual Revenue Range: $100M - $1 billion (sub-Fortune 1000).

Industry sources suggest firms in this range are more likely to outsource CSAs to a boutique firm. Industry guidance suggests the external rate will be about twice what internal staff is paid to account for downtime and profit. This implies a labor rate of approximately $150/hour. Given the large size and increased complexity of firms in this revenue range, the total number of estimated hours increases to 1,000 hours of labor.

$150/hour x 1,000 hours = $150,000 per firm.

Annual Revenue Range: >$1 billion (Fortune 1000 and Fortune 500)

We anticipate these firms will hire the most established and higher cost auditors. Industry experts estimated labor rates of $290/hour for blended rates of partners to associates. Again, given the larger size and increased complexity, the total number of estimated hours increases to 1,250 hours of labor.

$290/hour x 1,250 hours = $362,500 per firm.

Reductions for firms using existing security frameworks to assess their cybersecurity programs

Some firms already use existing security frameworks to assess their cybersecurity programs. While existing frameworks are not a perfect map to the proposed requirements, commonalities across these frameworks could help firms that use these frameworks to mitigate costs of implementing the proposed CSA requirements. In some cases, existing frameworks are used not as the basis of an audit but instead as simply sources of guidance. In other cases, current frameworks allow businesses themselves to determine the audit's scope and objectives. This is different from the proposed regulation, which requires key components to be identified, assessed, and documented by an independent auditor.

We consider four common security frameworks – NIST CSF 2.0, CIS Critical Security Controls v.8, ISO/IEC 27001, and SOC 2, Type II – and for each framework, there is some overlap with the 18 core components of the CSA. To reiterate, these are not perfect matches, and even if a company utilizes a framework to assess its cybersecurity program, that does not guarantee the business's compliance with the proposed CSA requirements. However, the presence of similar security functions and controls indicates there will be some cost mitigation for companies already implementing one of these frameworks to assess its cybersecurity program. Each framework is unique, and the purpose of the frameworks varies. Furthermore, there is no data source detailing how many companies utilize various frameworks.

Instead, we rely on conversations with industry experts to estimate the following share of firms utilizing an existing security framework to assess their cybersecurity programs:

- < $100M revenue: 10% utilize some existing security framework to assess its cybersecurity program
- $100M - $1 billion revenue: 20% utilize some existing security framework to assess its cybersecurity program
- >$ 1 billion revenue: 50% utilize some existing security framework to assess its cybersecurity program

With regard to cost mitigation, we assume that if a company utilizes an existing framework to assess its cybersecurity program, this will result in a 30% reduction in costs to complete the CSA. As a further robustness check, we offer two additional scenarios below that model a 10% and 50% reduction in costs. In total, the cost reduction would be:

% of firms using existing security framework to assess its cybersecurity program x 70% of per firm cost in each revenue bracket.

This would ultimately produce the following first year cost estimates for the proposed rulemaking:

<$100M revenue

- $56,250 per firm not using an existing security framework to assess its cybersecurity program (90% of firms)
- $39,375 per firm using existing security framework to assess its cybersecurity program (10% of firms).

$100M - $1 billion revenue

- $150,000 per firm not using an existing security framework to assess its cybersecurity program (80% of firms)
- $105,000 per firm with existing security framework to assess its cybersecurity program (20% of firms)

>$1 billion revenue

- $362,500 per firm not using an existing security framework to assess its cybersecurity program (50% of firms)
- $253,750 per firm using an existing security framework to assess its cybersecurity program (50% of firms).

Taken together, we have the following cost estimates:

Firms with <$100M Annual Revenue:

Costs = [# of businesses subject to CSA with revenue below $100M and not using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue below $100M and not using an existing security framework to assess its cybersecurity program] + [# of businesses subject to CSA with revenue below $100M and using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue below $100M and using an existing security framework to assess its cybersecurity program]

Calculation inputs:

1. # of businesses subject to CSA with revenue <$100M and not using an existing security framework to assess its cybersecurity program [16,568]
2. Cost of completing CSA with revenue <$100M and not using an existing security framework to assess its cybersecurity program [$56,250]
3. # of businesses subject to CSA with revenue <$100M and using an existing security framework to assess its cybersecurity program [1,841]
4. Cost of completing CSA with revenue <$100M and using an existing security framework to assess its cybersecurity program [$39,375]

Firms with $100M – $1B Annual Revenue:

Costs = [# of businesses subject to CSA with revenue between $100M and $1B and not using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue between $100M and $1B and not using an existing security framework to assess its cybersecurity program] + [# of businesses subject to CSA with revenue between $100M and $1B and using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue between $100M and $1B and using an existing security framework to assess its cybersecurity program]

Calculation inputs:

1. # of businesses subject to CSA with revenue $100M – $1B and not using an existing security framework to assess its cybersecurity program [4,956]
2. Cost of completing CSA with revenue $100M – $1B and not using an existing security framework to assess its cybersecurity program [$150,000]
3. # of businesses subject to CSA with revenue $100M – $1B and using an existing security framework to assess its cybersecurity program [1,239]
4. Cost of completing CSA with revenue $100M – $1B and using an existing security framework to assess its cybersecurity program [$105,000]

Firms with >$1B Annual Revenue:

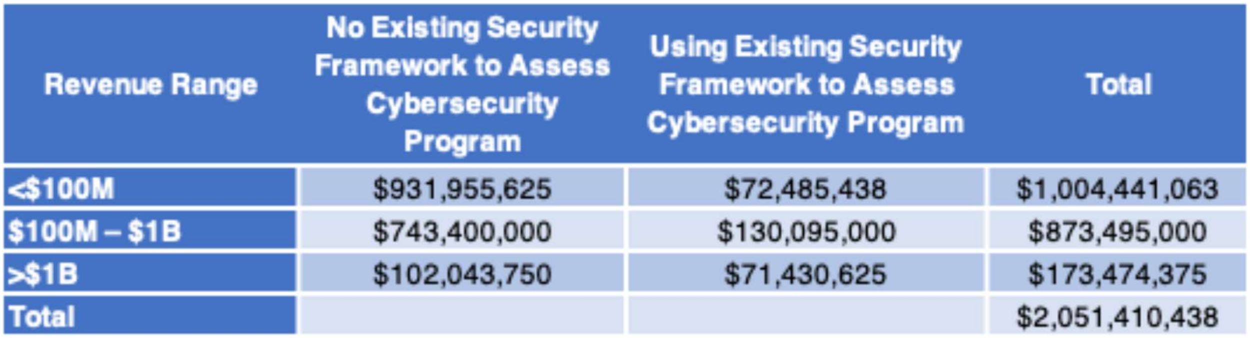
Costs = [# of businesses subject to CSA with revenue above $1B and not using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue above $1B and not using an existing security framework to assess its cybersecurity program] + [# of businesses subject to CSA with revenue above $1B and using an existing security framework to assess its cybersecurity program] * [cost of completing CSA with revenue above $1B and using an existing security framework to assess its cybersecurity program]

Calculation inputs:

1. # of businesses subject to CSA with >$1B and not using an existing security framework to assess its cybersecurity program [281.5]
2. Cost of completing CSA with revenue >$1B and not using a security framework to assess its cybersecurity program [$362,500]
3. # of businesses subject to CSA with revenue >$1B and using an existing security framework to assess its cybersecurity program [281.5]
4. Cost of completing CSA with revenue >$1B and using an existing security framework to assess its cybersecurity program [$253,750]

In total, this yields the following first-year direct cost estimates as shown in Table 2-8:

Table 2-8: First-Year CSA Direct Cost Estimates (Proposed Regulations Scenario 30% Reduction)



Revenue Range	No Existing Security Framework to Assess Cybersecurity Program	Using Existing Security Framework to Assess Cybersecurity Program	Total
<$100M	$931,955,625	$72,485,438	$1,004,441,063
$100M – $1B	$743,400,000	$130,095,000	$873,495,000
>$1B	$102,043,750	$71,430,625	$173,474,375
Total			$2,051,410,438

Note: All figures in 2022 $

Ongoing Costs of Proposed CSA Regulations

The proposed regulations require CSAs to be repeated with subsequent audits completed each calendar year. Thus, there will be ongoing costs. We assume the majority of costs will be incurred in the first year of the regulation as firms develop the infrastructure to implement the proposed requirements. In subsequent years costs should fall drastically as the system of the audit will have been developed and can be repeated. Furthermore, once the regulation becomes law, new firms or services from existing firms will likely emerge to focus on assisting companies in complying with the proposed CSA requirements. Both of these will decrease costs in following years.

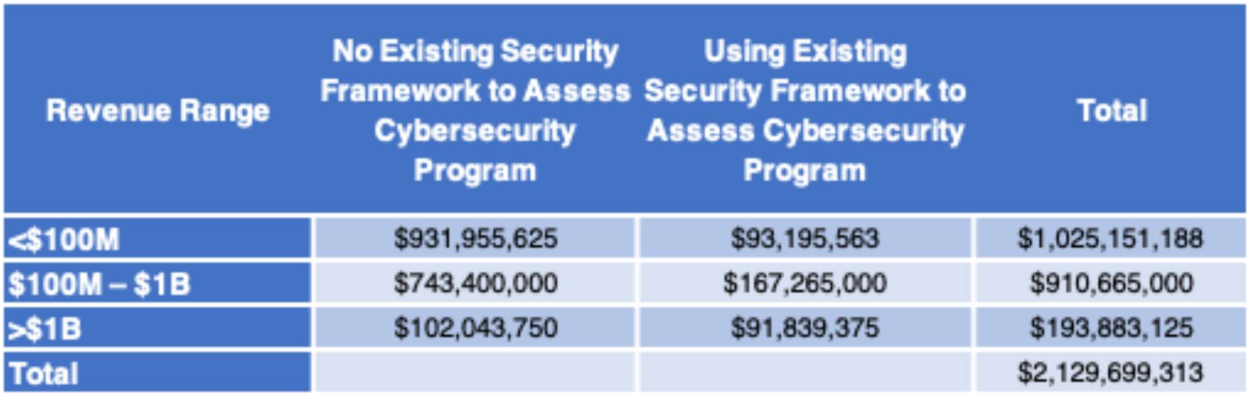
Based on these assumptions we model a gradually declining cost structure based on other security frameworks that see a reduction in costs in following years to recertify an audit. We estimate that subsequent audits will represent 15 – 30% of total year one compliance costs, with the higher compliance cost threshold occurring in earlier years before gradually falling.

This would suggest a range between **$615,423,131** and **$307,711,566** in following years.

Additional Security Framework Cost Reduction Scenarios

We model two additional cost reduction scenarios for businesses with existing security framework to assess their cybersecurity program. We model a 10% and 50% reduction in costs. Total costs are overall similar as costs are primarily driven by firms with under $100M in revenue and we assume that only 10% of these firms have a security framework. Table 2-9 shows the 10% reduction in cost and Table 2-10 shows the 50% reduction.

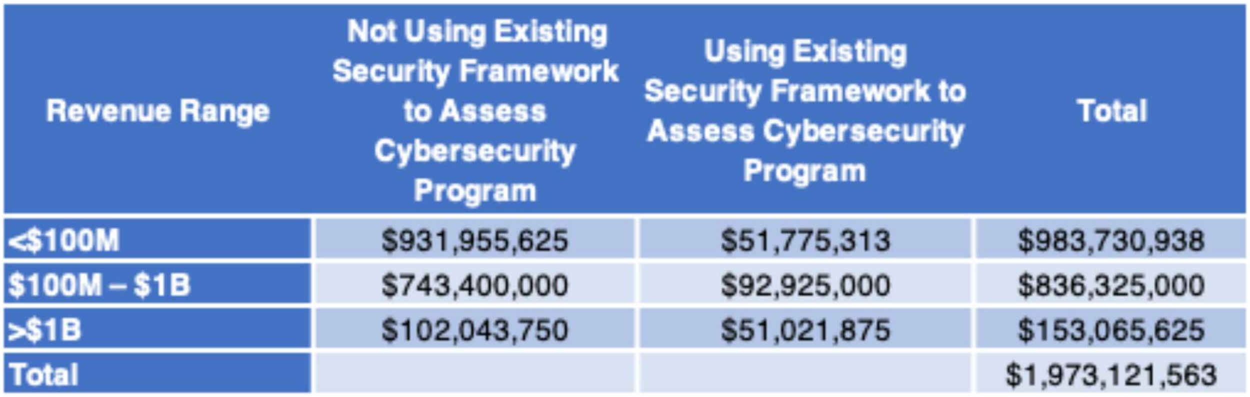
Table 2-9: First Year CSA Direct Cost Estimates (Proposed Regulations Scenario 10% Reduction)



Revenue Range	No Existing Security Framework to Assess Cybersecurity Program	Using Existing Security Framework to Assess Cybersecurity Program	Total
<$100M	$931,955,625	$93,195,563	$1,025,151,188
$100M – $1B	$743,400,000	$167,265,000	$910,665,000
>$1B	$102,043,750	$91,839,375	$193,883,125
Total			$2,129,699,313

Note: All figures in 2022 $

Table 2-10: First-Year CSA Direct Cost Estimates (Alternative Scenario 50% Reduction)



Revenue Range	Not Using Existing Security Framework to Assess Cybersecurity Program	Using Existing Security Framework to Assess Cybersecurity Program	Total
<$100M	$931,955,625	$51,775,313	$983,730,938
$100M – $1B	$743,400,000	$92,925,000	$836,325,000
>$1B	$102,043,750	$51,021,875	$153,065,625
Total			$1,973,121,563

Note: All figures in 2022 $

2.2.3 Proposed RA and ADMT Regulations

Risk Assessment Baseline

The proposed requirements for RA and ADMT are part of a large rulemaking package with many new requirements. However, we anticipate overall costs for these rules to be comparatively low compared to the other rulemaking given many of the requirements described in the proposed regulation were already required by existing laws, such as existing requirements under the CCPA and other state privacy laws.

Risk Assessment

The primary cost of an RA is having to conduct an RA for each processing activity—or comparable set of processing activities—that triggers the RA requirements and having to submit abridged RAs. We attribute the majority of initial costs for RAs to sections 7152 and 7154. However, as we discuss below, most of these costs should have already been borne by companies in order to comply with existing law while the incremental requirements being proposed are relatively limited.

These sections include:

- Section 7152. RA Requirements: This section establishes the requirements that businesses must conduct the RA. Of particular importance are subsections 7152(a)(4), 7152(a)(5), and 7152(a)(6). These subsections require businesses to identify and quantify certain benefits to processing consumers' PI, as applicable and when possible, along with safeguards to address negative impacts of processing PI. Associated costs are driven by labor costs of conducting the RAs.
- Section 7154. Prohibition on Processing: Requires businesses to consider the benefits of processing PI versus the risks to consumers' privacy and, in the event the costs outweigh benefits, would prohibit the business from processing PI. In addition to labor costs associated with implementation, costs associated with this subsection could also potentially include lost revenue from not processing PI.

However, costs associated with these subsections will be heavily mitigated by existing legal requirements that already necessitate key elements of the proposed requirements. For Section 7152, businesses will not be conducting a full cost-benefit analysis from nothing, but instead can leverage existing business practices as well as systems they use to comply with existing law (e.g., federal and state laws prohibiting unfair acts and practices and the existing CCPA regulations). For example, to comply with laws prohibiting unfair acts and practices, businesses implicitly need to identify the benefits of a given activity and conclude that their practices do not cause significant harm to consumers that is not outweighed by countervailing benefits. In addition, in practice, businesses already know precisely what PI is being used for and what the benefits of its processing are to the business. This is an implicit requirement under unfair trade practices law. Moreover, section 7002 of the existing regulations already requires businesses to consider negative impacts to consumers and the existence of safeguards. Because many of the inputs to the proposed RA regulation are already required (implicitly or otherwise) to be collected, the bulk of costs for section 7152 are largely organizational and record-keeping based.

For section 7154, the prohibition on processing would initially suggest a loss of revenue attributed to the regulation, but again this should more accurately be attributed to existing legal requirements. Namely, US federal and state laws prohibit unfair trade practices. Conducting an activity where the risks to consumers privacy outweigh the benefits would be considered an unfair trade practice. We assume that all businesses are complying with existing laws, and therefore we assess no costs associated with the value from lost data collection.

Next, we discuss the subsections that will incur incremental regulatory costs not attributable to existing statute.

Number of Affected Businesses

We estimate the number of affected businesses using a scenario analysis with low, medium, and high proportions of CCPA covered businesses meeting the requirements to be covered by the proposed RA and ADMT rules. These estimates are 25%, 50%, and 100%, which correspond to 13,082, 26,163, and 52,326 businesses, respectively.

First-Year Direct Costs of Proposed RA Regulations

As previously discussed, all costs attributed to the regulation are organizational and record based. The vast majority of costs can be attributed to section 7152. Although minor costs may be associated with other sections such as 7050(g), 7151, 7155(b) and (c), or 7157, we incorporate these costs into the overall hourly cost, which is dictated by 7152. This approach is consistent with the CSA cost analysis where the majority of costs can be attributed to one section.

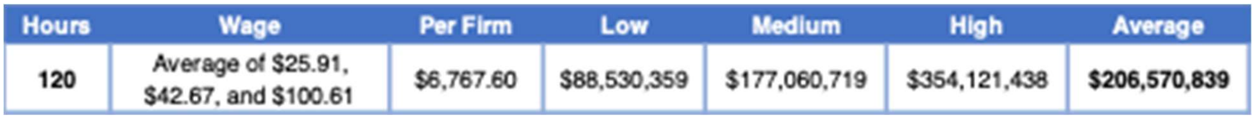
Given that the elements of the RA requirements that are attributable to the proposed regulation include only organization of information that was already required by existing law to be collected, we assume that the incremental requirements attributable to the proposed regulation will be completed by a range of positions including clerical, compliance officers, lawyers, and executives. We have no way of estimating the relative portions of work that will be completed by each position, so we use the average wage across each position minus executives who overall will represent a small portion of estimated hours. Wage data comes from the Occupational Employment and Wage Statistics (OEWS) program of the EDD. OEWS estimates an hourly wage of $25.91 for office and administrative support occupations, $42.67 for compliance officers, and $100.61 for lawyers in Q1 2023. The yields a blended hourly rate of approximately $56.40.

While complete RAs are typically months-long processes involving multiple employees, only a portion of costs should be ascribed to the regulation. As we have noted above, the quantification of certain benefits and negative impacts to consumers should already be considered by businesses. Therefore, the only costs that should be attributed are organizational. Finally, it should be noted that firms might need to complete multiple RAs. We make no assumptions here about the number of RAs needed per firm but propose the bulk of costs would be attributed to completing the first RA. In communication with industry sources, we estimate 120 hours needed to complete the organizational and regulatory requirements.

This yields the compliance cost estimate of $6,768 per firm. This smaller number reflects the regulatory delta. Attributing costs to the full RA would be significantly higher, but that is not what is tasked here. The majority of costs for an RA are mitigated by the baseline, which is why our modeled costs are lower. Total costs range between **$89 million** to **$354 million** depending on the scenario as shown in Table 2-11 below. Given the uncertainty, we present the average across the three scenarios of **$207 million** as our primary point estimate for first-year direct costs of RA requirements. This estimate is used as the input into the macroeconomics model.

Note that firms subject to GDPR or Colorado's Privacy law already face largely similar requirements as the proposed regulations. Although there is not a perfect overlap between what is required by different jurisdictions, we assume that complying with GDPR or Colorado law will mitigate some of these costs. Rather than make an assumption about what portion of costs are mitigated we assume all businesses will face the same cost structure.

Table 2-11: RA First-Year Cost Estimates



Hours	Wage	Per Firm	Low	Medium	High	Average
120	Average of $25.91, $42.67, and $100.61	$6,767.60	$88,530,359	$177,060,719	$354,121,438	$206,570,839

Note: All figures in 2022 $

Ongoing Direct Costs of Proposed RA Regulations

The proposed regulation introduces ongoing cost requirements associated with section 7155(a). Of particular importance are sections 7155(a)(2), which requires businesses to review and update the RA every three years, and section 7152(a)(3), which requires businesses to update the RA if there is a material change.[24] We have no way of reliably estimating how many businesses will have material changes to their use of PI, so instead we assume that businesses will review their RA annually, which would simultaneously fulfill both requirements. Some businesses will have no changes, while others with a material change must assess new risks and submit a new abridged RA. We estimate that subsequent RAs—including both new RAs for new PI-processing, as well as reviews and updates to existing PI-processing—will represent 15–30% of total year one compliance costs, with the higher compliance cost threshold occurring in earlier years before gradually falling.

Using the average direct cost estimate this would suggest a range between **$61,971,252** and **$30,985,626** in subsequent years.

ADMT Baseline

The proposed ADMT regulations may initially appear to be proposing a collection of new requirements entirely attributable to the proposed regulations because they cover a new technology that is not part of the existing regulations nor explicitly covered by statute.

[24] 7152(a)(1) is incorporated in our total direct cost estimate.

However, our analysis of the proposed rulemaking suggests that some of the costs are associated with statutory requirements.

Subsections 7201, 7220, 7221, and 7222 are responsible for the bulk of costs. While other subsections might have small associated costs, much of these constitute incremental changes beyond existing baseline requirements.[25] We estimate that the costs of these other subsections are trivial compared to the larger subsections, and we thus assume estimation of the more significant compliance costs will incorporate these smaller costs.

Section 7201

This section adds requirements for businesses using physical or biological profiling for a significant decision or extensive profiling. Subsection 7201(a)(1) requires businesses to either conduct an evaluation of the physical or biological identification or profiling technology to ensure it works as intended and does not discriminate, or if the business obtained the technology from another person, review that person's evaluation, including any relevant requirements or limitations. Subsection 7201(a)(2) requires businesses to implement policies, procedures, and training to ensure that the physical or biological identification or profiling technology works as intended for the business's proposed use and does not discriminate.

Both of these subsections will incur regulatory costs to businesses, although for businesses complying with regulations from other jurisdictions, some costs may be mitigated. For example, businesses subject to the Colorado AI Act are already required to manage risks of discrimination. Additionally, businesses that use generative artificial intelligence (GenAI) and act as contractors for the state of California face additional compliance requirements from the state of California that will require similar information to be identified. Finally, section 7002 of the existing regulations requires businesses to already consider negative impacts to consumers and relevant safeguards, which would be something a business could leverage in complying with the proposed regulations.

All of these existing activities associated with other legal requirements will help mitigate costs but will not fully absorb costs. We are unable to estimate the number of businesses using ADMT that will be subject to the Colorado AI Act, or what portion of them use GenAI when doing work for the state of California. Furthermore, Section 7002 mitigates costs associated with complying with proposed regulation 7201 but does not address testing the algorithms in the first place. Therefore, businesses will still incur costs here associated with the proposed regulation that we include in our total estimate discussed below.

[25] For example, 7011(e)(2)(F)-(G), (e)(3)(E) is only adding language to existing notifications.

Section 7220

This section adds pre-use notice requirements for ADMT. Specifically, subsection 7220(a) requires that businesses that use ADMT for significant decisions, extensive profiling, or training uses provide a pre-use notice. Subsections 7220(b)-(c) provide the requirements for how a Pre-use Notice must be provided and what must be included in the notice. Subsection 7220(d) allows a business to consolidate its Pre-use Notices in different ways (e.g., single ADMT for multiple purposes).

Much like section 7201, these subsections will incur regulatory costs but will have some cost mitigants for businesses complying with other laws. Businesses subject to the Colorado AI Act and/or that use GenAI, must comply with similar provisions but not all costs will be covered (or all businesses). Overall costs for this section will be lower compared to other sections as costs are primarily notification based.

Section 7221

This section adds requirements for how consumers are able to opt-out of the businesses' use of ADMT. We focus only on the subsections that will incur costs. Subsection 7221(a) states that businesses must provide consumers with the ability to opt-out of the uses of ADMT set forth in section 7200 (i.e., for significant decisions, extensive profiling, or training uses). Subsection 7221(c) requires that businesses provide two or more methods for submitting opt-out of ADMT requests. At least one method must reflect the manner in which the business primarily interacts with the consumer. Subsection 7221(d) requires that methods for submitting requests to opt-out of ADMT must be easy to execute, require minimal steps, and comply with subsection 7004. 7221(g) requires that a business can deny a request that it has a good-faith, reasonable, and documented belief is fraudulent, and inform the requestor that it will not comply with the request and provide an explanation of why it believes the request is fraudulent. Subsection 7221(h) requires that the business provide a means by which the consumer can confirm that their opt-out of ADMT request has been processed. Subsection 7221(j) allows a consumer to submit requests using an authorized agent if the consumer provides signed permission to the agent. It also allows a business to deny an authorized agent's request if the agent does not provide the signed permission to the business. Subsection 7221(k) requires that businesses wait at least 12 months before asking consumers that opted out of ADMT to consent to the business's use of that ADMT. Subsection 7221(m) states that when a consumer has opted out of ADMT before the business initiated the processing, the business must not initiate processing of the consumer's PI using that ADMT. Subsection 7221(n) states that if a consumer submitted an opt-out of ADMT request after the business-initiated processing, the business must: (n)(1): Cease processing the consumer's PI using that ADMT as soon as possible, and no later than 15 days. The business must not use nor retain any PI previously processed by that ADMT; and (n)(2): Notify all other persons to whom the business disclosed information using that ADMT that the consumer has opted out and instructing them to comply with the opt-out within the same time frame.

The cost structure of these subsections is largely the same. The proposed implementation of the right to opt-out of ADMT mirrors what is in the statute or existing regulations with respect to other CCPA rights and is now extended to ADMT. Therefore, businesses will already have created the structures or systems but will now need to extend them to ADMT. For example, subsection 7221(c) requires businesses provide two or more methods for submitting opt-out of ADMT requests. Businesses subject to CCPA already must comply with these requirements for existing CCPA rights (e.g., the right to opt-out of sale/sharing). Thus, the operational system to opt-out of sale/sharing of PI has already been created, and these costs are attributed to the baseline. The only additional costs attributable to the regulation will be extending that existing structure to uses of ADMT. That being said, although the structure for these operational systems exists for analogous CCPA rights, there will be multiple hours of software developer time needed to leverage these systems for uses of ADMT.

Section 7222

This section focuses on requests to access information about a business's use of ADMT. Again, we highlight only the subsections that will incur costs. Subsection 7222(a) states that businesses must provide consumers with the ability to access information about their use of ADMT for significant decisions and extensive profiling. Subsection 7222(b) identifies what must be provided in response to a request to access ADMT.[26] Subsection 7222(e) states that if a business denies a verified access request because of a conflict with other laws or an exception to the CCPA, the business must inform the requestor and explain the basis of the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer. Subsection 7222(h) requires that service providers or contractors provide assistance to businesses in responding to access to ADMT requests, including by providing PI in their possession or enabling businesses to access that information. Subsection 7222(k) requires that additional notice requirements apply when a business uses ADMT to make an adverse significant decision. The business must provide the consumer with notice of their access ADMT right within 15 days of the adverse significant decision, specifically that: the business used ADMT to make a significant decision about them; the business cannot retaliate against them for exercising their CCPA rights; the consumer has the right to access ADMT and how they can exercise that right; and if the business is relying on the human appeal exception, how to appeal the decision.

Much like section 7220, the majority of costs in this section are notification based, and in many instances can leverage existing notification systems required by previous rounds of rulemaking. Furthermore, for subsection 7222(b) costs can be mitigated partially for companies subject to the Colorado AI Act and/or that use GenAI as a state contractor. Although overall costs are lower compared to sections 7201 and 7221, there will be

[26] Subsections 7222(b)(1) – 7222(b)(5) provide the specific details – each of which would have varying degrees of cost.

significant hours needed to update notification systems, and we include these hours in our overall hourly estimate.

Number of Affected Businesses

We estimate the number of affected businesses using a scenario analysis with low, medium, and high proportions of CCPA covered businesses meeting the requirements to be covered by the proposed ADMT rules. These estimates are 25%, 50%, and 100%, which correspond to 13,082, 26,163, and 52,326 businesses respectively.

First-Year Direct Costs of Proposed ADMT Regulations

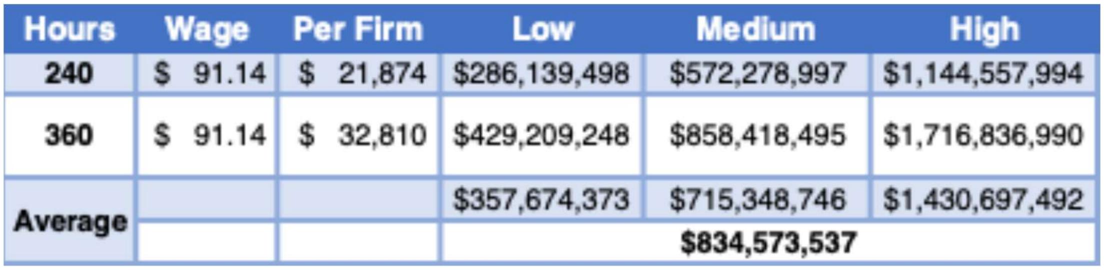
The ADMT rulemaking presents a unique challenge for estimating costs attributable to the proposed regulation, because although much of the rulemaking is novel, many of the subsections build on existing requirements. Realistically, businesses will tackle the entire regulatory package at once to become complaint, but being able to accurately disaggregate compliance costs attributable to the regulation from compliance costs attributable to statute and existing regulations is not feasible. Furthermore, some portion of companies who are subject to the Colorado AI Act or use GenAI as a state contractor will already be undergoing some of the requirements presented here.

Therefore, much like our estimation strategy for the CSA rulemaking, we model the total costs of compliance as a single estimate instead of considering each regulatory delta. We estimate conservatively that it will take a business approximately one quarter to meet the compliance requirements associated with the regulatory deltas. We reiterate that while overall costs would be higher when considering the total effort required to bring a business into compliance, not all these costs are attributable to the proposed regulation. As discussed above, many costs are attributable to previous rounds of rulemaking, which will allow companies to build on existing systems. Compliance estimates come from our own understanding of the regulatory delta and how it relates to the other hourly estimates we derived from industry experts on the RA and CSA regulations.[27]

Using the software developer hourly rate of $91.14, this corresponds to $21,874 to $32,810 in first-year direct compliance costs per business. Using the number of estimated firms from our scenario analysis this gives the following low, medium, and high total cost estimates as shown in Table 2-12. Once again, given the uncertainty, we present the average across the three scenarios of **$835 million** as our primary point estimate for first-year direct costs of ADMT requirements. This estimate is used as the input into the macroeconomics model.

[27] Based on 4 – 6 hours per day for 60 working days.

Table 2-12: ADMT First-Year Direct Cost Estimates



Hours	Wage	Per Firm	Low	Medium	High
240	$ 91.14	$ 21,874	$286,139,498	$572,278,997	$1,144,557,994
360	$ 91.14	$ 32,810	$429,209,248	$858,418,495	$1,716,836,990
Average			$357,674,373	$715,348,746	$1,430,697,492
				$834,573,537	

Note: All figures in 2022 $

Ongoing Direct Costs of Proposed ADMT Regulations

Modeling the ongoing direct costs of the ADMT rulemaking is challenging. There will certainly be ongoing costs as either new businesses enter the market that use ADMT or existing businesses introduce or add additional ADMT to their operation. However, there is no way to estimate how ADMT use will increase with businesses overtime. While it is likely that its use will increase rapidly over the next several years, at the same time there will also be new regulations introduced that would mitigate the costs attributable to the proposed regulations.

Given the large amount of uncertainty, we use the similar ongoing cost estimation strategy as other parts of this regulatory package. We estimate that subsequent years will represent 15% – 30% of total year one compliance costs, with the higher compliance cost threshold occurring in earlier years before gradually falling. As more jurisdictions enact laws regulating ADMT the smaller ongoing impact reflects a larger portion of costs being mitigated. Using the average direct cost estimate across all thresholds, this would suggest a range between **$250,372,061** and **$125,186,031** in subsequent years.

2.2.4 Total Costs

Combining the cost estimates for CCPA updates, CSA, ADMT, and RA described in Section 2.4, we estimate total costs for the proposed regulations to be **$3.5 billion** in the first year and to average **$1.0 billion** across the first ten years following implementation. Estimated initial costs for a typical business range from $7,045 to $122,666. The estimated ongoing costs for a typical business are $26,015.

First-year total costs are comprised of approximately $369M in costs associated with updates to CCPA regulations, $2.0B in costs associated with CSA, $207M in costs associated with RA, and $835M in costs associated with ADMT. While CCPA updates do not have estimated ongoing costs, there are ongoing annual costs associated with each of other elements including CSA (estimated range of $308M-$615M per year), RA (estimated range of $31M–$62M per year), and ADMT (estimated range of $125-$250M per year).

3 Benefits

Numerous types of benefits flow to individuals in California from the enactment of the CCPA and CPRA legislation. Similarly, a wide variety of benefits flow to both California businesses and consumers from proposed regulations that further implement those laws. Covered businesses are expected to strengthen their protection of consumer PI as well as more effectively enable consumers to exercise their privacy rights. The protection of consumer PI and the ability of consumers to manage uses of their PI are relatively new features of the California economy with limited sources of data and methods available to quantify the expected benefits of proposed regulations.

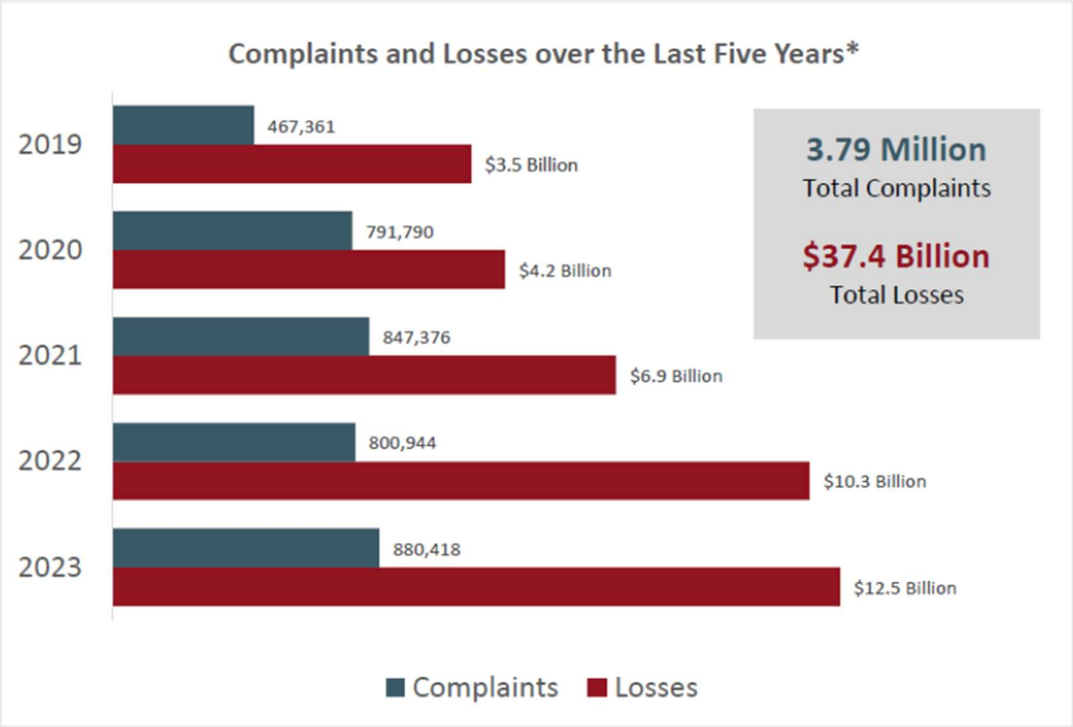
The vast majority of expected benefits from the proposed regulations cannot be quantified, so this SRIA contains an extensive discussion of unquantified benefits expected to accrue to both businesses and individuals. Some of these unquantified or qualitative benefits include improvements to the health, safety, welfare, and quality of life for California individuals. Recognizing the heterogeneity or diversity of businesses impacted and the uncertainties regarding a potentially wide range of long-term responses to proposed new requirements, many unquantified benefits will be incurred by California businesses as well. The assessment of regulatory benefits begins with assessment of a narrow set of benefits that can be quantified and are expected to result from reductions in the risk of cybercrimes against firms in California with linkages to the protection of consumer PI.

3.1 Quantitative Benefits

Quantified Benefits of Proposed Regulations - Cybersecurity Risks

In recent years, cybercrimes have steadily risen and have led to billions of dollars in annual economic losses in California and the United States. According to the most recent Internet Crime Report, the Federal Bureau of Investigation (FBI) received 3.79 million complaints (average of 758,000 complaints per year) during the period of 2019-2023. The total amount of monetary losses to businesses and individuals associated with these complaints was $37.4 billion, as shown in Figure 3-1 below.

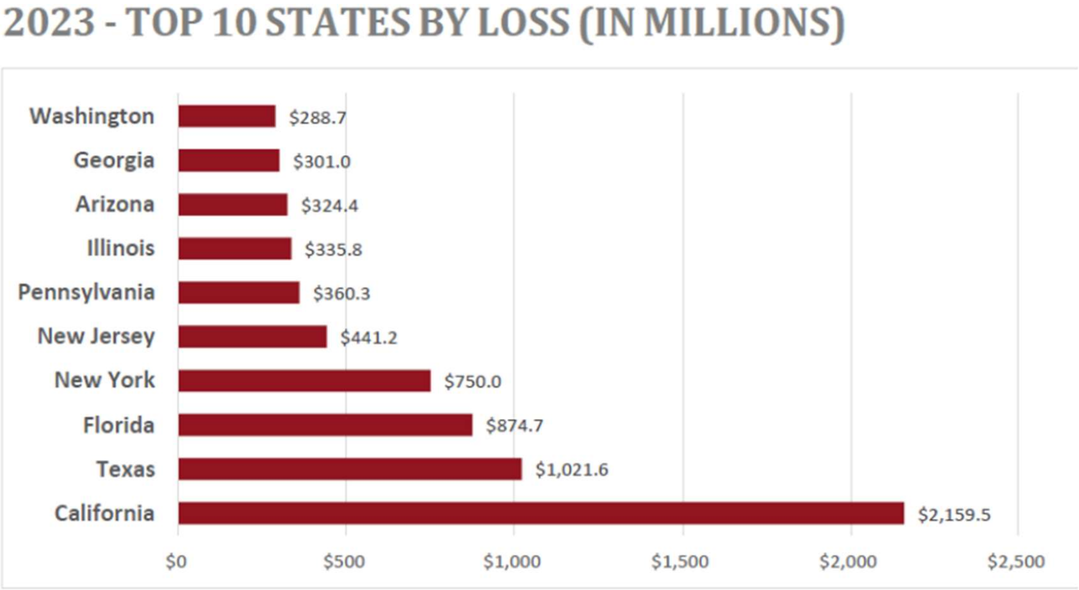
Figure 3-1: Complaints and Losses over the Last Five Years Reported by FBI



Source: FBI 2023 Internet Crime Complaint Center (IC3) Report

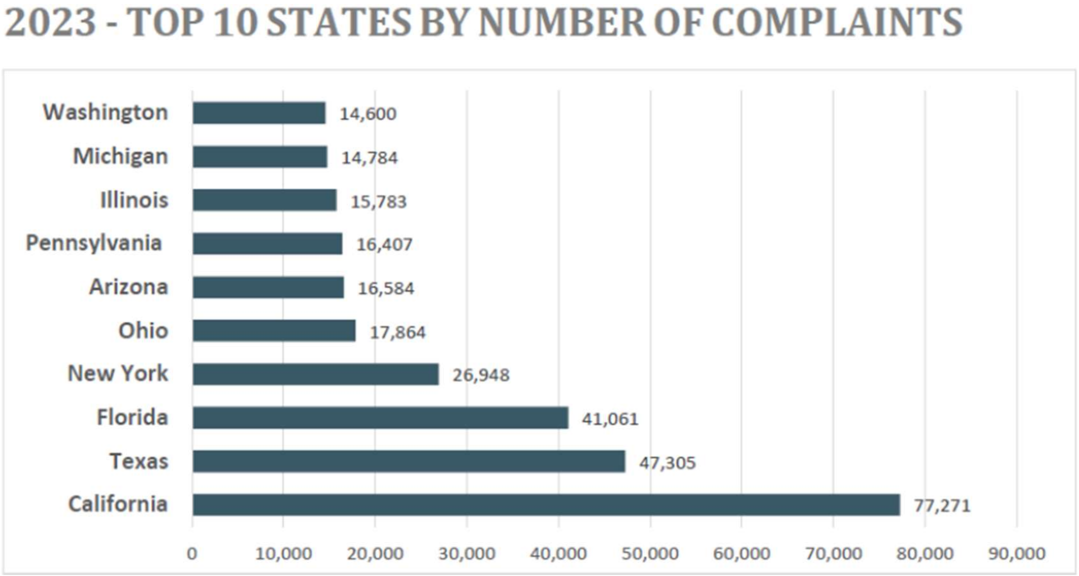
Among all states, California persistently has the largest amount of victim complaints and victim losses caused by internet crimes or cybercrimes. In 2023, for example, victim losses in California were nearly $2.2 billion, more than doubling the losses in the second highest state, Texas (Figure 3-2). The number of victim complaints was 77,271 in California in 2023, close to twice the amount of complaints in the next highest state (Figure 3-3).

Figure 3-2: Top Ten States by Victim Loss Caused by Cybercrimes in 2023



Source: FBI 2023 IC3 Report

Figure 3-3: Top Ten States by Number of Victim Complaints Caused by Cybercrimes in 2023



Source: FBI 2023 IC3 Report

The extremely high volume of cybercrimes in California and the consistently increasing level of monetary losses due to those crimes suggest the importance and necessity of taking steps to mitigate the negative effects caused by cybercrimes. The proposed regulations are anticipated to bring substantial benefits to California businesses and consumers, including by setting requirements in three areas: CSA, RA, and ADMT. The beneficial impact of the updates to the existing CCPA regulations, and the regulations on ADMT are difficult to quantify, and will be discussed in the unquantified benefits section. This section focuses on the quantifiable beneficial impacts of California businesses conducting CSAs and RAs.

Beneficial Impacts of Cybersecurity Audits ("CSAs")

Under the proposed regulations, CSAs are the annual audits that every CCPA covered business whose processing of consumers' PI presents significant risk to consumers' security as set forth in Section 7120, subsection (b), is required to complete. CSAs assess and document how the business's cybersecurity program protects PI from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activities that can result in the loss of availability of PI. CSAs identify and address gaps or weaknesses in the business's cybersecurity program.

The proposed regulations require certain California businesses to conduct CSAs to identify, assess, and document measures to protect privacy, including, but not limited to, multi-factor authentication, strong unique passwords or passphrases, encryption of PI, account management, and access controls. These regulations also require CSAs to identify, assess, and document internal and external vulnerability scans, penetration testing, vulnerability disclosure and reporting, and network monitoring and defenses, including the deployment of:

1. Bot-detection and intrusion-detection and intrusion-prevention systems; and
2. Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of PI).

The importance of cybersecurity awareness, education, and training is also addressed within the proposed regulations. CSAs require the identification, assessment, and documentation of training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system. The identification, assessment, and documentation of such awareness, education, and training must include how the business maintains current knowledge of changing cybersecurity threats and countermeasures.

In addition, CSAs must identify, assess, and document how the business manages its response to security incidents; how the business tests its incident-response capabilities; and the business's continuity and disaster-recovery plans, including data-recovery capabilities and backups. CSAs must also document the business's plan to address the gaps and weaknesses identified, including the resources it has allocated to resolve them and the timeframe in which it will resolve them.

Both academic studies and private CSA practitioners have provided supporting evidence for the effectiveness of the above proposed CSA regulations in reducing potential monetary losses caused by cybercrimes. Steinbart et al. (2018) is an empirical study finding a relationship between CSAs and actual cybersecurity outcomes. As it points out, “Given the increasing financial impact of cybercrime, it has become critical for companies to manage information security risk. The practitioner literature has long argued that the internal audit function (IAF) can play an important role both in providing assurance with respect to information security and in generating insights about how to improve the organization's information security.”

This study empirically supports that the quality of the relationship between internal audit and information security (which will be improved through the identification, assessment, and documentation requirements of CSAs) has a positive effect on the number of reported internal control weaknesses and incidents of noncompliance, as well as on the numbers of security incidents detected, both before and after they caused material harm to the organization. Proper identification, assessment, and documentation of cybersecurity risks and problems required by CSAs will help with early detection and reporting of internal control weaknesses and incidents of noncompliance and hence lead to reduction of cybercrimes. As the authors point out, “It is important to detect and subsequently correct internal control weaknesses because they represent vulnerabilities that criminals can exploit.” Without CSAs, businesses may not be able to detect internal control weaknesses in time, and therefore cannot correct them in time to avoid losses.

In addition, the authors find that higher levels of management support for information security and having the chief information security officer (CISO) report independently of the IT function have a positive effect on the quality of the relationship between the internal audit and information security functions and information security outcomes. CSA regulations require organizational independence for the auditor; require the documentation of when assessments of the business’s cybersecurity program are reported to the business’s board, governing body, or—if neither of those exists—to the business’s highest-ranking executive responsible for the program; and require a member of the board, governing body, or—if neither of those exists—the business’s highest-ranking executive responsible for oversight of the business’s CSA compliance to certify that the business completed its CSA as set forth in the proposed regulations. These requirements can lead to more effective detection of internal control weaknesses and further reduce the financial impact of cybercrimes.

Additional evidence for CSAs’ effectiveness in reducing losses is provided by industry experts conducting cybersecurity assessments and audits. When industry experts were asked, “For firms that have conducted an assessment or an audit, are they more likely to detect these major breaches and be able to manage them more quickly, thus minimizing the negative impact?” they answered, “Yes, for sure. . . To conduct the audit effectively, companies will need to know the whereabouts of their data, which many companies haven't done yet. Knowing the data's location serves multiple purposes: it enhances protection, reduces the risk of breach or misuse, and improves business operations. Interestingly, paying attention to data location can also lead to revenue generation. We've observed companies utilizing data inventories initially for compliance and later leveraging them for marketing purposes. It's an unintended positive externality of this law."

They also find that reports from assessments and audits will lead to subsequent corrective action by businesses, including holding individuals accountable for remediating the findings about cybersecurity issues. Specifically, "If internal audit is in charge of the formal audit and there are material findings, these findings are assigned to named individuals with specified timelines—30, 60, or 90 days, typically aligning with audit committee meetings, which usually occur every three months. The audit function will provide a report and update, holding individuals accountable for remediating the findings. It's the most rigorous approach." Even with the less rigorous route of assessments, a list of risks and gaps will be identified. These identified risks and gaps "then become a question of the potential impact of a control failure on the company. This impact could include loss of revenue from business customers, loss of consumers, damage to brand reputation, or fines from California—the most feared consequence."

CSAs and the required reports will be a significant motivator for the executive team to ensure remediation of identified cybersecurity weaknesses and make necessary investments to improve the cybersecurity maturity level within businesses. Industry practitioners confirmed that "there's not a huge driver for remediation until an executive sees a number they don't like or a color on a slide that doesn't present them well to executive leadership—it's human behavior, but it's about maturity rating." "In fact, a finding from internal audit will often drive considerable investment. …You need an oversight function or the independent internal audit function to have some kind of hammer over the person that's responsible for this. And often, the person responsible for this wants that. I have clients who have partnered with internal audit; they'll call them and say, 'please audit me. I have a lot of stuff going on and problems.' But until you do it and until we get this report, senior leadership is not going to fund this, so that's how it works."

CSAs can also encourage businesses to follow a range of best practices to mitigate the losses after cybersecurity incidents by requiring the identification, assessment, and documentation of how the business tests its incident-response capabilities and its continuity and disaster-recovery plans. Steinbart et al. (2018) find that "the number of security incidents discovered after causing harm is important because organizations cannot 'stop the bleeding' and take steps to recover from an incident until they discover that they have been attacked. Indeed, organizations often do not become aware of significant information security breaches until long after the attack occurred (Ernst & Young, 2015; Lewis, 2013; Verizon, 2015). Therefore, timely detection of security breaches after they cause harm can still potentially mitigate the organization's losses."

Industry practitioners also confirmed that "usually, in a Fortune 500 company, it is now common practice to conduct a root cause analysis post-mortem and remediate the root cause if there is an important breach. Requirements to conduct CSAs can provide businesses with information to improve the quality of root cause analyses and remedial actions to address cybersecurity risks. Often, the solution involves training someone not to repeat the mistake. Sometimes, if the issue is a software problem, it might involve fixing a vulnerability in the software."

In summary, CSA requirements in the proposed regulations will lead to reduced monetary losses caused by different types of cybercrimes. In Section 3.2.3 we estimate a range of benefits of the proposed regulations focused on avoided monetary losses to businesses and consumers.

Beneficial Impacts of Risk Assessments ("RAs")

The proposed regulations require that every CCPA covered business whose processing of consumers' PI presents significant risk to consumers' privacy must conduct a RA before initiating that processing.

The business must specifically identify its purpose for processing consumers' PI, the categories of PI to be processed, and whether they include SPI, as well as several operational elements of the activity. For example, RAs require the business to identify its planned method for collecting, using, disclosing, retaining, or otherwise processing PI; and the technology to be used in the processing.

In addition, the business must specifically identify the benefits as well as the negative impacts to consumers' privacy associated with the processing of the PI, the sources and causes of these negative impacts, and the safeguards that it plans to implement to address the negative impacts identified.

RA and CSA regulations together can increase the likelihood of timely detection of cybersecurity incidents before they result in PI security breaches, which also contributes to mitigating monetary losses caused by cybercrimes. For example, a business that must comply with CSA regulations must identify, assess, and document its deployment of intrusion-detection and data-loss-prevention systems and how it manages its responses to security incidents. A business that must conduct an RA may identify unauthorized access to PI as a negative impact that could result from its processing, and the business may address that impact by investing in and implementing additional safeguards, such as additional or more finely tuned intrusion-detection and data-loss prevention systems and modifications to its incident response management. Thus, the proposed regulations together can help to ensure timely discovery of cybersecurity incidents and mitigate their impacts.

These RA and CSA requirements work together to improve the protection of businesses' and individuals' private information and lower the probability of identity theft, malware, and other related cybercrimes, hence reducing the associated monetary losses. It is impossible to separate the impact of CSAs and RAs on risk reduction of cybercrimes and the associated avoided losses. Hence, we combine the impacts of CSAs and RAs when estimating the avoided annual monetary losses related to seven types of cybercrime in the following section.

Limited Quantification of Benefits

This section focuses on quantifying the benefits of CSAs and RAs using data on reported cybercrime losses. There are no data available to support the quantification of benefits resulting from the updates to the existing CCPA regulations or of the ADMT regulations, or other benefits of the CSA and RA regulations unrelated to the prevention of these cybercrimes, so we will discuss those benefits in the unquantified benefits section.

Approach to Quantify Benefits of CSAs and RAs

It is challenging to quantify the benefits of CSAs and RAs because these benefits vary by maturity level of businesses, are usually long-term, and may not manifest themselves right away. In addition, the value of digital assets protected by CSAs and RAs can be difficult to determine, as many of the assets do not have a specific accounting value. Fortunately, recent studies and newly available data make it feasible to quantify at least a portion of the expected benefits of proposed regulations.

Recent studies find that most discovered data breaches (a common type of cybersecurity incident) could have been prevented if the victim organization had employed ‘‘best practices’’ concerning information security controls at the time of the breach (PricewaterhouseCoopers 2013; Verizon 2014, 2015). Steinbart et al. (2018) provide a few examples of what best practices should address: “It is important to detect and subsequently correct internal control weaknesses because they represent vulnerabilities that criminals can exploit. Similarly, employee noncompliance with security policies (e.g., sharing passwords, clicking on links in fraudulent emails, and failing to update security-related software) often contributes to security breaches.”

The proposed CSA regulations require that California businesses identify, assess, and document their protections for consumers’ PI, including certain best practices in cybersecurity protection recommended by prominent cybersecurity frameworks and resources and industry and academic experts, which can avoid the potential losses to consumers and businesses from cybersecurity incidents. The proposed RA regulations also require businesses to identify potential negative impacts to consumers, including unauthorized access to their PI, and relevant safeguards prior to engaging in certain processing activities. These regulations can potentially increase risk management maturity levels and avoid at least a portion of the expected losses caused by cybercrimes. Indeed, a recent study by Slapnicar et al. (2022) develops a Cybersecurity Audit Index (CAI) to measure the effectiveness of CSAs generally and finds that CAI is positively associated with cybersecurity risk management maturity. Requiring businesses to consider safeguards before conducting certain PI processing activities in a RA can contribute to improvements in both cybersecurity and privacy security.

The FBI Internet Crime Complaint Center (IC3) reports provide excellent data and resources for estimation of a subset of expected benefits of the proposed regulations for CSAs and RAs through avoided monetary losses. The IC3's mission is to provide the public with a reliable and convenient reporting mechanism to submit information concerning suspected cyber-enabled criminal activity. It is the central point for victims to report cybercrime activity. Complainants are asked to document accurate and complete information related to cybercrimes including the associated monetary losses.

By evaluating requirements in the proposed regulations to the reported cybercrimes in the IC3 reports, we identified seven cybercrimes that are expected to be mitigated following implementation of these regulations. Specifically, these crimes include Business Email Compromise (BEC), Corporate Data Breach, Identity Theft, SIM Swap, Ransomware, Botnet, and Malware.

Business Email Compromise

According to IC3 reports, BEC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques that enable unauthorized transfers of funds.

To reduce or minimize losses caused by BEC crimes, the FBI recommends that procedures such as multi-factor authentication should be put in place to verify payments and purchase requests outside of email communication. This aligns with proposed CSA regulations requirement that businesses subject to CSAs identify, assess, and document their use of multi-factor authentication. Other recommended best practices by the FBI include carefully examining the email address, URL, and spelling used in any correspondence and not clicking on anything in an unsolicited email or text message asking the recipient to update or verify account information. These best practices are strengthened by the conduct of RAs and CSAs that identify the risks to PI and the importance of employee training requirements.

The proposed CSA regulations cover assessment of all the recommended best practices by the FBI in terms of reducing or minimizing the monetary losses caused by BECs. It's reasonable to expect that if businesses follow new requirements of proposed regulations, the monetary losses to California businesses and individuals resulting from BEC crimes will be reduced.

Corporate Data Breach

A corporate data breach defined by IC3 is the use of a computer intrusion to acquire confidential or secured information. This does not include computer intrusions targeting personally-owned computers, systems, devices, or personal accounts such as social media or financial accounts. CSAs directly address this type of cybercrime by requiring businesses subject to CSAs to identify, assess, and document their deployment of intrusion-detection, intrusion-prevention, and data-loss-prevention systems. The proposed regulations are expected to lower the associated monetary losses associated with corporate data breaches.

Identity Theft

Identity theft occurs when someone wrongfully obtains and uses PI in some way that involves fraud or deception, typically for economic gain. The proposed CSA regulations require a business to assess how its cybersecurity program protects PI from unauthorized access, use, modification, or disclosure; and protects against unauthorized activities that can result in the loss of security of PI. The proposed RA regulations require the business to identify its planned method for collecting, using, disclosing, retaining, or otherwise processing PI; and the technology to be used in the processing. This requirement is expected to enhance the protection of PI at the beginning of the processing of PI.

In addition, the proposed RA regulations require that the business must specifically identify the benefits as well as the negative impacts to consumers' privacy associated with the processing of the PI, the sources and causes of these negative impacts, and the safeguards that it plans to implement to address the negative impacts identified. It is reasonable to expect that most monetary losses caused by Identity Theft can be reduced by the proposed CSA and RA regulations, as well as the steps that businesses will take following completion of these requirements.

SIM Swap

Subscriber Identity Module or SIM Swap is the use of unsophisticated social engineering techniques against mobile service providers to transfer a victim's phone service to a mobile device in the criminal's possession. SIM Swap is a cybercrime that targets the telecommunication industry, which will be impacted by proposed regulations. California businesses subject to the CSA regulations will need to identify, assess, and document their cybersecurity training for anyone to whom the business provides access to its information system. Further, the CSA must identify, assess, and document how the business maintains current knowledge of changing cybersecurity threats and countermeasures. Such cybersecurity awareness, education, and preventive trainings in the proposed regulations will help businesses in the telecommunication industry keep up with changing cybersecurity threats and develop appropriate countermeasures. These requirements will mitigate the monetary losses resulting from SIM Swap in the future.

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system until money is paid to the attacker. The proposed CSA regulations require the identification, assessment, and documentation of a business's deployment of data-loss-prevention systems (e.g., software to detect and prevent unauthorized access) and the business's continuity and disaster-recovery plans, including data-recovery capabilities and backups. A business that must conduct an RA may identify unauthorized access to or destruction of PI, as well as unauthorized activity resulting in the loss of availability of PI, as negative impacts that could result from its processing, and the business may identify the risk of ransomware as a source and cause of these negative impacts.

The business may address those impacts and risk by implementing additional safeguards, such as additional or more finely tuned data-loss prevention systems and additional or improved business continuity and disaster-recovery plans, including data-recovery capabilities and backups. Thus, the proposed CSA and RA regulations together will contribute to enhanced corporate data security and cybercrime risk reduction. These requirements and the steps that businesses take as a result of completing RAs and CSAs can either lower the likelihood of a successful ransomware attack, or, in the case of an attack, dramatically lower the resulting monetary losses by having improved data-recovery capabilities and backups.

Botnet

A botnet is a group of two or more computers controlled and updated remotely for an illegal purpose such as a Distributed Denial-of-Service (DDoS) or Telephony Denial of Service attack or other nefarious activity. Botnet attacks typically involve stealing data, sending large quantities of spam and phishing emails, or launching massive DDoS attacks. Botnet attacks occur when large numbers of machines have been taken over by the attacker. The proposed CSA regulations and the steps that businesses take due to completing CSAs can directly address this type of crime by requiring that businesses identify, assess, and document their deployment of bot-detection and other internal and external vulnerability scans as prevention measures. The proposed CSA regulations are expected to reduce the associated monetary losses from botnet cybercrimes.

Malware

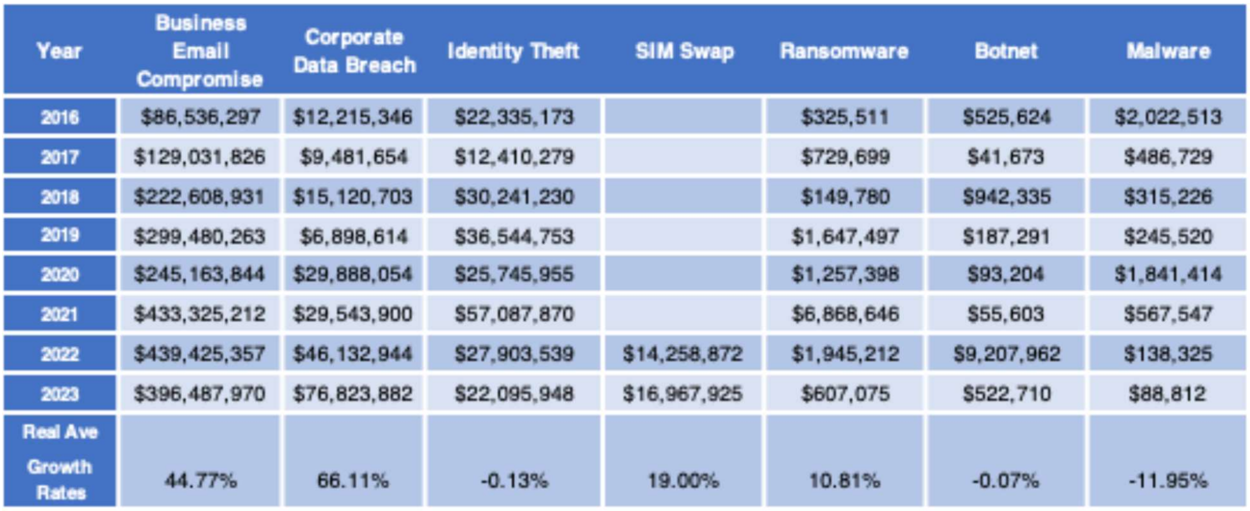
Malware is software or code intended to damage, disable, or be capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data. The proposed CSA regulations require a business to assess how its cybersecurity program protects PI from unauthorized access, destruction, use, modification, or disclosure. They also require that businesses identify, assess, and document their cybersecurity training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system. A business that must conduct an RA may identify unauthorized access, destruction, use, modification, or disclosure; and unauthorized activity resulting in the loss of availability of PI as negative impacts that could result from its processing.

The business may identify the risk of malware as a source and cause of these negative impacts, and it may address those impacts and risk by implementing additional safeguards, such as additional or more finely tuned antimalware protections and additional or improved cybersecurity awareness, education, and training designed to avoid the introduction of malware into the business's information system. Thus, the proposed CSA and RA regulations together, and steps that businesses take as a result of complying with them, are expected to reduce the monetary losses associated with malware attacks targeting California businesses.

Table 3-1 below presents the reported monetary losses associated with seven types of cybercrimes in California from 2016 to 2023 in 2022 dollars. The last row quantifies real average growth rates of monetary losses due to each type of cybercrime. The Real Average Growth Rates are computed using the values of the beginning year and the ending year:

Real Average Growth Rates = [(EndingValue-BeginningValue)/BeginningValue] / Number of Years.

Table 3-1: CA Monetary Losses from Seven Cybercrimes Impacted by Proposed Regulations (2016-2023)



Year	Business Email Compromise	Corporate Data Breach	Identity Theft	SIM Swap	Ransomware	Botnet	Malware
2016	$86,536,297	$12,215,346	$22,335,173		$325,511	$525,624	$2,022,513
2017	$129,031,826	$9,481,654	$12,410,279		$729,699	$41,673	$486,729
2018	$222,608,931	$15,120,703	$30,241,230		$149,780	$942,335	$315,226
2019	$299,480,263	$6,898,614	$36,544,753		$1,647,497	$187,291	$245,520
2020	$245,163,844	$29,888,054	$25,745,955		$1,257,398	$93,204	$1,841,414
2021	$433,325,212	$29,543,900	$57,087,870		$6,868,646	$55,603	$567,547
2022	$439,425,357	$46,132,944	$27,903,539	$14,258,872	$1,945,212	$9,207,962	$138,325
2023	$396,487,970	$76,823,882	$22,095,948	$16,967,925	$607,075	$522,710	$88,812
Real Ave Growth Rates	44.77%	66.11%	-0.13%	19.00%	10.81%	-0.07%	-11.95%

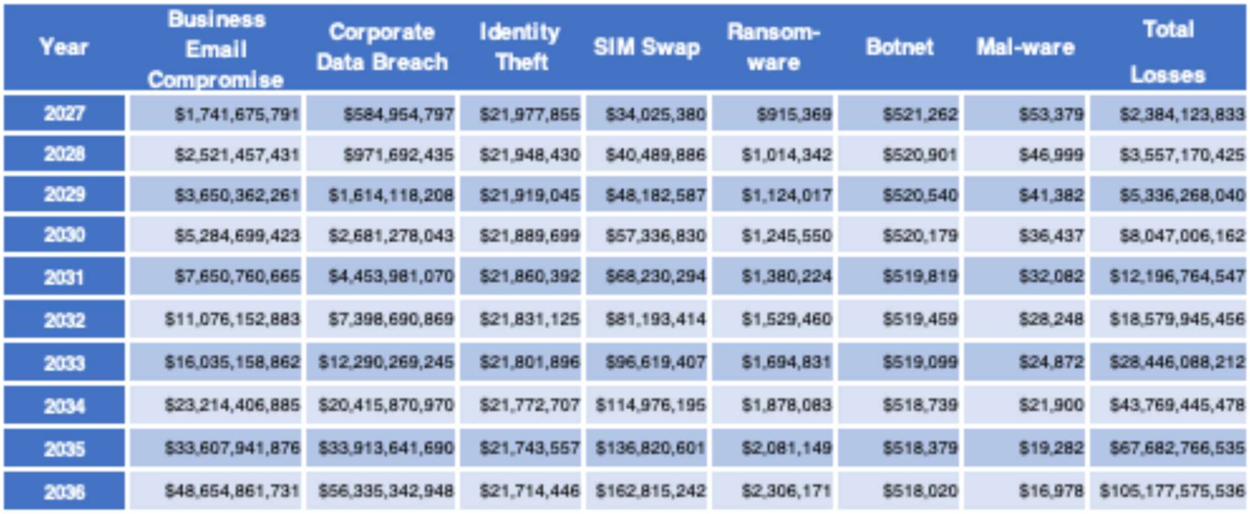
Sources: FBI IC3 Reports from 2016 to 2023, California Consumer Price Index by Department of Industrial Relations.
Note: All figures in 2022 $

When estimating future avoided cybercrime monetary losses, we use Real Average Growth Rates to compute the trend in expected change over time.

3.2 Baseline for Cybercrimes in California

Table 3-2 summarizes the baseline trend in California of annual monetary losses for seven types of cybercrimes from 2027 to 2036 in 2022 dollars. As shown in Table 3-2, the total annual losses are expected to reach **$2.4 billion** in 2027 and **$105.2 billion** in 2036, in the absence of proposed regulations.

Table 3-2: Baseline Trend in Monetary Losses for Seven Types of Cybercrimes



Year	Business Email Compromise	Corporate Data Breach	Identity Theft	SIM Swap	Ransom-ware	Botnet	Mal-ware	Total Losses
2027	$1,741,675,791	$584,954,797	$21,977,855	$34,025,380	$915,369	$521,262	$53,379	$2,384,123,833
2028	$2,521,457,431	$971,692,435	$21,948,430	$40,489,886	$1,014,342	$520,901	$46,999	$3,557,170,425
2029	$3,650,362,261	$1,614,118,208	$21,919,045	$48,182,587	$1,124,017	$520,540	$41,382	$5,336,268,040
2030	$5,284,699,423	$2,681,278,043	$21,889,699	$57,336,830	$1,245,550	$520,179	$36,437	$8,047,006,162
2031	$7,650,760,665	$4,453,981,070	$21,860,392	$68,230,294	$1,380,224	$519,819	$32,082	$12,196,764,547
2032	$11,076,152,883	$7,398,690,869	$21,831,125	$81,193,414	$1,529,460	$519,459	$28,248	$18,579,945,456
2033	$16,035,158,862	$12,290,269,245	$21,801,896	$96,619,407	$1,694,831	$519,099	$24,872	$28,446,088,212
2034	$23,214,406,885	$20,415,870,970	$21,772,707	$114,976,195	$1,878,083	$518,739	$21,900	$43,769,445,478
2035	$33,607,941,876	$33,913,641,690	$21,743,557	$136,820,601	$2,081,149	$518,379	$19,282	$67,682,766,535
2036	$48,654,861,731	$56,335,342,948	$21,714,446	$162,815,242	$2,306,171	$518,020	$16,978	$105,177,575,536

Sources: FBI IC3 Reports from 2016 to 2023, California Consumer Price Index by Department of Industrial Relations.
Note: All figures in 2022 $

It is important to recognize that monetary losses data caused by cybercrimes obtained from IC3 reports provide only a lower bound for the potential avoided losses and likely dramatically underestimate such losses. This is because only a small share of cybercrime victims chose to report their losses to FBI. For example, the FBI recently found that only about 20% of Hive ransomware's victims reported the incident to law enforcement. Data on reporting rates of other types of cybercrimes were not available. Given that this is the only information available on report rates of cybercrimes, we assume that the 20% reporting rate applies to other types of cybercrimes as well, when calculating the total avoided losses in the next section.

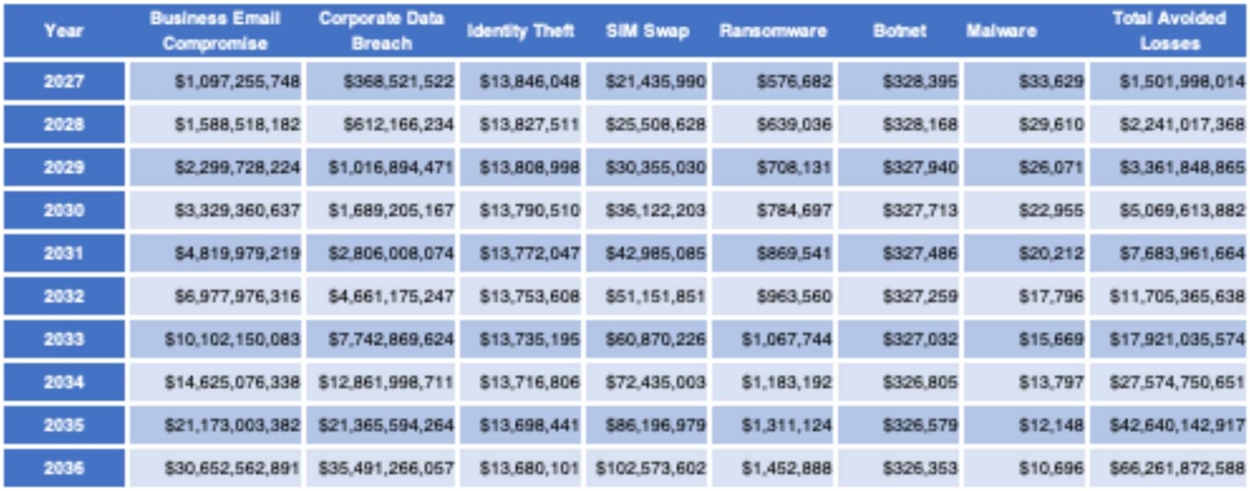
Analysis of Benefits from Reduction in Cybercrimes

The proposed CSA and RA regulations impose certain requirements upon, and provide best-practice guidance to, businesses to reduce or mitigate negative impacts to consumers, including the monetary losses and other harms caused by cybercrimes. As discussed above, both academic studies and private sector practitioners have provided supporting evidence that these regulations can effectively reduce cyber risk and lead to potential benefits to California businesses and individuals.

According to 2023 IBM Data Breach Report (which surveys organizations globally), organizations with a high level of noncompliance with existing cybersecurity laws and regulations showed an average cost of $5.05 million, which exceeded the average cost of a data breach by $560,000, a difference of 12.6%. This percentage difference provides a reasonable proxy for a conservative estimate of the magnitude of avoided cybercrime losses to result from implementation of the proposed regulations in California. As shown in IC3 reports, California has the highest number of cybercrimes and the highest monetary losses associated with these crimes among all U.S. states. And the U.S. has the highest data breach costs among all nations consecutively for 13 years (2023 IBM Data Breach Report). The actual benefits of implementing these regulations in California is likely to be higher than a 12.6% loss reduction. We want to provide a conservative estimate of the quantified direct benefits of the proposed regulations, so we assume a 12.6% reduction of these seven cybercrimes for California firms subject to proposed regulations as well.

In addition, we assume that reported losses to IC3 are done by businesses that process PI of California consumers and are covered by the CCPA. As mentioned before, we assume a 20% reporting rate for the seven types of cybercrimes based on evidence from IC3 reports. Based upon the above, we can estimate the avoided losses of seven cybercrimes for all businesses subject to CSA and RA requirements under CCPA coverage.

Table 3-3: Annual Avoided Losses of 12.6% Reduction in Seven Cybercrimes with CCPA Coverage (2027-2036)



Year	Business Email Compromise	Corporate Data Breach	Identity Theft	SIM Swap	Ransomware	Botnet	Malware	Total Avoided Losses
2027	$1,097,255,748	$368,521,522	$13,846,048	$21,435,990	$576,682	$328,395	$33,629	$1,501,998,014
2028	$1,588,518,182	$612,166,234	$13,827,511	$25,508,628	$639,036	$328,168	$29,610	$2,241,017,368
2029	$2,299,728,224	$1,016,894,471	$13,808,998	$30,355,030	$708,131	$327,940	$26,071	$3,361,848,865
2030	$3,329,360,637	$1,689,205,167	$13,790,510	$36,122,203	$784,697	$327,713	$22,955	$5,069,613,882
2031	$4,819,979,219	$2,806,008,074	$13,772,047	$42,985,085	$869,541	$327,486	$20,212	$7,683,961,664
2032	$6,977,976,316	$4,661,175,247	$13,753,608	$51,151,851	$963,560	$327,259	$17,796	$11,705,365,638
2033	$10,102,150,083	$7,742,869,624	$13,735,195	$60,870,226	$1,067,744	$327,032	$15,669	$17,921,035,574
2034	$14,625,076,338	$12,861,998,711	$13,716,806	$72,435,003	$1,183,192	$326,805	$13,797	$27,574,750,651
2035	$21,173,003,382	$21,365,594,264	$13,698,441	$86,196,979	$1,311,124	$326,579	$12,148	$42,640,142,917
2036	$30,652,562,891	$35,491,266,057	$13,680,101	$102,573,602	$1,452,888	$326,353	$10,696	$66,261,872,588

Sources: FBI IC3 Reports from 2016 to 2023, California Consumer Price Index by Department of Industrial Relations.
Note: All figures in 2022 $

Although Table 3-3 only shows the avoided losses of seven types of cybercrimes, a quantifiable subset of loss avoidance caused by the proposed regulations, the potential benefits can still be huge. The direct benefits to California businesses of a 12.6% reduction of these seven cybercrimes are estimated to be approximately **$1.5 billion** in 2027 and **$66.3 billion** in 2036.

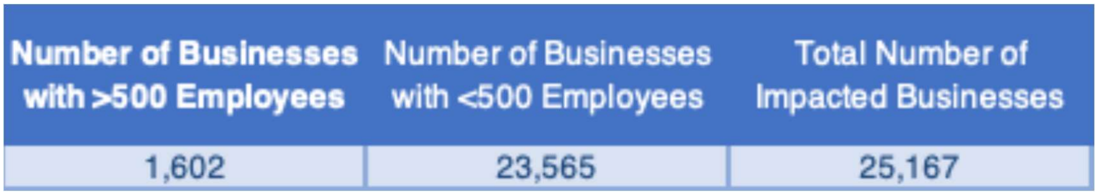
In the following analysis, we discuss the proposed CSA and RA regulations, as well as four regulatory alternatives considered, which include different annual revenue thresholds and whether or not the business generates over 50% of its revenue from selling PI. Next, we focus on quantifying the combined benefits of proposed CSAs and RAs regulations.

Quantified Benefits of Proposed CSA and RA Regulations

We analyze the impact on California businesses with greater than $28 million in annual revenues or generate more than 50% of their revenue from sharing or sale of PI. These conditions correspond to the criteria of proposed CSA coverage. We start with the impact on businesses resulting from CSA requirements and then analyze the combined impact of proposed CSA and RA regulations to estimate the resulting avoided monetary losses due to reductions in cybercrimes.

The total number of impacted businesses under proposed CSA regulations is 25,167. According to the data provided in 2023 IBM Data Breach Report, the avoided losses vary with firm sizes. In fact, the cost of a data breach for a firm with >500 employees is consistently 1.5 times the cost of a firm with <500 employees. We take this fact into consideration and further break down the number of impacted California businesses based upon whether the number of employees is >500 or <500 as shown below in Table 3-4:

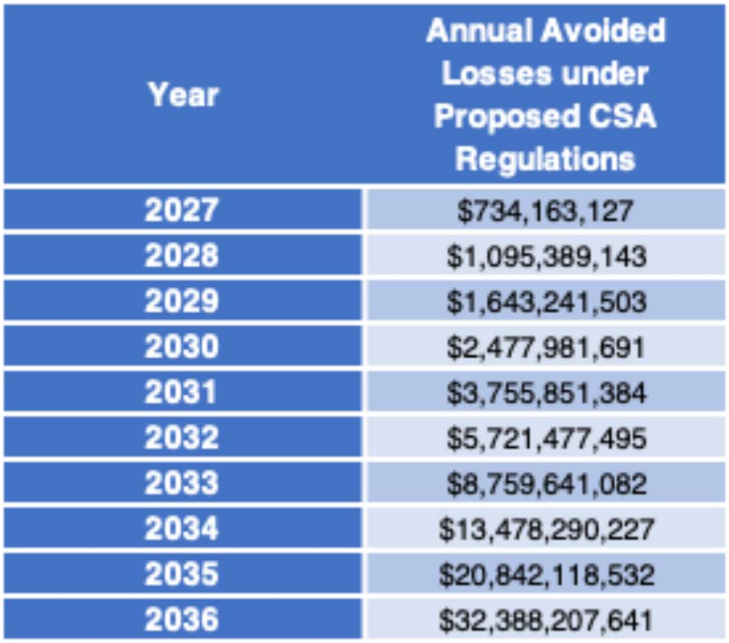
Table 3-4: Impacted California Businesses Based upon Number of Employees under Proposed CSA Regulations



Number of Businesses with >500 Employees	Number of Businesses with <500 Employees	Total Number of Impacted Businesses
1,602	23,565	25,167

According to the data provided in 2023 IBM Data Breach Report, the average cost of a data breach for a business with more than 500 employees is about 1.5 times the average cost of a data breach for a business with less than 500 employees. This is the only data we have found on the relationship between cybercrime losses and business size. Based on this evidence, we assume that the avoided losses of seven cybercrimes follow a similar pattern. The expected annual avoided monetary losses for California businesses under proposed CSA regulations from 2027 to 2036 are given in Table 3-5 below.

Table 3-5: Annual Avoided Monetary Losses under Proposed CSA Regulations (2027-2036)



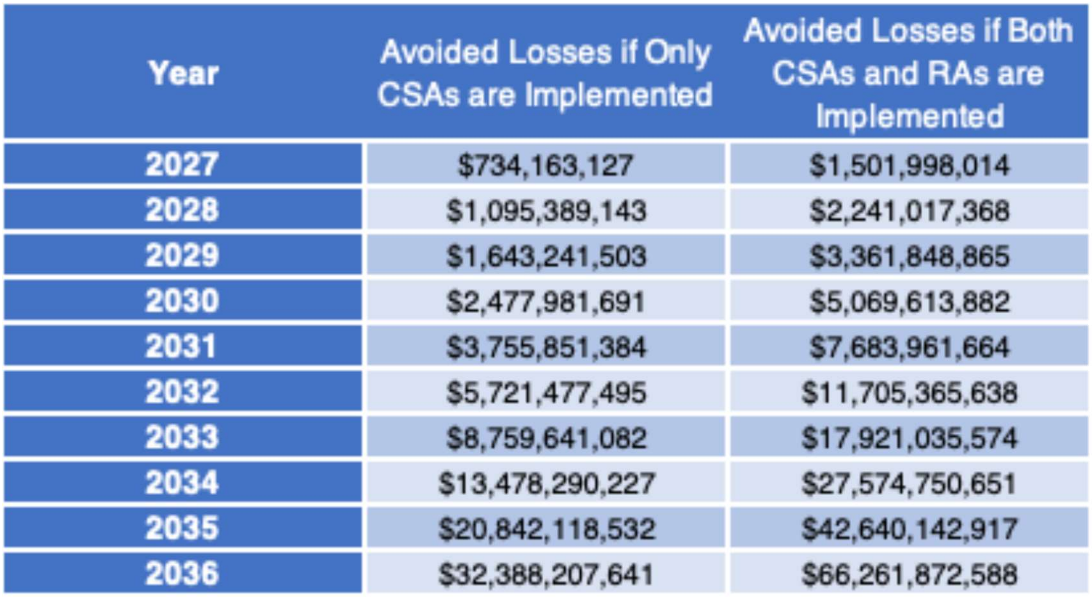
Year	Annual Avoided Losses under Proposed CSA Regulations
2027	$734,163,127
2028	$1,095,389,143
2029	$1,643,241,503
2030	$2,477,981,691
2031	$3,755,851,384
2032	$5,721,477,495
2033	$8,759,641,082
2034	$13,478,290,227
2035	$20,842,118,532
2036	$32,388,207,641

Note: All figures in 2022 $

As shown in Table 3-5, the expected annual avoided losses under proposed CSA regulations will be approximately **$734 million** in 2027 and over **$32 billion** by the year 2036.

Now we consider the number of impacted California businesses under proposed RA regulations. This number ranges from 13,082 to 52,326 businesses. As discussed before, the proposed CSA and RA regulations work together to help businesses avoid monetary losses associated with cybercrimes. It is not possible to apportion the share of risk reduction to the proposed CSA or RA regulations. If we assume that both the proposed CSA and RA regulations contribute to avoided losses due to reduction of all seven types of cybercrimes, then the combined number of impacted businesses ranges from 25,167 to 52,326. If only CSA regulations are implemented, the number of impacted businesses will be 25,167, and the avoided losses are reported as monetary figures in the left column of Table 3-6. When both CSA and RA regulations are implemented and they are complimentary in terms of reducing the losses caused by seven types of cybercrimes, then the number of impacted businesses will be 52,326, and avoided losses are reported as monetary figures in the right column of Table 3-6.

Table 3-6: Avoided Monetary Losses due to Proposed CSA and RA Regulations (2027-2036)



Year	Avoided Losses if Only CSAs are Implemented	Avoided Losses if Both CSAs and RAs are Implemented
2027	$734,163,127	$1,501,998,014
2028	$1,095,389,143	$2,241,017,368
2029	$1,643,241,503	$3,361,848,865
2030	$2,477,981,691	$5,069,613,882
2031	$3,755,851,384	$7,683,961,664
2032	$5,721,477,495	$11,705,365,638
2033	$8,759,641,082	$17,921,035,574
2034	$13,478,290,227	$27,574,750,651
2035	$20,842,118,532	$42,640,142,917
2036	$32,388,207,641	$66,261,872,588

Note: All figures in 2022 $

The expected annual avoided losses due to proposed CSA and RA regulations combined ranges from **$1.5 billion** in 2027 to **$66.3 billion** in 2036. These estimates reflect the total quantified direct benefits for the proposed regulations.

3.3 Unquantified Benefits

The proposed consumer privacy regulations focus on four specific areas of consumer protection. The first area is cybersecurity, and it requires certain businesses to audit how they protect PI from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of PI. With better CSA, companies are better able to develop mature cybersecurity systems, pinpoint the weaknesses of their current security functions, and implement updates in their controls to bolster the security of their systems and result in added protection of consumers' PI.

The second area focuses on RA, and it requires businesses to assess the privacy risks and benefits of certain activities. The goal of this assessment is to ensure that a business does not engage in processing consumers' PI where the risks to privacy outweigh associated benefits. This aspect of the regulations provides consumers with more protections for their privacy and safeguards against discrimination in ADMT, including the use of extensive profiling technologies.

The third area of the proposed regulations mandates that businesses provide consumers with the ability to opt-out of, and access information about, certain uses of ADMT. In addition, these proposed regulations also mandate that businesses assess their development and use of ADMTs for certain physical or biological identification or profiling by evaluating the technology to ensure it works as intended for their proposed use and requires them to implement safeguards. The primary benefits of these propose regulations are giving consumers more control over their PI with the opt-out and access options and preventing automated decisionmaking processes from making or influencing decisions that involve discrimination or inappropriate profiling.

The final area relates to updates to previous rules that implemented the California Consumer Privacy Act. Specifically, these updates include requirements that make it easier for consumers to access information about a business's privacy practices. The updates provide additional transparency for consumers (e.g., regarding their rights to access PI and to correct inaccurate PI, and about the status of their requests to opt-out of sale/sharing and to limit). The updates also impose additional requirements and provide clarity for businesses as to how to implement consumers' requests (e.g., ensuring that consumers' requests to delete and correct are fully implemented). Lastly, the updates provide clarity for businesses as to how to make it easy for consumers to exercise their rights and how to avoid being confusing to consumers. The updates benefit consumers by saving them time and making it easier for them understand and control businesses' use of their PI. The updates benefit businesses by saving them time in their interactions with consumers and in processing duplicative consumer requests (e.g., duplicative requests to opt out of sale/sharing or to limit the business's use of their PI).

3.4 Wide Range of Unquantified Benefits

The proposed regulations have many benefits, most of which go beyond pecuniary measures. There are also some others that cannot be measured adequately due to data limitations. The unquantified benefits of the proposed regulations also apply to the alternatives considered within this rulemaking.

For consumers, the new rules will reduce the time and resource demands of protecting privacy, enforcing the right to limit data use and disclosure, and using their agency in checking the accuracy of the PI collected by businesses. In addition, when businesses are better able to develop mature cybersecurity systems, pinpoint the weaknesses of their current security functions, and implement updates in their controls to bolster the security of their systems—as we expect will result from businesses' implementation of the CSA and RA regulations—they will better protect consumers' PI, including by reducing the incidences and severity of data breaches. The associated unquantified benefits of the proposed regulations include avoiding the physical, reputational, and psychological harm that results from unauthorized access, destruction, use, modification, or disclosure of PI; and from unauthorized activity that results in the loss of availability of PI. The unquantified benefits include avoiding the social and psychological costs of identity theft and fraud, such as fear, anxiety, stress, and other inconveniences.

In addition, the proposed regulations require businesses that use ADMTs in certain ways to take steps to increase transparency and consumer awareness about their opt-out of ADMT and access ADMT rights (for example, by requiring that businesses notify consumers about the use of their PI for certain uses of ADMT). As a result, consumers gain the ability to access information about how that technology was used with respect to them, and in many instances, can be more informed about how to opt out of the use of their data via this technology. The proposed regulations also require these businesses—as part of their risk-assessment obligations—to identify the actions they have taken or plan to take to maintain data quality. The proposed regulations also mandate businesses to verify that their use of physical or biological identification or profiling automated technologies for certain purposes function as intended and that they do not discriminate on the basis of protected classes. These proposed regulations will provide individuals with more control over their PI and are expected to increase the quality of data that businesses use, improve the knowledge, understanding, accuracy and efficacy that businesses have with accessing and using such information, and reduce incidences of discrimination.

There are also many benefits for businesses and the economy that are not quantified. Businesses not only gain additional guidance about compliance requirements, but also lower the potential costs of consumer privacy protection by standardizing processes and increasing their operational efficiency. The proposed regulations will help businesses build trust and loyalty from consumers. This increase in trust improves the business's reputation and boosts the ability to reach more potential customers. Having improved privacy compliance standards also enables business owners to reduce the impact of cybercrimes, improve their data management systems, and focus more of their resources on further developing their businesses. Overall, by complying with the regulations, businesses can take advantage of more secure privacy protections, including less bias and discrimination, potential for job and business creation, and increased investment in protections for PI. These benefits will help the California economy be more competitive and continue to grow while enforcement costs decline due to lower impacts of cybercrime, increased transparency of data usage, more accessible individual control over PI, and reduced privacy harms to consumers.

3.4.1 Cybersecurity Audits

Cybersecurity programs protect the PI that businesses have collected and the insights they have developed from evaluating the information. They also secure the systems and structures that companies have over their production processes, services, orders, deliveries, and management as long as PI is processed. CSAs play an important role in evaluating the strength of cybersecurity programs as they check the processes and controls that businesses have implemented to secure their PI gathering, updating, transmission, processing, and storage.

In general, CSAs check that security systems and processes are in place and working as intended (California Department of Technology, 2024). They are also "essential to identifying cybersecurity program weaknesses and developing appropriate recommendations for corrective actions" (U.S. Government Accountability Office, 2023). Unsurprisingly, CSAs are positively linked to the maturity of cybersecurity systems (Islam, Farah, & Stafford, 2018; Slapnicar, Vuko, Cular, & Drascek, 2022). However, businesses may not be inclined to incur the costs of adequate investment in cybersecurity systems and improvements in their cybersecurity practices, including engaging in CSAs. Businesses have a built-in bias for allocating resources for revenue-generating projects, so they tend to be less likely to invest in functions such as cybersecurity (Gordon, 2007).

Considering that businesses may not invest enough on cybersecurity systems and processes, they may be more vulnerable to cyberattacks, so existing laws and regulations were developed to motivate this type of investment. However, cyber experts have indicated that current cybersecurity regulations do not adequately address the modern cybersecurity risks that businesses face (Starks, 2023). The proposed cybersecurity regulations, especially those relating to CSA, can incentivize businesses to regularly examine their exposure to cyber risks and evaluate their cybersecurity infrastructure and processes. CSAs will help businesses build more effective cybersecurity infrastructure for evaluating internal controls, finding potential areas of vulnerability, and contributing to the development of best cybersecurity practices and processes (Sabillon, Serra-Ruiz, Cavaller, & Cano, 2018; Aditya, Ferdiana, & Santosa, 2018; Gauthier & Brender, 2021; Layton and Watters, 2014).

Even if there are no disciplinary actions for failing to follow CSA best-practice guidance, businesses should implement them because they can lead to the development of more mature cybersecurity systems that protect the organization's assets from threats of cyberattacks (Sanchez-Garcia, Rea-Guaman, Gilabert, & Calvo-Manzano, 2024). This is where the role of the government regulations on CSA can have significant contribution. The proposed CSA regulations not only articulate the requirements for completing thorough and independent CSA, but they may also have a positive externality of motivating boards of directors and other members of corporate management to make the necessary investments to align with cybersecurity best practices (Gale, Bongiovanni, & Slapnicar, 2022).

Another benefit of the CSA regulations will be that individuals and businesses that have desired knowledge and expertise in cybersecurity protections will benefit from higher demand for their services. With higher demand, training and employment in this industry increases. According to some prominent experts, this increased demand for cybersecurity employees and services may be even more pronounced in businesses – particularly middle-sized businesses – that are not as familiar with more modern cybersecurity systems or do not have as much capacity to attend to the new regulatory requirements. Although payments for these services can be deemed as revenue for CSA providers and as costs for the other businesses, those that pay for CSA gain the insights and benefits from these audit services.

Moreover, businesses taking additional measures - such as evaluating cyber risks using CSA - to protect consumer data can reduce the incidence and severity of data breaches. These breaches impose significant risks on California consumers and businesses. With these data breaches, consumers experience disruptions to the regular business and public services they use (Madnick, 2023). They face inconveniences and costs associated with having to file data and/or identity theft reports, update their records, accounts, and passwords, monitor their credit, and replace their affected debit and credit cards. Many consumers also suffer lost opportunities due to inaccurate information from data breaches, which can further exacerbate the psychological harm they face. Victims of data hacking, for instance, experience an intrusion into their “digital space.” These experiences cause adverse emotional impact, an increased sense of vulnerability, and a sense of violation. Individuals whose data may have been compromised through data breaches of businesses can experience depression and heightened fears and anxieties about their PI being misused and about facing a higher likelihood of economic, psychological, and social harm in the future (Palassis, et al., 2021).

Without the CSA mandated by these proposed regulations, businesses risk experiencing a wide array of damages stemming from more severe data breaches and other cybercrimes. Businesses that do not conduct effective CSA are more likely to fail to catch issues in their internal controls and processes. Because of the existing lapses in cybersecurity systems and processes, when businesses encounter cyberattacks, they are less equipped to defend against the attack and mitigate the damages when they occur. Furthermore, without the evaluations of internal controls, processes, and training under CSA, the workers are more likely to become more stressed, fatigued, or distracted and become less effective in upholding a safe, cyber environment, leading to further gaps in cybersecurity measures (Nobles, 2022).

Following data breaches, businesses suffer adverse impacts on their reputation and valuation. Even if businesses utilize resources by hiring public relations and forensic investigators to mitigate reputational and organizational damages, the adverse impacts of data breaches may last for a considerable amount of time, especially if the breaches severely impacted consumers (Huang, Wang, Wei, & Madnick, 2023; Tosun, 2021). Businesses may also face litigation costs, judgments, and civil penalties for unauthorized access of consumers’ PI. Some may even face ransomware damages unless they pay the instigators of the attack. Breaches may also impact the pricing of insurance contracts, as the risk evaluations the businesses face change when a breach occurs (Eling & Loperfido, 2017).

In addition, the proposed CSA regulations consider guidance provided in prominent cybersecurity frameworks and resources. The requirements that businesses’ CSA identify, assess, and document specific components of a business’s cybersecurity program, as applicable, may also serve as substantive cybersecurity guidance for companies. By standardizing the CSA process while retaining flexibility for businesses, the cost of audits may decline over time, especially for third-party auditors that scale up their business and offer the same service to multiple businesses. In addition to improving data security and raising the quality of inventory management, the standardization of CSA can also decrease the cybersecurity costs for businesses conducting their internal audits as these businesses apply similar best practices and employ more experienced and knowledgeable personnel. Businesses will become proficient in dealing with data breaches swiftly and effectively, when they conduct and learn from higher quality and more informative CSA (IBM, 2023).

3.4.2 Risk Assessments

On many occasions, the risks that consumers face from businesses' activities collecting PI exceed the claimed efficiency gains from evaluating consumer records (Armitage, et al., 2023 & Hagey, 2019). The proposed regulations may improve the ability of consumers to exercise their right to opt out of data collection, processing, sharing, and selling by requiring businesses to consider the risks to consumers' privacy, including the risk of insufficient disclosures to consumers about how their PI will be processed and their rights to opt out. These proposed regulations may then lead to reduced risks that consumers face, especially those relating to data breaches, scams, and fraud. Since these proposed regulations promote the removal of deficiencies in protecting PI, consumers seeking to reduce the risks they face with their PI do not have to expend as many resources to protect their privacy (Skatova, et al., 2023; Vila, Greenstadt, & Molnar, 2003).

Another potential benefit of these proposed RA regulations is the standardization of privacy protection. The proposed regulations, such as an assessment of risks to business inventories of PI, serve as guidance about the minimum privacy protection standards that web service providers need to uphold (Vila, Greenstadt, & Molnar, 2003). The proposed regulations also require businesses to identify the minimum PI necessary to achieve the purpose of their processing. This requirement can urge businesses to focus their data collection on what they need, leading businesses to minimize their information gathering and further improve privacy protection.

Proposed RA regulations benefit not just the consumer but also the businesses offering online services (Kox, Straathof, & Zwart, 2017). Not only do the proposed regulations help to prevent discrimination and protect consumer privacy, but they also require businesses to identify how they maintain the quality of PI collected and used by AI or ADMT. With more efficient, secure, and privacy-protective data collection processes and checks, businesses can uphold the trust of clients while reducing the amount of time and resources they need to utilize consumer data and comply with privacy statutes and regulations. In addition, a higher degree of business trustworthiness translates to rising familiarity with the business and improved consumer buying intention and overall purchasing behavior (Soleimani, 2022; Flavian & Guinaliu, 2006; and Bhattacherjee, 2002).

By complying with these proposed RA regulations, businesses that collect PI must have an improved system for data processing so that businesses can reduce the instances of data breaches and avoid the adverse impact on their activities and their consumers (Huang, Wang, Wei, & Madnick, 2023). Businesses also benefit from being able to process more accurate consumer data. With improved data quality, businesses can develop more effective predictive models and extract better-quality insights from their data analytics and can make more productive business decisions (Ehrlinger & Wob, 2022). With better data security and internal controls, companies will also require fewer resources to prevent data breaches from occurring (Cisco, 2024).

If businesses closely adhere to the regulatory protection requirements, they will be able to reduce the costs of data storage and protection by collecting and retaining less data. They will also benefit from more trustworthy cybersecurity systems. These cost-savings and improvements in cybersecurity will improve the business's reputation and trustworthiness and will not only generate more consumer transactions, but they will also attract more investment. This is because adhering to the new regulations could "foster a greater sense of predictability for companies and consumers and minimize the uncertainty that case-by-case enforcement may engender" (Federal Trade Commission, 2022). In the long term, they can then dedicate more resources to innovating new products and further expanding their business activities. Any potential data breaches they face may then become less severe so that the businesses face fewer lost opportunities from having to reallocate their internal resources to handle data breaches and privacy violations.

California businesses will also benefit from being required to consider the risks to consumers' privacy, including the risk of insufficient disclosures to consumers about how their PI will be processed; this will increase transparency in disclosing how they utilize PI. As explained by Godel, et al., 2017, businesses can highlight how the usage of PI can benefit consumers by reducing costs, saving time, and earning larger benefits with data collection and processing. This system provides context that individuals can use as they weigh the value of their privacy against allowing businesses to gather their data in exchange for additional conveniences and services. With this transparency, consumers are more likely to maintain the data collection process instead of focusing on the potential risks that they face when their PI is collected (Frik & Gaudeul, 2020; Acquisti, John, & Loewenstein, 2013).

Overall, with these proposed RA regulations, consumers can enjoy improved privacy protection and transparency as they can hold businesses more accountable for their data processing. Individuals may more easily practice their opt-out rights. They also face less risks of information leaks and are able to build more trust in online businesses and institutions. Businesses also benefit from optimized data collection practices and maintenance along with improved trust from consumers. This new set of regulations not only enable businesses to build better relationships with their customers but also allow them to conduct their businesses and practices more safely and efficiently in the long term.

3.4.3 Automated Decisionmaking Technology

A third important area of proposed regulations is ADMT. These proposed regulatory requirements will greatly increase transparency and lead to more informed consumers. They also enable more consumers to opt out of a business's use of their data, particularly for data processing involving ADMT used to make significant decisions, conduct extensive profiling, and for training uses of ADMT. Since these proposed regulations can lead to increased opt-outs from the use of ADMT for profiling for behavioral advertising, there may be less targeted advertising that tends to promote products from low quality vendors (Mustri, Adjerid, & Acquisti, 2023; Ali, et al., 2019). These proposed regulations also lower the amount of hiring discrimination as businesses are forced to or voluntarily evaluate whether the ADMTs being utilized for hiring are discriminatory in any way and whether or not they are working as intended.

Following the proposed ADMT regulations, when businesses examine whether ADMTs exhibit discrimination, the dataset used to train the model must be evaluated more closely. When using data from consumers, the datasets may closely reflect the separation and segregation that individuals face in their communities. Nondiscriminatory economic frameworks along with other frameworks that minimize biases in the data will be required to avoid disparities in outcomes among different demographics. In doing so, the biases and prejudices can be minimized so that they are not integrated into the ADMTs businesses use (Lang & Kahn-Lang Spitzer, 2020). To make a clear assessment of the quality of the data, a formalism of the data evaluation is likely to be a natural result of these proposed ADMT regulations. With these formalisms, the quality of the actions used to assess the data and the interplay of those actions can be better evaluated. These formalisms will help develop effective and consistent methods to evaluate and improve the quality of datasets used in ADMT development, training, and applications (Belkhale, Cui, & Sadigh, 2024; Ehrlinger & Wob, 2022; Vetro, Torchiano, & Mecati, 2021).

The ADMT regulations provide exceptions to the opt-out option with some caveats. The opt-out option is available without exception if the consumer data is used to train ADMT for certain uses or to profile individuals for behavioral advertising. Where the opt-out option is required, the proposed regulations allow consumers to opt-out of a business's profiling for behavioral advertising used to make automated price adjustments, enabling consumers to avoid price targeting and discrimination (Shiller, 2020; Norfleet, 2022). Aspects of these proposed regulations that check for discrimination will reduce the algorithmic bias, even with limited raw data sets (Chen, 2023). For example, when training ADMT used for jail-or-release decisions, a business that evaluates the ADMT to avoid discrimination could address racial equity, including the use of economic frameworks to develop unbiased machine learning tools that simultaneously reduce crime rates and mitigate the racial bias inherent in these automated decisionmaking systems (Kleinberg, et al., 2018).

In addition, the proposed ADMT regulations require businesses that use ADMT for significant decisions or extensive profiling to issue a pre-use notice, provide accessible opt-out options, and allow the consumer to easily access information about how the business utilized the ADMT to make decisions about them. These requirements apply to covered businesses unless they qualify under the security, fraud, and safety exception, the human appeal exception, and the evaluation exception, which can apply under specific circumstances enumerated in the proposed regulations. More specifically, the evaluation exception applies to businesses using ADMT, only if they evaluated their use of ADMT to ensure that it works as intended and does not discriminate and implement safeguards, such as those against discrimination. This anti-discriminatory component of the proposed regulations has a wide range of applications in business practices and activities. For instance, the proposed regulations may reduce incentives for businesses with employment vacancies to depend on online media to screen their job candidates unless they evaluate their ADMT to ensure that it works as intended and is not discriminatory (Acquisti & Fong, 2020). Therefore, businesses that use ADMT for significant decisions will have to make sure that the ADMT fulfills its intended purpose and does not exhibit discrimination bias.

Consumers and businesses stand to gain significantly from avoiding discrimination and bias in ADMT. When businesses are required to, or voluntarily, evaluate for and safeguard against discrimination, they can achieve a more diverse workforce linked to higher productivity and lower rates of employee turnover (Swonk, n.d.; Mallory, et al., 2017). Evaluating ADMT for bias will also help reduce social inequality, as opportunities are not restricted by specific demographics in different sectors of the economy, such as in lending, labor, and housing (Zuiderveen Borgesius, 2018). Avoiding discrimination based upon protected characteristics can improve the health outcomes of individuals and could avoid the lifetime costs associated with deteriorating mental and physical health due to such biases and stress (Elias & Paradies, 2016; Weidinger, et al., 2021). In addition, with more conscientious use of consumer data, companies will pivot from personalizing prices based on individual profiling practices to focusing on market insights derived from analyzing more broad-based consumer behavior (Dube & Misra, 2023; Seele, Dierksmeier, Hofstetter, and Schultz, 2019). Evaluating ADMT for bias will also help reduce social inequality, as opportunities are not restricted by specific demographics in different sectors of the economy, such as in lending, labor, and housing (Zuiderveen Borgesius, 2018). Avoiding discrimination based upon protected characteristics can improve the health outcomes of individuals and could avoid the lifetime costs associated with deteriorating mental and physical health due to such biases and stress (Elias & Paradies, 2016; Weidinger, et al., 2021).

3.4.4 Updates to Existing CCPA Regulations

The proposed regulations updating the existing CCPA regulations ("updates") require businesses to provide additional transparency to consumers and to take additional steps to implement consumers' requests to correct. For example, when a business processes a consumer's request to correct and the business is not the source of the information that the consumer contends is inaccurate, the updates require the business to provide the consumer with the name of the source, or to inform the source that the information is incorrect and must be corrected. These requirements benefit consumers and businesses by addressing incorrect information at its source and preventing the further proliferation of inaccurate information about the consumer. In addition, when a business denies a consumer's request to correct, the updates require the business to inform the consumer that, upon the consumer's request, the business will note (internally and to any person with whom the business discloses, shares, or sells the PI), that the consumer contests the accuracy of the PI. This additional transparency gives consumers the ability to dispute the accuracy of PI about them when the business discloses, shares, or sells the PI. These updates give consumers more control over their PI and can lead businesses to take additional steps to avoid the proliferation of inaccurate information and optimize their data collection practices.

The proposed updated requirements will significantly reduce the amount of time, effort, and other resources that consumers need to expend to exercise their privacy rights. These proposed updates to existing CCPA regulations clarify the requirements mandating businesses to inform consumers about their privacy rights to request access and evaluate their collected PI. The rules require businesses to simplify and clarify access to information about business privacy practices and compliance, especially with the process to opt-out of data sharing and sales. Under the updates, consumers will also be more informed about what they can do if they are not satisfied with the businesses' response to their request to delete at least part of the consumer's PI. With this additional clarity about consumer privacy and data protection and improved access to information, consumers can save time and face less confusion and stress when practicing their privacy rights.

3.5 How Many Consumers are Impacted by the Proposed Regulations?

The proposed regulations will impact all consumers in California. Businesses within California possess PI of millions of consumers and they will possess the PI of many more in future years. The proposed regulations provide additional privacy protections and enhanced ability of current and future Californians to exercise their privacy rights. Quantified benefits of reduced cybersecurity risks directly impact consumers whose PI is possessed, shared, sold. To the extent proposed regulations lead to higher prices of goods and services provided by covered businesses, the proposed regulations will impact consumers of those goods and services. Unquantified benefits of proposed regulations will yield benefits to all individuals within California.

Every individual in California is considered a consumer and the DOF estimate of California's population released in April 2024 is 39,128,162.[28] We use this figure as the Agency's estimate of consumers impacted by the proposed regulations.

[28] See DOF California population forecast at https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Demographics/Documents/E-1_2024_Press_Release.pdf

4 Macroeconomic Impacts

4.1 Methodology

The economy-wide impacts of the proposed Agency regulations have been evaluated using the BEAR forecasting model. The BEAR Model is a dynamic computable general equilibrium (CGE) model of the California economy. The Model simulates detailed patterns of demand, supply, and resource allocation across the state, estimating economic outcomes over the period 2027-2036. For this SRIA, the BEAR Model is aggregated to 50 production sectors and commodity groups with detailed representation of those most likely affected by the proposed regulations.

The current version of the BEAR Model is calibrated using 2022 IMPLAN data for the California economy.[29] Assessments of the baseline, proposed regulations and alternatives considered use the DOF conforming forecasts from July 2024. The conforming forecast represents current official assumptions regarding baseline GDP growth and population forecasts for California (Appendix 3). The BEAR Model structure is summarized in Appendix 4 and fully documented in BEAR (2024).

4.2 Inputs to the Macroeconomic Impacts Assessment

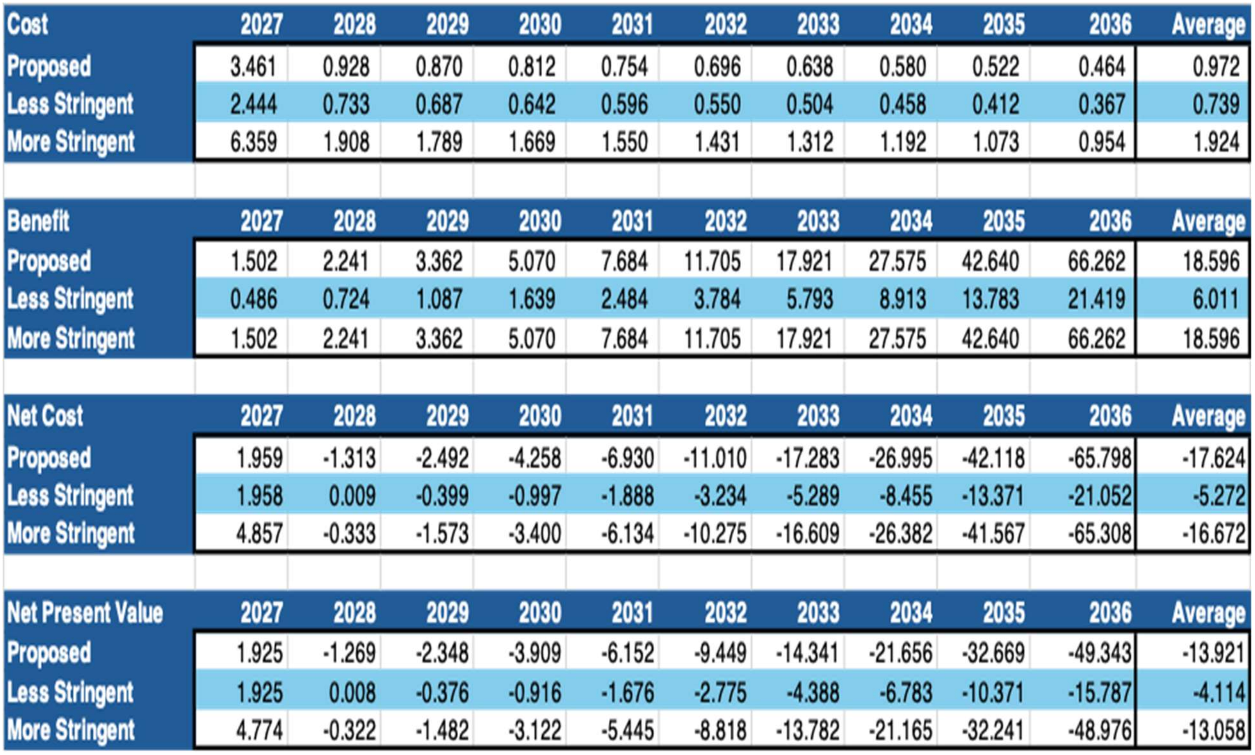
In addition to the BEAR Model's detailed database on the baseline structure of the California economy, the macroeconomic assessment is calibrated to incremental, sector-specific direct costs and benefits that would arise from the proposed regulations considered by the Agency for this rulemaking package. These are summarised in a simple macroeconomic tabulation (Table 4-1) below, but here only direct regulatory costs and benefits are aggregated across the economy. Three scenarios are assessed for macroeconomic impacts: (1) the proposed regulations (Proposed), (2) a Less Stringent Alternative, and (3) a More Stringent Alternative. Details regarding the estimation of these are given below.

These aggregates are relevant only in terms of general magnitudes, and it would be misleading to interpret them further for two reasons. Firstly, costs and benefits fall on different stakeholders, leading to much more complex adjustment patterns and welfare effects. Second, annual direct effects are only a fraction of economywide, intertemporal impacts. These regulatory effects would be mediated and amplified by linkages to and from directly impacted stakeholders across the economy, leading to so-called "multiplier" impacts that must be explicitly included in a SRIA for major regulations. These effects are captured in two steps, first making detailed allocations of direct costs and benefits to regulated sectors and beneficiaries of enhanced consumer privacy protection, and then implementing these with the CGE model as dynamic counterfactuals to the 2027-2036 reference or baseline scenario. One feature of Table 4-1 that does deserve emphasis is

[29] The IMPLAN database is extensively documented at https://implan.com/

the strong shift over time from positive to negative net costs. This is driven by the sustained accumulation of benefits from stronger protections for consumers' privacy, in the wake of relatively modest costs over time for the more protective adjustments made by businesses subject to the proposed regulations. The estimated total costs over the decade assessed is $9.725 billion. The estimated total quantified benefits over the decade are $186 billion.

Table 4-1: Aggregation of Direct Regulatory Costs and Benefits



Cost	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Proposed	3.461	0.928	0.870	0.812	0.754	0.696	0.638	0.580	0.522	0.464	0.972
Less Stringent	2.444	0.733	0.687	0.642	0.596	0.550	0.504	0.458	0.412	0.367	0.739
More Stringent	6.359	1.908	1.789	1.669	1.550	1.431	1.312	1.192	1.073	0.954	1.924
Benefit	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Proposed	1.502	2.241	3.362	5.070	7.684	11.705	17.921	27.575	42.640	66.262	18.596
Less Stringent	0.486	0.724	1.087	1.639	2.484	3.784	5.793	8.913	13.783	21.419	6.011
More Stringent	1.502	2.241	3.362	5.070	7.684	11.705	17.921	27.575	42.640	66.262	18.596
Net Cost	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Proposed	1.959	-1.313	-2.492	-4.258	-6.930	-11.010	-17.283	-26.995	-42.118	-65.798	-17.624
Less Stringent	1.958	0.009	-0.399	-0.997	-1.888	-3.234	-5.289	-8.455	-13.371	-21.052	-5.272
More Stringent	4.857	-0.333	-1.573	-3.400	-6.134	-10.275	-16.609	-26.382	-41.567	-65.308	-16.672
Net Present Value	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Proposed	1.925	-1.269	-2.348	-3.909	-6.152	-9.449	-14.341	-21.656	-32.669	-49.343	-13.921
Less Stringent	1.925	0.008	-0.376	-0.916	-1.676	-2.775	-4.388	-6.783	-10.371	-15.787	-4.114
More Stringent	4.774	-0.322	-1.482	-3.122	-5.445	-8.818	-13.782	-21.165	-32.241	-48.976	-13.058

Note: All figures in 2022 $ billions.

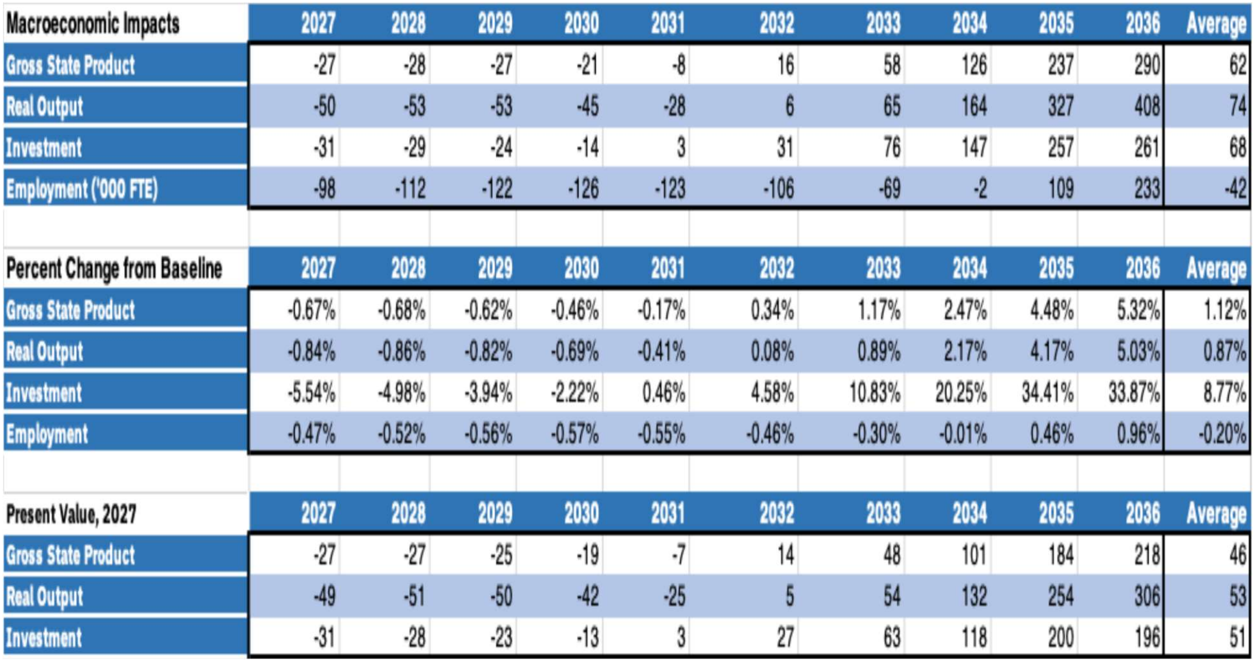
More comprehensive indirect and induced effects are simulated as they would pass through supply and expenditure chains and institutional transfers across the California economy. All these effects are captured by the BEAR Model and then aggregated into net economic impacts, annually over the period 2027-2036, and discounted using the Federal Funds rate as a proxy for intertemporal time preference.[30] The BEAR Model (CGE) operates with real prices only, so inflation is not considered directly, and all the macroeconomic variables reported below should be interpreted as 2022 base year dollar ($) adjusted.

[30] See, e.g. https://fred.stlouisfed.org/series/FEDFUNDS

4.3 Macroeconomic Estimates

The following tables present macroeconomic impact assessments of the proposed regulations or the two alternatives of Less Stringent and More Stringent regulations.

Table 4-2: Economy-Wide Impacts of Proposed Regulation



Macroeconomic Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-28	-27	-21	-8	16	58	126	237	290	62
Real Output	-50	-53	-53	-45	-28	6	65	164	327	408	74
Investment	-31	-29	-24	-14	3	31	76	147	257	261	68
Employment ('000 FTE)	-98	-112	-122	-126	-123	-106	-69	-2	109	233	-42
Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-0.67%	-0.68%	-0.62%	-0.46%	-0.17%	0.34%	1.17%	2.47%	4.48%	5.32%	1.12%
Real Output	-0.84%	-0.86%	-0.82%	-0.69%	-0.41%	0.08%	0.89%	2.17%	4.17%	5.03%	0.87%
Investment	-5.54%	-4.98%	-3.94%	-2.22%	0.46%	4.58%	10.83%	20.25%	34.41%	33.87%	8.77%
Employment	-0.47%	-0.52%	-0.56%	-0.57%	-0.55%	-0.46%	-0.30%	-0.01%	0.46%	0.96%	-0.20%
Present Value, 2027	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-27	-25	-19	-7	14	48	101	184	218	46
Real Output	-49	-51	-50	-42	-25	5	54	132	254	306	53
Investment	-31	-28	-23	-13	3	27	63	118	200	196	51

Notes: All figures in 2022 $ billions. Employment in full-time equivalent (FTE) thousands.

The salient feature of the proposed regulations (Table 4-2) is a reversing trend in economic growth, from net reductions to net increases with respect to the baseline. Referring back to Table 4-1, this can be seen as a lagged response to the reversal of net direct costs from positive to negative. Simply put, the proposed regulations have high upfront costs, but low ongoing costs, and this shows up in early years as a net cost to the economy. The benefits of stronger protections for consumers' privacy far outweigh these costs in the long run, improving the investment climate and eventually overcoming cumulative adjustment costs incurred by California businesses required to comply with proposed regulations, their workers, and their supply chain partners. Note that the modelling of investment impacts does not even take account of the vast array of unquantified benefits described above. The driver of the investment reversal in these results is enhanced private net income and savings from reductions in cybercrimes. If we could include such behavioral adaptations and direct beneficial qualitative impacts, the macroeconomic benefits would be far more dramatic.

This direct impact is composed of a $3.5 billion direct cost to businesses subject to the CCPA, resulting in a much larger adverse impact on investment (-$31 billion) because it directly impacts cost and profit margins. The investment shortfall reduces current output (-$50 billion), employment (-98,000 FTE), and gross state product or GSP (-$27 billion).

From this point, the trend moderates and then reverses as the limited set of quantified benefits consistently exceed costs. Note that the first year of compliance is by far the most adverse; incremental costs after that are modest in the next few years until the quantified benefits of proposed regulations overcomes them and becomes growth positive.

The investment shock amplifies the apparent adjustment in 2027, but it must be emphasized that, compared to the underlying baseline scenario, these adjustments present no threat of a macroeconomic reversal. Percent impacts on all other macroeconomic aggregates are less than 1% of 2027–2028 values, which in the baseline grow at nearly 4%. Projected employment impacts are less than half of one percent. In other words, across the decade considered, implementing the proposed regulations would never cause negative aggregate growth for California, and would end that decade as a source of economic stimulus.

It should also be emphasized that costs and benefits are structurally quite different and generally accrue to different groups of stakeholders. It should be emphasized that, while costs are incurred by the California businesses impacted by the proposed regulations, as set forth in Section 2, benefits are much more general and have been allocated across all sectors of the economy in proportion to value added. Other rules for targeting benefits could yield different microeconomic impacts, but there are no reliable predictions of the detailed incidence of cybercrime damages over next decade, let alone patterns of crimes averted by proposed regulations. The main growth (investment, employment, etc.) drivers for these results are macroeconomic, however, driven by the aggregate savings-investment constraint applied to baseline labor and capital allocation patterns.

We estimate that California businesses, as set forth in Section 2, incur costs, including increased labor costs and reduced profits and statewide saving. Impacted businesses accruing across the entire economy (not only to impacted businesses) and represent savings from the reduction in a subset of cybercrimes, as set forth in Section 3. In the absence of detailed information about exact patterns of future cybercrime, these savings are allocated across all sectors in proportion to their value-added. In fact, we do not know exactly who will experience the savings from reduced cybercrimes, but the cumulative savings are substantial (averaging $18.6 billion in annual avoided losses) and will support higher economywide investment levels through the same aggregate saving-investment balance. This leads to incremental and compounded average investment growth of about 3.1% annually and 34% over a decade. This improvement in the investment climate is fully consistent with the intention of proposed regulations to further protect consumers' privacy (including by protecting their personal information) and facilitate responsible innovation.

4.4 Creation or Elimination of Jobs within California

The aggregate job results follow the slower growth trend in early years of the period considered, yielding an average of about 98,000 fewer new jobs in 2027, measured as

Full-Time Equivalent (FTE or 1,900 working hours) units per year. While there are disparate employment impacts to the information and professional, scientific, and technical services industries compared to industries not subject to the proposed regulations, the sectors covered are likely to be more skill-intensive, finding alternate employment is expected to be easier for these workers. When a proposed regulation represses investment in such a sector, job losses are more easily offset than in less-skilled sectors. At the aggregate statewide level, however, these changes are nearly imperceptible (less than one quarter of one percent on average) and would be extremely unlikely to reverse baseline job growth in these dynamic industries or across California. Over the decade evaluated, the proposed regulations are expected to lead to significant long-term job creation.

4.5 Incentives for Innovation

Substantive industry regulations can often be expected to induce innovation. The specific innovation drivers vary from case to case, but can include investment to offset expected incremental costs, perceived competitive disadvantage, or taking advantage of emergent opportunities. In situations like the present case, where existing practices are subjected to restrictions, it is reasonable to expect incumbent firms to invest in product differentiation to offset any loss of business arising from the restriction in question.

4.6 Creation of New Businesses or Elimination of Existing Businesses within California

The implications of the proposed regulations for California businesses required to comply are intuitive. Compliance costs directly impinge on profit and investment, may divert business to out-of-state alternatives, and offer incentives for product differentiation and industry consolidation. In all cases, however, expected revenue shortfalls are single-digit percentages of baseline values. Thus, it is unlikely that any but the most specialized companies will see significant revenue risk, and in any case, they have the options of diversification, innovation, and consolidation to offset this. Only time will tell how this adjustment plays out at the firm level, where it depends on detailed initial conditions and many behavioral considerations outside the scope of this assessment.

4.7 Competitive Advantages or Disadvantages for Businesses Currently Doing Business within California

To the extent that the proposed regulations restrict business activity of California businesses covered by the CCPA, the proposed regulations will impact the businesses' individual competitiveness against out-of-state competitors. We do not possess sufficiently detailed enterprise-level data to predict these competitive adjustments at the microeconomic level. Having said that, however, our analysis indicates that California itself will not face significant percentage firm revenue and employment declines, which are generally in the low single-digit percentages of a more rapidly growing baseline trend.

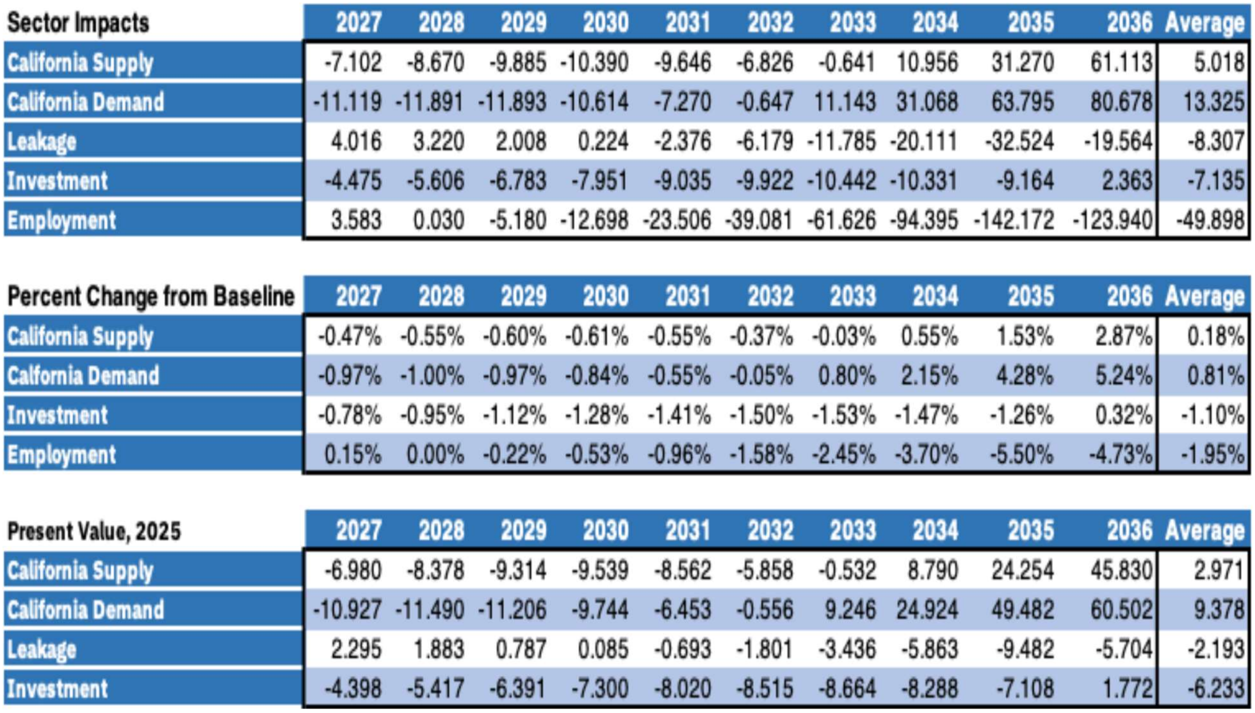
These findings can be seen in Table 4-3 below, which shows values of supply, demand, and related estimates for the 2-digit NAICS sectors, mainly 51-Information and 52-Finance.

Several features deserve closer examination. Note that this accounting will net out all commercial “diversion” between enterprises within a given NAICS category, since more detailed data are not available on economy-wide linkages for these activities. As expected, the proposed regulations increase cost and reduce revenue for some covered California businesses, reducing in-state revenue and investment in the sector, but this decline averages less than one-tenth of one percent in each year (not compounded) over the forecast period. Despite a net loss of revenue, the larger NAICS sector appears to be quite resilient, retaining over 99% of revenue on a baseline growing at over 3.5%.[31] Meanwhile, recall that a limited quantification of benefits, which accrue across the entire economy, are only partially reflected in these sector results, are large, and eventually more than offset the macroeconomic costs of sector compliance.

With respect to out-of-state competition, it is apparent from these results that, as demand falls less than supply in a given year, some business will be diverted across California’s border to available alternatives in other jurisdictions (denoted “Leakage” in the table). This is to be expected, but the net slowing of growth for commerce remains modest. Relative impacts (as a percent of revenue) for the sector are of course more substantial than in comparison to the statewide economy, but they remain modest.

[31] It should be emphasized that the BEAR Model (CGE) assumes labor and investment are mobile and can shift activities within the larger sector and across the economy relatively easily. Adjustments for individual workers and managers may be more challenging, but the macroeconomic model cannot track this.

Table 4-3: Sectoral Impacts of the Proposed Regulations



Sector Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
California Supply	-7.102	-8.670	-9.885	-10.390	-9.646	-6.826	-0.641	10.956	31.270	61.113	5.018
California Demand	-11.119	-11.891	-11.893	-10.614	-7.270	-0.647	11.143	31.068	63.795	80.678	13.325
Leakage	4.016	3.220	2.008	0.224	-2.376	-6.179	-11.785	-20.111	-32.524	-19.564	-8.307
Investment	-4.475	-5.606	-6.783	-7.951	-9.035	-9.922	-10.442	-10.331	-9.164	2.363	-7.135
Employment	3.583	0.030	-5.180	-12.698	-23.506	-39.081	-61.626	-94.395	-142.172	-123.940	-49.898

Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
California Supply	-0.47%	-0.55%	-0.60%	-0.61%	-0.55%	-0.37%	-0.03%	0.55%	1.53%	2.87%	0.18%
Calfornia Demand	-0.97%	-1.00%	-0.97%	-0.84%	-0.55%	-0.05%	0.80%	2.15%	4.28%	5.24%	0.81%
Investment	-0.78%	-0.95%	-1.12%	-1.28%	-1.41%	-1.50%	-1.53%	-1.47%	-1.26%	0.32%	-1.10%
Employment	0.15%	0.00%	-0.22%	-0.53%	-0.96%	-1.58%	-2.45%	-3.70%	-5.50%	-4.73%	-1.95%

Present Value, 2025	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
California Supply	-6.980	-8.378	-9.314	-9.539	-8.562	-5.858	-0.532	8.790	24.254	45.830	2.971
California Demand	-10.927	-11.490	-11.206	-9.744	-6.453	-0.556	9.246	24.924	49.482	60.502	9.378
Leakage	2.295	1.883	0.787	0.085	-0.693	-1.801	-3.436	-5.863	-9.482	-5.704	-2.193
Investment	-4.398	-5.417	-6.391	-7.300	-8.020	-8.515	-8.664	-8.288	-7.108	1.772	-6.233

Notes: All figures in 2022 $ billions. Employment in FTE thousands.

There are two basic structural adjustments in response to the proposed regulations. Firstly, covered sectors will have to adjust to compliance requirements, hiring additional workers and incurring higher labor costs in the short term, impinging on profit, investment, overall employment, and capital in the medium term.[32] The other salient impact comes from the demand side of the economy, as reductions in losses related to cybercrimes involving PI leads to increases in real income for individuals and enterprises. These savings will be recycled through demand, stimulating the economy through traditional multiplier linkages. In California, 70% of aggregate demand comes from households and 70% of household consumption goes to services. In other words, 49% of the incremental benefits from reduced cybercrime losses will be channeled to demand for labor-intensive services, far outweighing the job losses due to compliance costs in more capital-intensive compliant sectors. Financial benefits eventually strongly overtake costs of the proposed regulations over the decade considered, but expenditure shifting to more labor-intensive activities makes these regulations even more pro-employment.

4.8 Benefits to Health, Safety, and Welfare of California Residents, Worker Safety, and the State’s Environment and Quality of Life

The proposed regulations will enhance protection of consumer’s PI and increase the ability of individuals to exercise their privacy rights. Requirements to certify completion of

[32] The long-term pressure from compliance costs can also lead to industry restructuring (e.g. consolidation), but we do not model this explicitly.

RAs and CSAs will lead to reduced risks of cybercrimes against California businesses and individuals. Avoiding cybercrimes that involve consumer PI provides many types of benefits aside from financial measures as they include improvements to the health, safety, welfare, and quality of life for Californians.

Evaluating the cybersecurity risks with consumers' PI and the effectiveness of cybersecurity systems set up to combat these risks helps inform firms about how to enhance the safety of consumers' information and privacy. The cybersecurity improvements that California businesses make help alleviate the social and psychological costs that cybersecurity threats impose on California consumers. Effective cybersecurity programs also lower the costs that cybercrimes create. The reduced costs of production and business activity can lower the price of goods and services that consumers pay. This lower cost of consumption together with more cybersecurity and privacy-protective business practices leads to improvements of consumer welfare.

In addition, the assessment of risks related to how businesses manage and protect PI can lead to actions that help reduce those risks and improve safety within the workplace. Workers can focus their time and efforts on safety and efficiency, as they face less burden in protecting consumer PI, especially when businesses develop cybersecurity systems that mitigate risks and damages of cybercrimes.

Proposed requirements for training and uses of ADMTs will also provide benefits to businesses and individuals. Businesses that are required to evaluate their use of ADMTs will help ensure that the intended outcomes of those technologies are achieved, help improve efficiencies in the use of those ADMTs, and avoid a wide range of adverse outcomes associated with any of the unintended consequences of ADMTs implemented without such evaluations. The unintended consequences can include things like discrimination in both the hiring of employees and the provision of goods or services to consumers. Avoiding these adverse outcomes provides benefits in the workplace and to the health, safety, and welfare of California residents.

4.9 Extent to Which Costs or Benefits are Retained within the Business or by the Individual, and the Extent to Which They are Passed on to Others

The macroeconomic model captures economywide indirect and induced impacts of direct costs and benefits, as these extend along supply/input/factor demand chains from enterprises and expenditure/employment/income chains for consumers. Costs fall primarily on covered entities, but their response to these costs will impact others via supply chain linkages. Benefits fall on all actors in the economy, but particularly individuals who experience reduced financial losses with increased consumer privacy protection. The latter direct benefit impact will then trigger indirect and induced benefits in terms of real (retained) income, expenditure, and ongoing multiplier impacts.

What we see from such results for the proposed regulations is that long-term benefits significantly outweigh costs, overcoming sector pressures in the initial compliance phase and yielding above baseline economic growth by the end of the decade considered. It must be emphasized, however, that the costs and benefits of stronger protections for consumers' privacy generally fall on different stakeholders. Even though the latter eventually outweigh the former in the aggregate, individual adjustment experience will be quite heterogeneous. For those bearing costs, there will be strong incentives to adapt and innovate, but the BEAR Model does not capture these second-order behavioral impacts.

4.10 Small Business Impacts

To estimate the impact on small businesses we must first identify the portion of businesses subject to the proposed regulations that meet the small business classification. Under California Government Code § 14837, a small business is defined as a business that is:

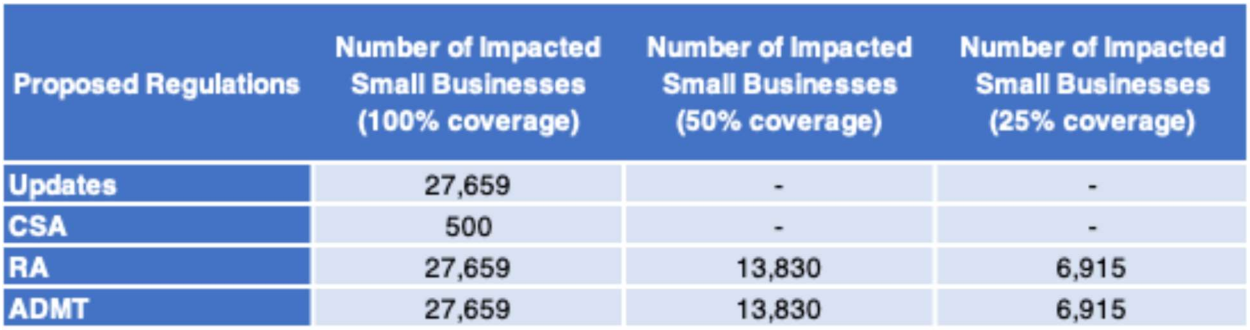
- Independently owned and operated.
- Not dominant in its field of operation.
- Has fewer than 100 employees.
- Has annual revenue <$15M

We are unable to identify which firms are independently owned and operated or which are dominant in their field, so we use the employee and revenue restrictions to identify small businesses. To estimate the number of small businesses covered by the proposed regulations we first restrict our sample of businesses to those that do not meet the annual revenue threshold of $28M that requires compliance with the proposed regulations.[33] This means the only small businesses that could be covered by the proposed regulations would need to either receive >50% of their annual revenue from sale/share of PI or buy/sell/share the PI of >100K people/consumers per year.

Second, we restrict the number of businesses we estimate to be required to comply with the proposed regulations to those with <100 employees. In total this produces the following estimated number of firms that are considered small businesses. All of these small businesses come from PI-intensive sectors and buy/sell/share/process high volumes of PI. Table 4-4 below shows the estimated number of affected small businesses.

[33] As described above several of the proposed regulations apply to businesses with annual revenue $>28M. For the subset of businesses that are covered but have annual revenue <$28M we do not have revenue estimates but assume their annual revenues are <$15M. Our estimates of small business coverage are therefore likely to be overinclusive.

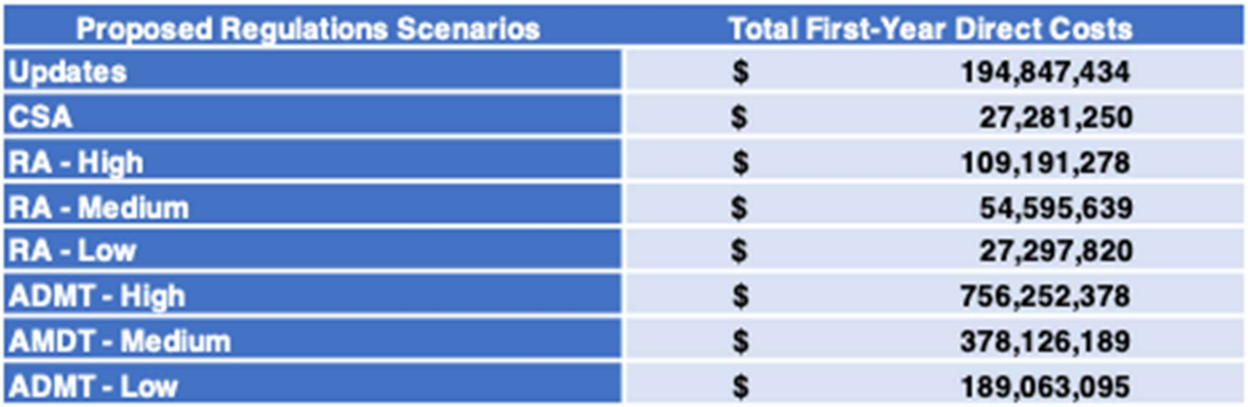
Table 4-4: Number of Small Businesses Required to Comply with Proposed Regulations



Proposed Regulations	Number of Impacted Small Businesses (100% coverage)	Number of Impacted Small Businesses (50% coverage)	Number of Impacted Small Businesses (25% coverage)
Updates	27,659	-	-
CSA	500	-	-
RA	27,659	13,830	6,915
ADMT	27,659	13,830	6,915

Using the same methodology as the previous sections above this yields the following small business costs shown in Table 4-5 below. Estimated initial costs for small businesses ranges from $7,045 to $92,896. The estimated ongoing cost for small businesses is $19,317.

Table 4-5: Direct First-Year Regulatory Costs to Small Businesses



Proposed Regulations Scenarios	Total First-Year Direct Costs
Updates	$ 194,847,434
CSA	$ 27,281,250
RA - High	$ 109,191,278
RA - Medium	$ 54,595,639
RA - Low	$ 27,297,820
ADMT - High	$ 756,252,378
AMDT - Medium	$ 378,126,189
ADMT - Low	$ 189,063,095

Note: All figures in 2022 $

4.11 Increase or Decrease of Investment in California

Although the macroeconomic impact on state investment is small, in percentage terms, it is a strong indicator of sentiment and momentum of the overall California economy. The investment climate will be affected by proposed regulations in different directions, with three primary factors to consider. First, high initial compliance costs will discourage other investment at least temporarily among covered businesses. Second, options for innovation to reduce reliance on PI may be taken up by such firms, competitors, or new entrants. Many firms will choose to use privacy-enhancing technologies, which will increase both investment and innovation. Finally, higher costs for individual firms may lead to consolidation of PI management services. We have estimated the investment impacts in both the macro and sectoral contexts above, but no data is currently available to predict changes in levels of innovation or business productivity.

5 Fiscal Impacts

This proposed rulemaking package contains multiple requirements for California businesses that will create a new workload for staff at the Agency and Department of Justice (DOJ). New workload at these agencies results from implementation of proposed regulations and can be separated into two categories: 1) one-time staff work to build the frameworks necessary to receive multiple required documents from more than 52,000 California businesses and letters of complaint from an uncertain number of California consumers; and 2) ongoing staff workload to review submitted documents and respond to submittals on a case-by-case basis.

Frameworks for Document Submissions to the Agency

The proposed regulations require covered California businesses to submit documents to the Agency. The frequency of document submittals will be annual or intermittently, when businesses have a material change that requires a revision or addition to their existing document submissions.

The Agency will need to develop a web portal or similar capability to receive submissions of the following documents from California businesses and consumers:

- Certification of Completion of a Cybersecurity Audit – Section 7124
- Certification of Conducting a Risk Assessment – Section 7157(b)(1)
- Abridged Form of Risk Assessment – Section 7157(b)(2)
- Letter of Consumer Complaint – Section 7022(g)(5) and others

5.1 One-Time Fiscal Impacts

The Agency's Information Technology Division will need to develop a web portal to accept the documents referenced above. The Agency estimates this would require 120 hours of an Information Technology Specialist I ($8,500 salary x 1.75 benefits and operating equipment and expenses) at $14,875 per month. Total one-time fiscal impact for creating these four webforms is 4 x $14,875 x (120/160) **= $44,625**. Note there will be minor workload for the ongoing maintenance of the webforms.

5.2 Ongoing Fiscal Impacts

The proposed regulations will create a new ongoing workload for Agency staff to administer submittals of documents to the Agency's website, review submissions, and respond to submitted documents on a case-by-case basis. The magnitude of these ongoing fiscal impacts is difficult to estimate at this time. Since this is a new requirement for businesses the quality of submitted documents and the required level of staff review is uncertain. The number of submissions that will need further review and preparation of an agency response is also highly uncertain. Finally, the time and staff expertise required to respond on a case-by-case basis will also be highly variable and uncertain until the Agency gains a level of experience with management of these new types of document submittals.

We estimate that 52,326 certifications of conducting an RA and an abridged form of the RA will be submitted via the Agency web portal. We estimate 25,167 Certification of Completion of Cybersecurity Audit will be submitted by covered California businesses. Finally, we estimate that approximately 350 consumer letters of complaint will be submitted annually to the Agency and some fraction of this number to the DOJ as well. The DOJ expects this impact to be insignificant to their current workload. This estimate of the Agency is based on the annual number of complaints the Agency has received and assumes a 25 percent increase with the form easily available to consumers to file a complaint. We estimate the fiscal impact of this ongoing workload scenario to be 50 percent time of an Associate Governmental Program Analyst ($6,000/mo. salary x 1.75 benefits and operating equipment and expenses) at $10,500 for an annual cost of **$63,000**.

We estimate each consumer complaint letter will require 1.5 hours for an Attorney ($11,500/mo. salary x 1.75 benefits and operating equipment and expenses at a monthly cost of $20,125) to review and respond as necessary. This results in an ongoing fiscal impact of 350 x ($20,125/160 hours x 1.5 hours) = **$66,035**.

Total Estimated Fiscal Impacts

One-time fiscal costs: $44,625

Ongoing fiscal costs: $63,000+$66,035 = $129,035

Estimated total fiscal impacts: **$44,625** one-time cost and **$129,035** ongoing costs.

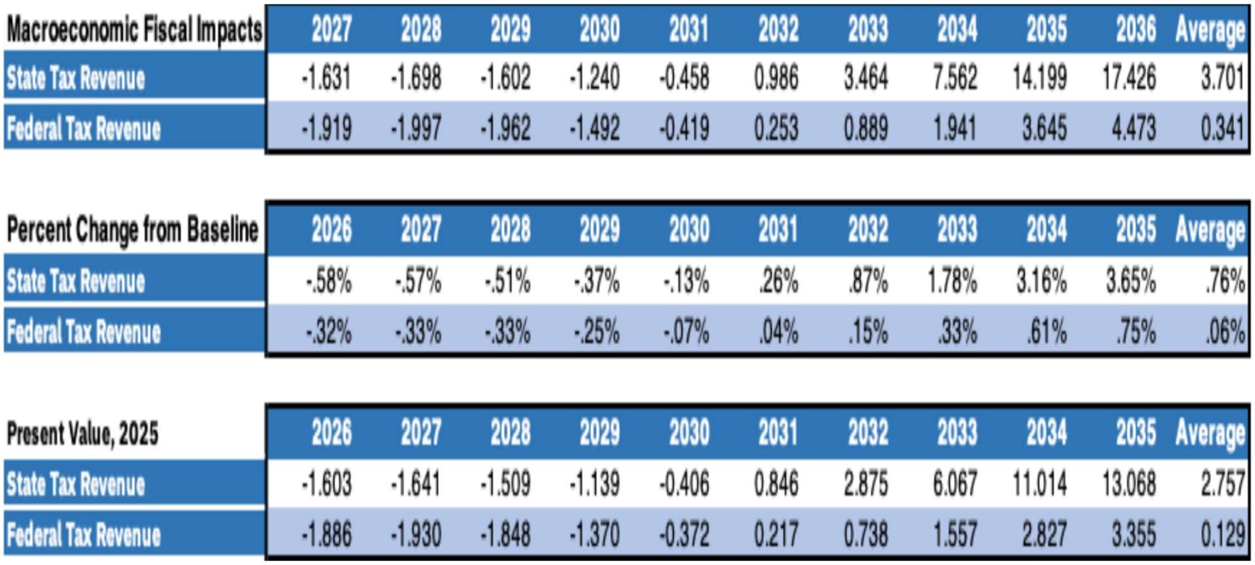
5.3 State and Federal Revenues

One might expect that reductions of firm revenue and GSP would be accompanied by lower revenue from many income-based fiscal sources. The BEAR CGE Model estimates that proposed regulations will result in small net changes, following aggregate net income adjustments from negative to positive trends in state and federal revenue. These effects are summarized in Table 5-1. A much more detailed fiscal model would be needed to trace all the components of these revenue gains. Suffice for the present to say that they are net effects of many public income and expenditure decisions and in any case are small to negligible relative to baseline fiscal values.

Having said this, revenues do increase with the pro-growth trend as the regulatory benefits exceed the costs. This result is reflected in the Model's treatment of fiscal accounting, assuming constant average tax and expenditure rates for the main drivers of government balance sheets (income, sales, property, etc.). The BEAR Model follows separate federal, state, and local accounts, but all are assumed to adjust linearly to changes their underlying bases. Likewise, we do not differentiate local fiscal institutions by location, but only divide them according to their place in the fiscal hierarchy. For example, counties are associated collectively with property tax, but not identified individually with localities, and their expenditures are assumed to be aggregated across the state and linear in revenue. Municipalities are associated collectively with sales tax, and state and federal government with income tax, but all rates are averaged and assumed constant.

As can be seen in Table 5-1, state tax revenues are negative the first five years following implementation, but then become increasingly positive through the remainer of the period of analysis. In percentage terms, the negative impact to state tax revenues in 2027 is small at –0.6% of baseline revenue, but rises to over 3.5% by 2036 with the decadal trend contributing about three quarters of one percent to average revenue.

Table 5-1: Estimated State and Federal Revenue Impacts of the Proposed Regulations



Macroeconomic Fiscal Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
State Tax Revenue	-1.631	-1.698	-1.602	-1.240	-0.458	0.986	3.464	7.562	14.199	17.426	3.701
Federal Tax Revenue	-1.919	-1.997	-1.962	-1.492	-0.419	0.253	0.889	1.941	3.645	4.473	0.341

Percent Change from Baseline	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	Average
State Tax Revenue	-.58%	-.57%	-.51%	-.37%	-.13%	.26%	.87%	1.78%	3.16%	3.65%	.76%
Federal Tax Revenue	-.32%	-.33%	-.33%	-.25%	-.07%	.04%	.15%	.33%	.61%	.75%	.06%

Present Value, 2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	Average
State Tax Revenue	-1.603	-1.641	-1.509	-1.139	-0.406	0.846	2.875	6.067	11.014	13.068	2.757
Federal Tax Revenue	-1.886	-1.930	-1.848	-1.370	-0.372	0.217	0.738	1.557	2.827	3.355	0.129

Note: All figures in 2022 $ billions.

5.4 Local Government

Generally, benefits of the proposed regulations can be expected to be relatively uniform across the state's population, while costs will be concentrated in urban areas. We currently lack the detailed spatial information to elucidate this heterogeneity, however. In the present analysis, there may be short-term net costs to local governments if net costs to businesses reduce their property or excise taxes, but these short-term negative effects become significantly outweighed by positive effects. Given the very small percentage changes involved, it is reasonable to assume local governments can cover these temporary gaps. Regardless of timing of net fiscal effects on local governments, these impacts are not reimbursable.

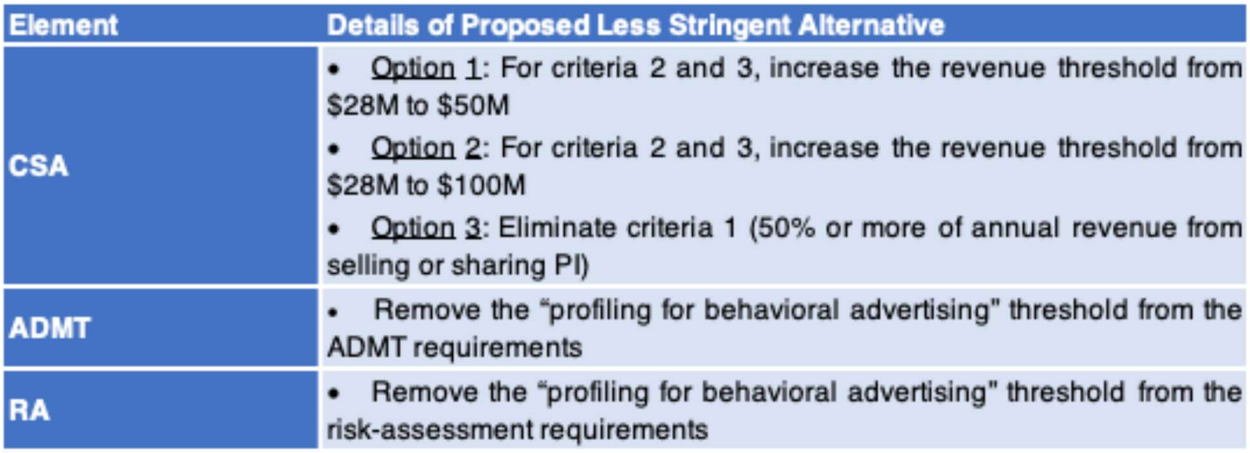
6 Economic Impacts of the Regulatory Alternatives

In addition to the baseline and the proposed regulations, DOF's guidelines require agencies to evaluate, if possible, at least two feasible alternatives. Thus, each SRIA should include three scenarios. One of the two alternatives should include regulatory actions that could be interpreted as less stringent or imposing lower direct costs. This is meant to represent a "second best" option in terms facilitating compliance while providing lesser benefits than the proposed regulation. The second alternative should be considered more stringent, with higher direct costs and perhaps higher direct benefits. To the extent possible, the baseline and alternatives should be analyzed with the same quantitative rigor as the proposed regulations. For this analysis, macroeconomic results for the proposed regulations reflect impacts assuming the DOF's projected growth rates for all relevant sectors of the California economy.

6.1 Less Stringent Alternatives

The Agency has proposed a series of changes to the proposed regulations that collectively represent a less stringent alternative (Table 6-1). To develop a single less stringent alternative scenario we average costs across the three CSA less stringent alternatives and combine them with the less stringent ADMT and RA alternatives.

Table 6-1: Elements of the Less Stringent Alternative



Element	Details of Proposed Less Stringent Alternative
CSA	• Option 1: For criteria 2 and 3, increase the revenue threshold from $28M to $50M • Option 2: For criteria 2 and 3, increase the revenue threshold from $28M to $100M • Option 3: Eliminate criteria 1 (50% or more of annual revenue from selling or sharing PI)
ADMT	• Remove the "profiling for behavioral advertising" threshold from the ADMT requirements
RA	• Remove the "profiling for behavioral advertising" threshold from the risk-assessment requirements

Estimated Coverage

The factors considered for less stringent alternatives in Table 6-1 will reduce the number of covered California businesses. The total number of businesses impacted by the proposed CSA regulations under a less stringent alternative, when only businesses with >$100 million in annual revenues are required to conduct CSAs, is estimated to be 7,258.

For ADMT and RA, to estimate the share of businesses that do behavioral advertising we assume that all companies that sell or share PI participate in behavioral advertising. Additionally, we assume that companies that display advertisements will be excluded in a less stringent alternative that removes the profiling for behavioral advertising for the ADMT and RA components of this regulatory alternative.

Based on our analysis of a sample of websites, we estimate that 18% of CCPA covered firms are sharing or selling PI. In principle, this is a subset of all businesses that do behavioral advertising because businesses could also use ADMT to profile consumers for behavioral advertising without selling or sharing PI. However, in practice we found few examples of firms displaying advertisements. We conducted a manual random review of 100 sampled websites and found that none of the websites in our sub-sample displayed advertisements. While some firms obviously do display advertisements, the share of covered firms with targeted advertisements appears to be sufficiently small that none of the businesses in our sub-sample did targeting advertisement. Our random sub-sample of covered businesses did not happen to include websites that most commonly display advertisements such as media or services that are provided for free (such as web-search). Instead, it included many large companies that are covered because they generate annual revenue >$28M. Therefore, our sampling scheme that included manual review of a sub-sample of 100 websites likely did not have enough power to detect the share of covered businesses that use targeted advertisements.

Another approach to estimate the portion of firms that use PI for advertising would be to look at industry sectors. The information sector – NAICS 51 – contains publishers, social media, and search. This sector is overinclusive as it also contains non-relevant industries such as movies, radio, and telecommunications. We find that 10.2% of firms subject to CCPA are in NAICS 51. Given none of firms found in our manually reviewed sub-sample, and the fact that the sector is overinclusive we estimate that 2% of CCPA firms use PI for advertising. We therefore assume that only 2% of firms do advertising solely with PI that they collected from their own distinctly-branded websites, applications, or services—or bought from another business—and do not share or sell the PI with others. It would be this 2% of firms that would be excluded under the less stringent RA alternative; and 20% of firms would be excluded under the less stringent ADMT alternative. This assumes that these businesses do not meet any of the other threshold criteria under the RA and ADMT proposed regulations.

6.1.1 Direct Costs of the Less Stringent Alternative

First year direct costs of the proposed CSA regulations are estimated as written and for the regulatory alternatives. As written the proposed regulations total costs will be **$2.05 billion**. We estimate costs for the less stringent alternative of CSA regulations to range from **$1.07 billion** to **$2.02 billion**.

First year direct costs of the proposed regulations for RA and ADMT are estimated as the total number of impacted businesses multiplied by an hourly rate multiplied by the number of hours needed to meet regulatory compliance. Total costs are estimated using the following approach.

Approximate costs of the less stringent alternative are a reduction from proposed regulations.

Proposed Regulations:

Costs = [# of businesses subject to regulation] * [hourly rate] * [number of hours]

Calculation inputs:

1. # businesses subject to regulation
    a. 100% of CCPA businesses (high) [52,326]
    b. 50% of CCPA businesses (medium) [26,163]
    c. 25% of CCPA businesses (low) [13,082]
2. Hourly rate
    a. RA [Average of $25.91, $42.67, and $100.61]
    b. ADMT [$91.14]
3. Number of Hours
    a. RA [120]
    b. ADMT [300]

Less Stringent Alternative:

Costs = [# of businesses subject to regulation] * [hourly rate] * [number of hours]

Calculation inputs:

1. # businesses subject to regulation
    a. RA
        i. 98% of CCPA businesses (high) [51,279]

        ii. 49% of CCPA businesses (medium) [25,640]
        iii. 24.5% of CCPA businesses (low) [12,820]
    b. ADMT
        i. 80% of CCPA businesses (high) [41,861]
        ii. 40% of CCPA businesses (medium) [20,930]
        iii. 20% of CCPA businesses (low) [10,465]

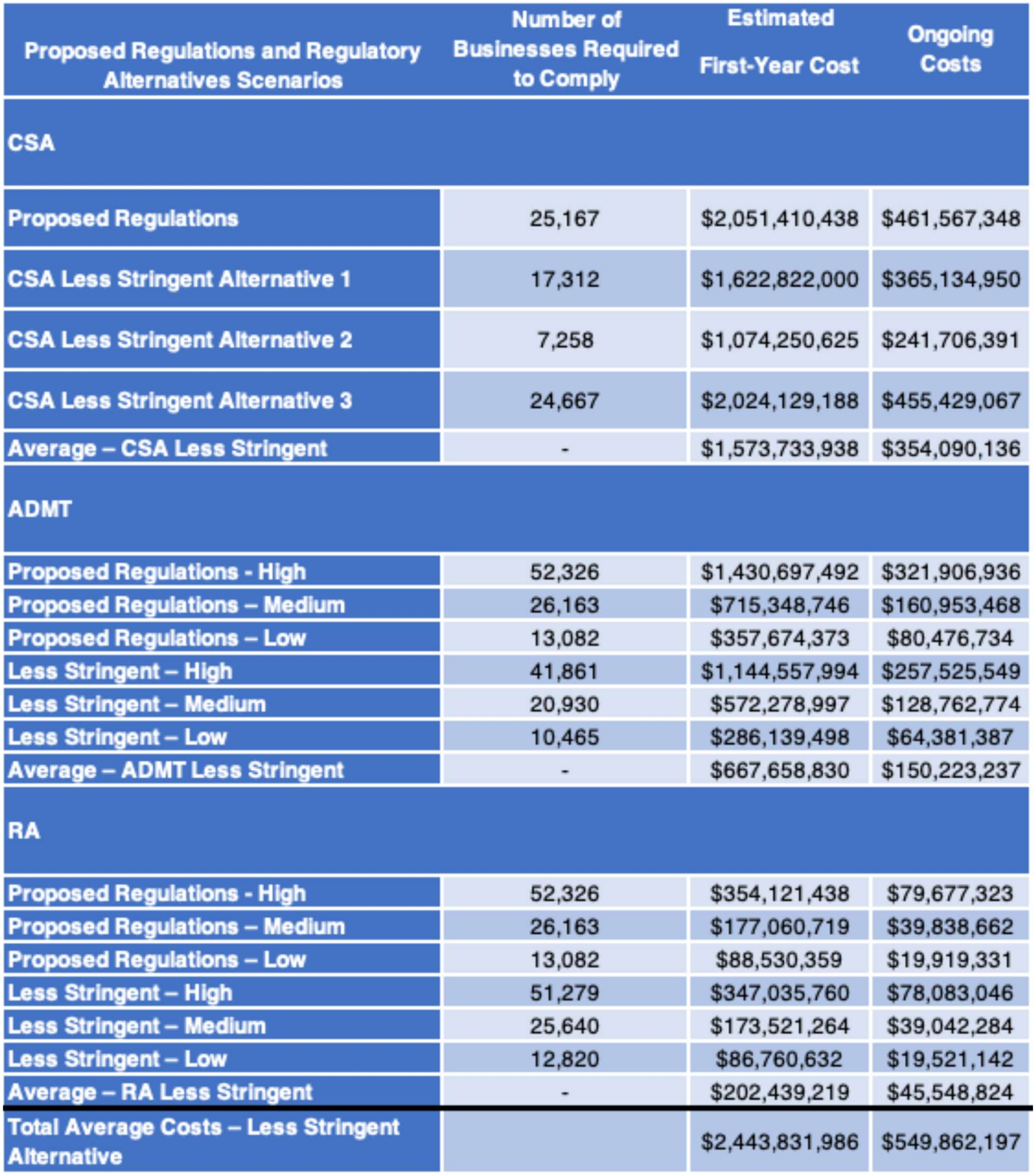
2. Hourly rate
    a. RA [Average of $25.91, $42.67, and $100.61]
    b. ADMT [$91.14]
3. Number of Hours
    a. RA [120]
    b. ADMT [300]

For RA, under the proposed regulations we estimate total first-year costs to be between $89 and $354 million. For the less stringent alternative we estimate first-year costs to be between **$87 million** and **$347 million**.

Ongoing costs are estimated using the same approach as used for the analysis of proposed regulations. We estimate that subsequent years will represent 15 – 30% of total year one compliance costs, with the higher compliance cost threshold occurring in earlier years before gradually falling. We present the average of this range (22.5%) in the ongoing cost column. Ongoing costs range from $19.9 million to $80 million for the RA proposed regulations and from **$19.5 million** to **$78 million** in the less stringent alternative.

For ADMT, under the proposed regulations we estimated first-year costs to be between $358 million and $1.43 billion with ongoing costs ranging between $80 million to $322 million. For the less stringent alternative we estimate first-year costs to be between **$286 million** and **$1.1 billion**. Ongoing costs range between **$64 million** to **$258 million**.

Table 6-2: Estimated Number of California Businesses Required to Comply with Proposed Regulations and Regulatory Alternatives and Estimated Costs



Proposed Regulations and Regulatory Alternatives Scenarios	Number of Businesses Required to Comply	Estimated First-Year Cost	Ongoing Costs
CSA			
Proposed Regulations	25,167	$2,051,410,438	$461,567,348
CSA Less Stringent Alternative 1	17,312	$1,622,822,000	$365,134,950
CSA Less Stringent Alternative 2	7,258	$1,074,250,625	$241,706,391
CSA Less Stringent Alternative 3	24,667	$2,024,129,188	$455,429,067
Average – CSA Less Stringent	-	$1,573,733,938	$354,090,136
ADMT			
Proposed Regulations - High	52,326	$1,430,697,492	$321,906,936
Proposed Regulations – Medium	26,163	$715,348,746	$160,953,468
Proposed Regulations – Low	13,082	$357,674,373	$80,476,734
Less Stringent – High	41,861	$1,144,557,994	$257,525,549
Less Stringent – Medium	20,930	$572,278,997	$128,762,774
Less Stringent – Low	10,465	$286,139,498	$64,381,387
Average – ADMT Less Stringent	-	$667,658,830	$150,223,237
RA			
Proposed Regulations - High	52,326	$354,121,438	$79,677,323
Proposed Regulations – Medium	26,163	$177,060,719	$39,838,662
Proposed Regulations – Low	13,082	$88,530,359	$19,919,331
Less Stringent – High	51,279	$347,035,760	$78,083,046
Less Stringent – Medium	25,640	$173,521,264	$39,042,284
Less Stringent – Low	12,820	$86,760,632	$19,521,142
Average – RA Less Stringent	-	$202,439,219	$45,548,824
Total Average Costs – Less Stringent Alternative		$2,443,831,986	$549,862,197

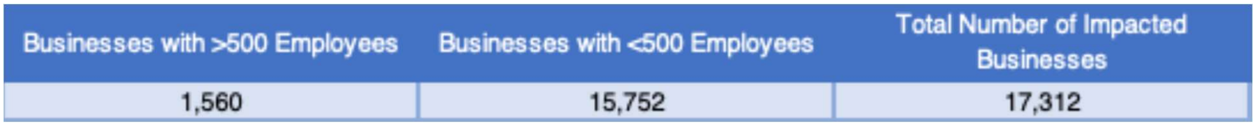
Note: All figures as number of firms or 2022 $

The estimated average total costs over the decade assessed of the Less Stringent Alternatives is $7.8 billion.

6.1.2 Direct Benefits of the Less Stringent Alternative

Direct benefits were estimated for three less stringent alternatives considered for CSA requirements. The first alternative considered for CSAs (Less Stringent Alternative 1) would cover businesses with greater than $50 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year or businesses that generated more than 50% of their revenue from PI in the preceding year. The total number of impacted businesses in Less Stringent Alternative 1 is 17,312. As noted earlier, according to figures in the 2023 IBM Data Breach Report the average cost of a data breach for a business with more than 500 employees is about 1.5 times the average cost of a data breach for a business with less than 500 employees. Further breakdown of the number of impacted businesses based on whether the number of employees is >500 or <500 is given in Table 6-3 below:

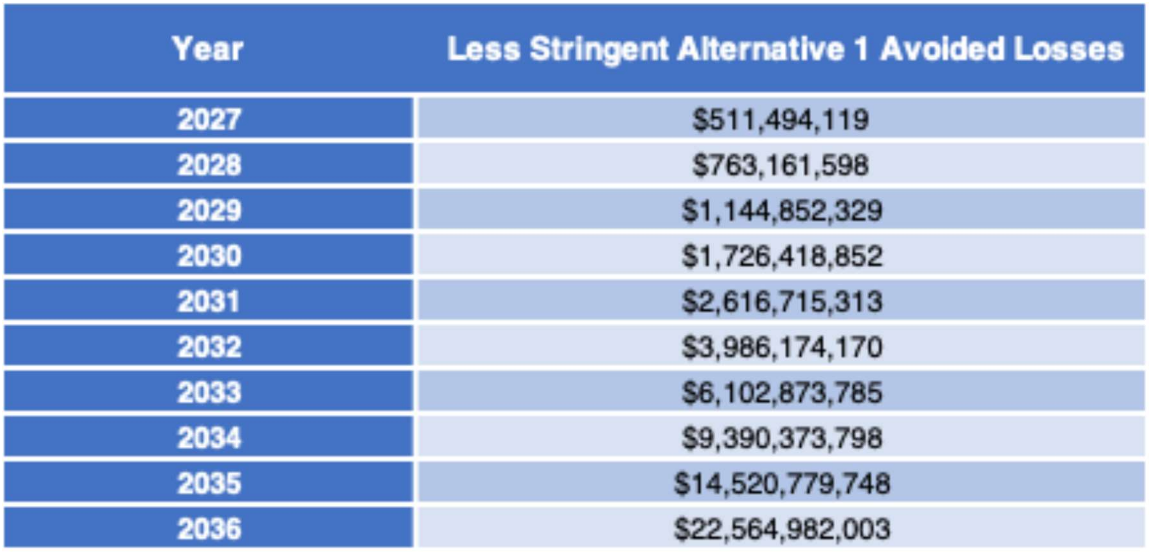
Table 6-3: Impacted Businesses Based on Number of Employees in Less Stringent Alternative 1



Businesses with >500 Employees	Businesses with <500 Employees	Total Number of Impacted Businesses
1,560	15,752	17,312

We estimate annual avoided losses in the Less Stringent Alternative 1 to range over time from 2027 to 2036 as shown in Table 6-4 below.

Table 6-4: Annual Avoided Monetary Losses in Less Stringent Alternative 1 (2027-2036)



Year	Less Stringent Alternative 1 Avoided Losses
2027	$511,494,119
2028	$763,161,598
2029	$1,144,852,329
2030	$1,726,418,852
2031	$2,616,715,313
2032	$3,986,174,170
2033	$6,102,873,785
2034	$9,390,373,798
2035	$14,520,779,748
2036	$22,564,982,003

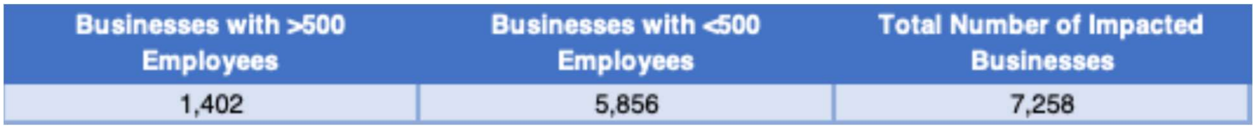
Note: All figures in 2022 $

The expected annual avoided losses (direct benefits) in Less Stringent Alternative 1 will be over **$511.5 million** in 2027 and rise to over **$22.6 billion** by the year 2036. These estimates are associated with businesses with greater than $50 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year or generated more than 50% of their revenue from the sharing or sale of PI in the preceding year. Because cybercrime risk reduction is associated with CSA and RA requirements and RA alternative regulations do not match up with CSA alternative regulations in terms of number of covered firms, we only scale direct benefits of avoided losses based upon the number of businesses impacted by alternative CSA regulations.

A second less stringent alternative that was considered for CSA requirements would cover only businesses with greater than $100 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year; and businesses that generated more than 50% of their revenue from sharing or sale of PI in the preceding year (Less Stringent Alternative 2).

The total number of impacted businesses in Less Stringent Alternative 2 is 7,258. Further breakdown of the number of impacted businesses based on whether the number of employees is >500 or <500 is given in Table 6-5 below:

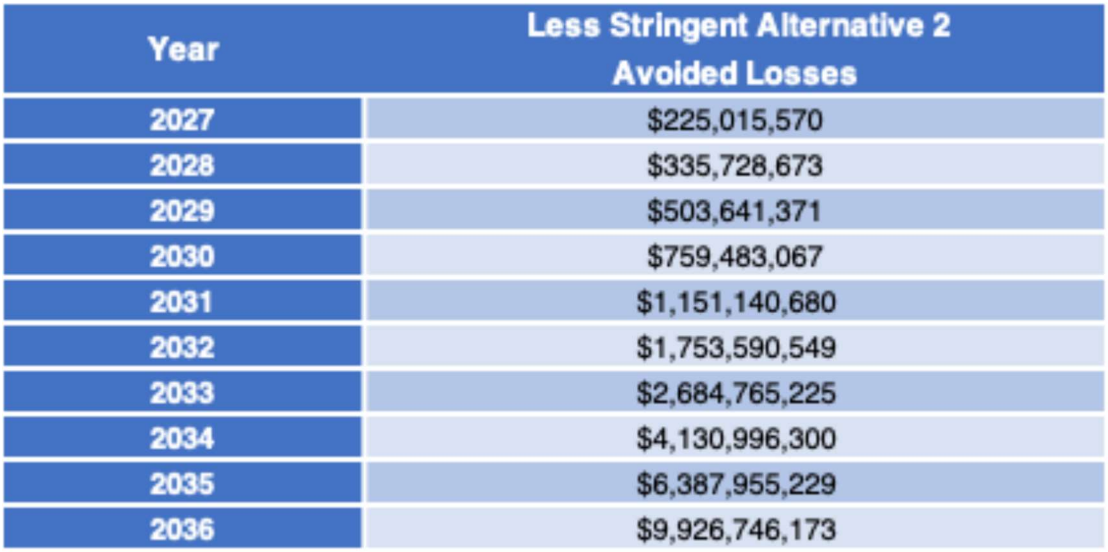
Table 6-5: Breakdown of Impacted Businesses Based on Number of Employees in Less Stringent Alternative 2



Businesses with >500 Employees	Businesses with <500 Employees	Total Number of Impacted Businesses
1,402	5,856	7,258

Based on the number of impacted businesses, we estimate annual avoided losses in the Less Stringent Alternative 2 to range over time from 2027 to 2036 as shown in Table 6-6 below.

Table 6-6: Annual Avoided Monetary Losses in Less Stringent Alternative 2 (2027-2036)



Year	Less Stringent Alternative 2 Avoided Losses
2027	$225,015,570
2028	$335,728,673
2029	$503,641,371
2030	$759,483,067
2031	$1,151,140,680
2032	$1,753,590,549
2033	$2,684,765,225
2034	$4,130,996,300
2035	$6,387,955,229
2036	$9,926,746,173

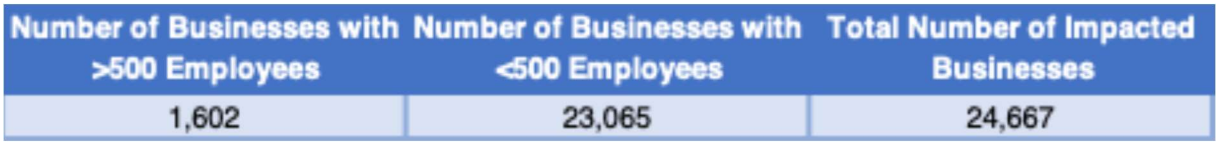
Note: All figures in 2022 $

The lower bound of expected annual avoided cybercrime losses resulting from the Less Stringent Alternative 2 will be over $225 million in 2027. These avoided losses rise to more than $9.9 billion by the year 2036. The direct benefit estimates are associated with the smallest number of impacted businesses, namely those with greater than $100 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year; or generated more than 50% of their annual revenue from the sharing or sale of PI in the preceding year. As noted with the Less Stringent Alternative 1 above, direct benefits are scaled based upon CSA alternative scenarios in terms of number of covered firms.

A third less stringent alternative for CSA coverage was considered and it has coverage of businesses with greater than $28 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year; but no criteria for minimum annual revenue from the sharing or sale of PI (Less Stringent Alternative 3).

The total number of impacted businesses in More Stringent Alternative 3 is 24,667. Further breakdown of the number of impacted businesses based on whether the number of employees is >500 or <500 is given in Table 6-7 below:

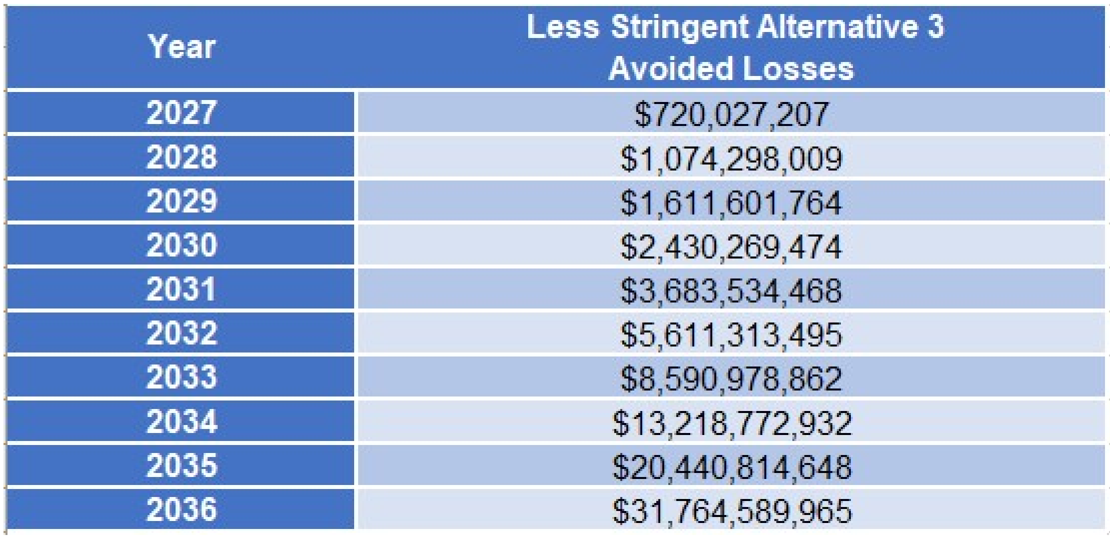
Table 6-7: Breakdown of Impacted Businesses Based on Number of Employees in Less Stringent Alternative 3



Number of Businesses with >500 Employees	Number of Businesses with <500 Employees	Total Number of Impacted Businesses
1,602	23,065	24,667

Based on the number of impacted businesses, we estimate annual avoided losses in the Less Stringent Alternative 3 ranges over time from 2027 to 2036 as shown in Table 6-8 below.

Table 6-8: Annual Avoided Monetary Losses in Less Stringent Alternative 3 (2027-2036)



Year	Less Stringent Alternative 3 Avoided Losses
2027	$720,027,207
2028	$1,074,298,009
2029	$1,611,601,764
2030	$2,430,269,474
2031	$3,683,534,468
2032	$5,611,313,495
2033	$8,590,978,862
2034	$13,218,772,932
2035	$20,440,814,648
2036	$31,764,589,965

Note: All figures in 2022 $

The lower bound of expected annual avoided losses in Less Stringent Alternative 3 will be over **$720 million** in 2027 and rises to about **$32 billion** by the year 2036. These estimates are associated with businesses having greater than $28 million in annual revenue that processed the PI of 250,000 or more consumers or households or processed the SPI of 50,000 or more consumers in the preceding year; but no criteria for revenue from the sharing or sale of PI. No quantitative data is available for direct benefits of proposed or alternative ADMT regulations.

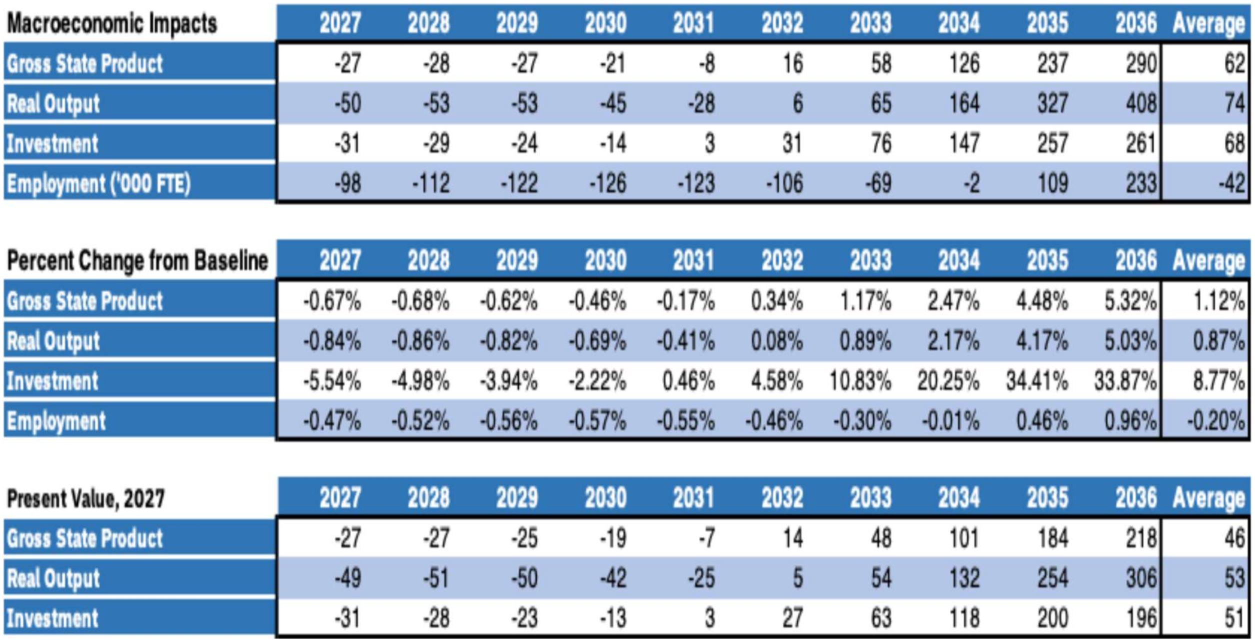
Taking the average across the three Less Stringent Alternatives we estimate that total quantifiable benefits for a Less Stringent Alternative will be **$486 million** in 2027 rising to **$21.4B** in 2036. The average total quantified benefits of the Less Stringent Alternatives are $60.1 billion.

6.1.3 Macroeconomic Estimates for the Less Stringent Alternative

The regulatory alternatives are compared with proposed regulations in Tables 6-9 through 6-11 below, showing the annual macroeconomic impacts against baseline values over the evaluation period 2027-36. At the outset, it must be emphasized that, because the California economy is assumed to be growing over this period without the proposed regulations, all three regulatory scenarios would see rising macroeconomic aggregates over time and this table only shows small negative or modest positive adjustments to that upward trajectory.

Table 6-9: Macroeconomic Impacts of the Proposed Regulations

(Table 4-2 restated)



Macroeconomic Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-28	-27	-21	-8	16	58	126	237	290	62
Real Output	-50	-53	-53	-45	-28	6	65	164	327	408	74
Investment	-31	-29	-24	-14	3	31	76	147	257	261	68
Employment ('000 FTE)	-98	-112	-122	-126	-123	-106	-69	-2	109	233	-42

Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-0.67%	-0.68%	-0.62%	-0.46%	-0.17%	0.34%	1.17%	2.47%	4.48%	5.32%	1.12%
Real Output	-0.84%	-0.86%	-0.82%	-0.69%	-0.41%	0.08%	0.89%	2.17%	4.17%	5.03%	0.87%
Investment	-5.54%	-4.98%	-3.94%	-2.22%	0.46%	4.58%	10.83%	20.25%	34.41%	33.87%	8.77%
Employment	-0.47%	-0.52%	-0.56%	-0.57%	-0.55%	-0.46%	-0.30%	-0.01%	0.46%	0.96%	-0.20%

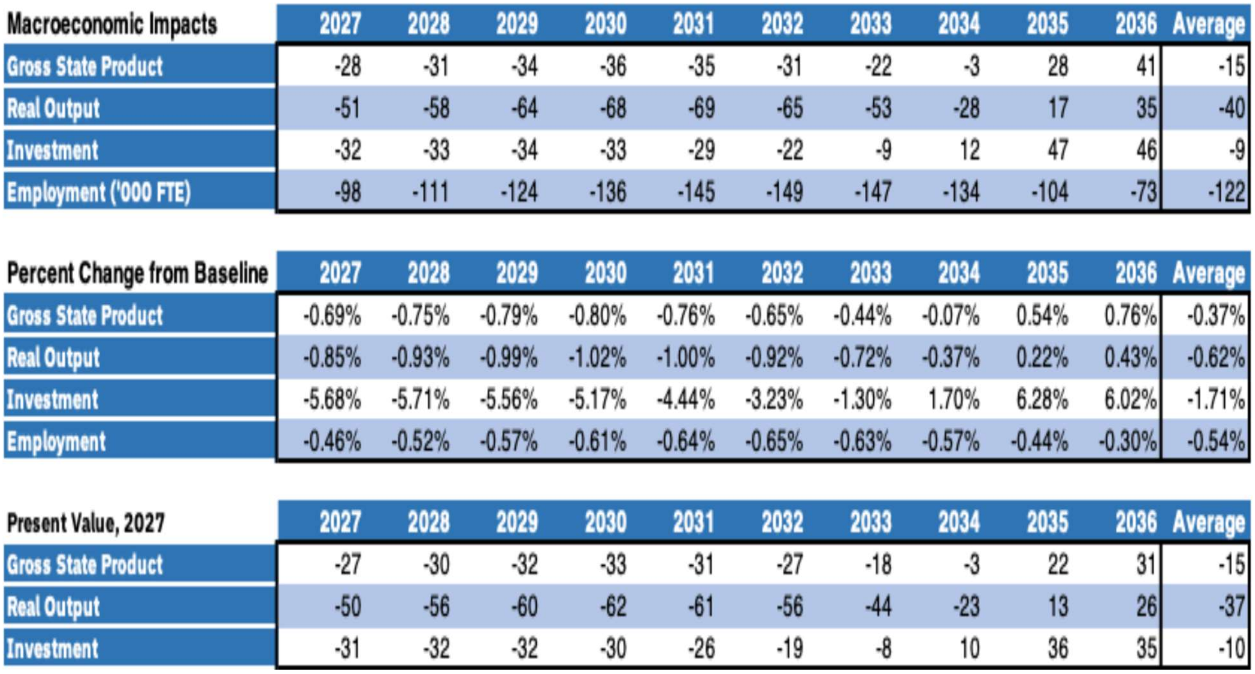
Present Value, 2027	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-27	-25	-19	-7	14	48	101	184	218	46
Real Output	-49	-51	-50	-42	-25	5	54	132	254	306	53
Investment	-31	-28	-23	-13	3	27	63	118	200	196	51

Notes: All figures in 2022 $ billions. Employment in FTE thousands.

The proposed regulations have already been discussed above. Again, the less stringent alternative (Table 6-10) uses the direct cost and benefit average across all less stringent alternatives. This establishes a single less stringent alternative for purposes of macroeconomic impact assessment.

The resulting estimates indicate more modest adjustment costs, which can be more acceptable to businesses subject to the proposed regulations, but the long-term net economic benefits across the California economy are significantly lower with the less stringent alternative than with the proposed regulations. Estimated annual and cumulative macroeconomic benefits still offset macroeconomic costs (except employment in the long run), but if the primary intention of the proposed regulations is stronger protections for consumers' privacy, small savings on compliance costs may not be justified if it forgoes more substantial benefits to California businesses and individuals.

Table 6-10: Macroeconomic Impacts of the Less Stringent Alternative



Macroeconomic Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-28	-31	-34	-36	-35	-31	-22	-3	28	41	-15
Real Output	-51	-58	-64	-68	-69	-65	-53	-28	17	35	-40
Investment	-32	-33	-34	-33	-29	-22	-9	12	47	46	-9
Employment ('000 FTE)	-98	-111	-124	-136	-145	-149	-147	-134	-104	-73	-122

Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-0.69%	-0.75%	-0.79%	-0.80%	-0.76%	-0.65%	-0.44%	-0.07%	0.54%	0.76%	-0.37%
Real Output	-0.85%	-0.93%	-0.99%	-1.02%	-1.00%	-0.92%	-0.72%	-0.37%	0.22%	0.43%	-0.62%
Investment	-5.68%	-5.71%	-5.56%	-5.17%	-4.44%	-3.23%	-1.30%	1.70%	6.28%	6.02%	-1.71%
Employment	-0.46%	-0.52%	-0.57%	-0.61%	-0.64%	-0.65%	-0.63%	-0.57%	-0.44%	-0.30%	-0.54%

Present Value, 2027	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-27	-30	-32	-33	-31	-27	-18	-3	22	31	-15
Real Output	-50	-56	-60	-62	-61	-56	-44	-23	13	26	-37
Investment	-31	-32	-32	-30	-26	-19	-8	10	36	35	-10

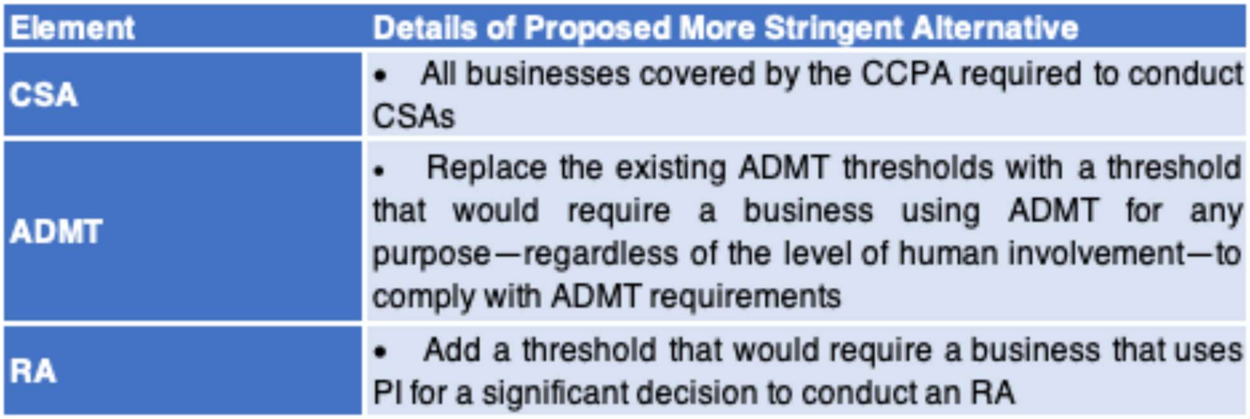
Notes: All figures in 2022 $ billions. Employment in FTE thousands.

The Agency finds that no alternatives were presented to or considered by the Agency that would be more effective in carrying out the purpose of these proposed regulations or would be as effective and less burdensome to affected private persons than these proposed regulations. Consistent with the above, while the less stringent alternative is associated with more modest adjustment costs for businesses, it is also associated with weaker protections for consumers' privacy.

6.2 More Stringent Alternative

The Agency has considered a series of changes to the proposed regulations that collectively represent a more stringent alternative. The proposed alternatives represent more inclusive coverage criteria and increase the compliance requirements. Overall, this yields a more inclusive number of impacted businesses, as well as additional compliance depending on the alternative and regulatory element (Table 6-11).

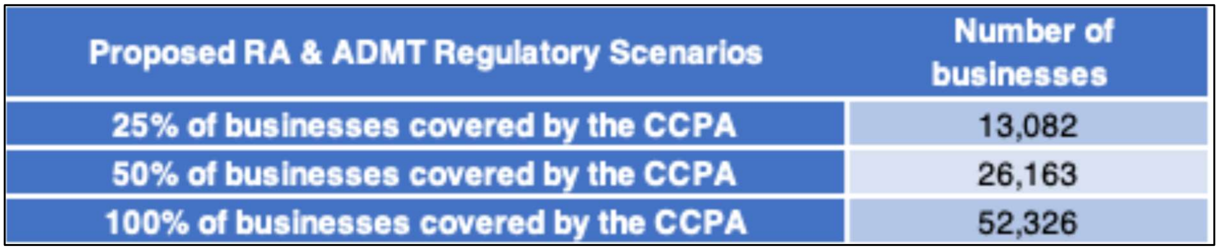
Table 6-11: Elements of the More Stringent Alternative



Element	Details of Proposed More Stringent Alternative
CSA	- All businesses covered by the CCPA required to conduct CSAs
ADMT	- Replace the existing ADMT thresholds with a threshold that would require a business using ADMT for any purpose—regardless of the level of human involvement—to comply with ADMT requirements
RA	- Add a threshold that would require a business that uses PI for a significant decision to conduct an RA

For CSA regulations the more stringent alternative corresponds to all businesses covered by the CCPA (52,326). As a reminder, under the proposed regulations we estimate the number of businesses required to comply with the proposed ADMT and RA regulations using a scenario analysis with low, medium, and high proportions of CCPA covered businesses meeting the coverage threshold. These estimates are 25%, 50%, and 100%, which correspond to 13,082, 26,163, and 52,326 California businesses, respectively.

Table 6-12: Number of California Businesses Required to Comply with the Proposed RA & ADMT Regulations



Proposed RA & ADMT Regulatory Scenarios	Number of businesses
25% of businesses covered by the CCPA	13,082
50% of businesses covered by the CCPA	26,163
100% of businesses covered by the CCPA	52,326

The more stringent alternative would increase the number of California businesses required to comply with ADMT and RA requirements. We are unable to estimate the exact amount of increased coverage, so as a conservative estimate we assume that 100% of California businesses subject to the CCPA will be covered. That is, only the high proportion scenario analysis is appropriate for the more stringent alternative. This implies 52,326 firms will fall under the more stringent alternative for both ADMT and RA. This number of impacted firms is used to assess direct costs and benefits of the more stringent alternative. Additionally, the more stringent alternative will require increased compliance activities. Again, data on the expected increase in hours is not known, so we use additional scenario analysis. Lacking data on the additional number of hours needed to complete the more stringent requirements with increased processing activities, we use the following scenarios: high (increase of 100% of hours), medium (increase of 50% of hours), and low (increase of 25% of hours).

6.2.1 Direct Costs of the More Stringent Alternative

Following the methodology described in the Direct Costs of Less Stringent Alternative section, we estimate costs for the more stringent CSA regulatory alternative to be $3.53B. CSA cost estimates assume businesses that already use a cybersecurity framework to assess their cybersecurity programs will have 30% lower implementation costs than businesses not currently using a cybersecurity framework to assess their cybersecurity programs.

Costs of the proposed RA and ADMT regulatory package are estimated as the total number of impacted businesses multiplied by an hourly rate multiplied by the number of hours needed to meet regulatory compliance. Total costs are estimated using the following approach.

Approximate costs for the More Stringent Alternative are:

Costs = [# of businesses subject to regulation] * [hourly rate] * [number of hours]

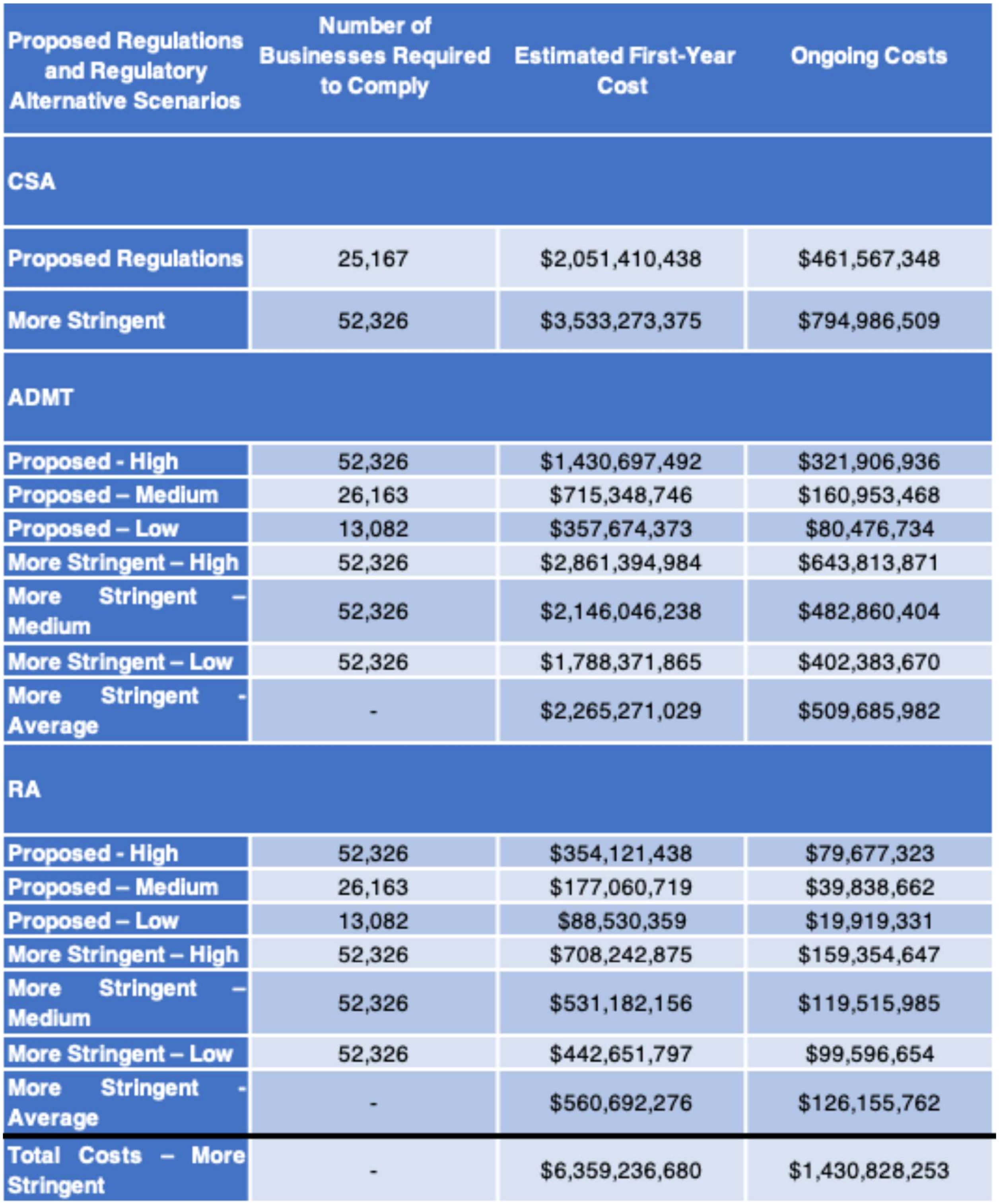
Calculation inputs:

1. # businesses subject to regulation
   a. 100% of CCPA businesses [52,326]
2. Hourly rate
   a. RA [Average of $25.91, $42.67, and $100.61]
   b. ADMT [$91.14]
3. Number of Hours
   a. 100% More (high)
      i. RA [240]
      ii. ADMT [600]
   b. 50% More (Medium)
      i. RA [180]
      ii. ADMT [450]
   c. 25% More (Low)
      i. RA [150]
      ii. ADMT [375]

For RA, under the proposed regulations we estimate total first-year costs to be between $89 and $354 million and for the more stringent alternative we estimate first-year costs to be between **$443 million** to **$708 million**. Ongoing costs are estimated using the same approach as in our analysis of the proposed regulations. We estimate that subsequent years will represent 15 – 30% of total year one compliance costs, with the higher compliance cost threshold occurring in earlier years before gradually falling. We present the average of this range (22.5%) in the ongoing cost column. Ongoing costs range from **$20 million** to **$80 million** for the proposed regulations and **$100 million** to **$159 million** in the more stringent alternative scenario.

For ADMT, under the proposed regulations we estimate first-year costs to be between $358 million and $1.43 billion and ongoing costs range between $80 million to $322 million. For the more stringent alternative we estimate first-year costs to be between **$1.8 billion** to **$2.9 billion** and ongoing costs range between **$402 million** to **$644 million** (Table 6-13).

Table 6-13: Estimated Number of California Businesses Required to Comply with Proposed Regulations and Regulatory Alternatives and Estimated Costs



Proposed Regulations and Regulatory Alternative Scenarios	Number of Businesses Required to Comply	Estimated First-Year Cost	Ongoing Costs
CSA			
Proposed Regulations	25,167	$2,051,410,438	$461,567,348
More Stringent	52,326	$3,533,273,375	$794,986,509
ADMT			
Proposed - High	52,326	$1,430,697,492	$321,906,936
Proposed – Medium	26,163	$715,348,746	$160,953,468
Proposed – Low	13,082	$357,674,373	$80,476,734
More Stringent – High	52,326	$2,861,394,984	$643,813,871
More Stringent – Medium	52,326	$2,146,046,238	$482,860,404
More Stringent – Low	52,326	$1,788,371,865	$402,383,670
More Stringent - Average	-	$2,265,271,029	$509,685,982
RA			
Proposed - High	52,326	$354,121,438	$79,677,323
Proposed – Medium	26,163	$177,060,719	$39,838,662
Proposed – Low	13,082	$88,530,359	$19,919,331
More Stringent – High	52,326	$708,242,875	$159,354,647
More Stringent – Medium	52,326	$531,182,156	$119,515,985
More Stringent – Low	52,326	$442,651,797	$99,596,654
More Stringent - Average	-	$560,692,276	$126,155,762
Total Costs – More Stringent	-	$6,359,236,680	$1,430,828,253

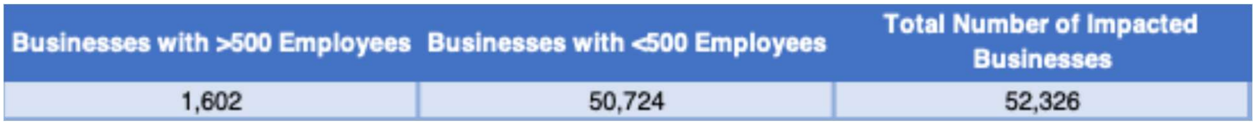
Note: All figures as number of firms or 2022 $

Combining costs associated with CSA, ADMT, and RA, total costs of the more stringent alternative averaged across the low/medium/high scenarios are estimated to be **$6.4 billion** in the first year. Total ongoing costs of this alternative are estimated to be **$1.4 billion** per year. The total costs of the More Stringent Alternative over the decade assessed is $19.6 billion.

6.2.2 Direct Benefits for More Stringent Alternatives

The Agency considered a more stringent alternative for CSA coverage that would require all businesses covered by the CCPA to conduct CSAs. Due to the inability to separate cybercrime risk reduction benefits between firms conducting CSAs and RAs and the inability to quantify direct benefits of ADMT regulations, the total number of impacted businesses in the more stringent alternative is 52,326 or the same as proposed regulations for RAs. Further breakdown of the number of impacted businesses based on whether the number of employees is >500 or <500 is given in Table 6-14 below:

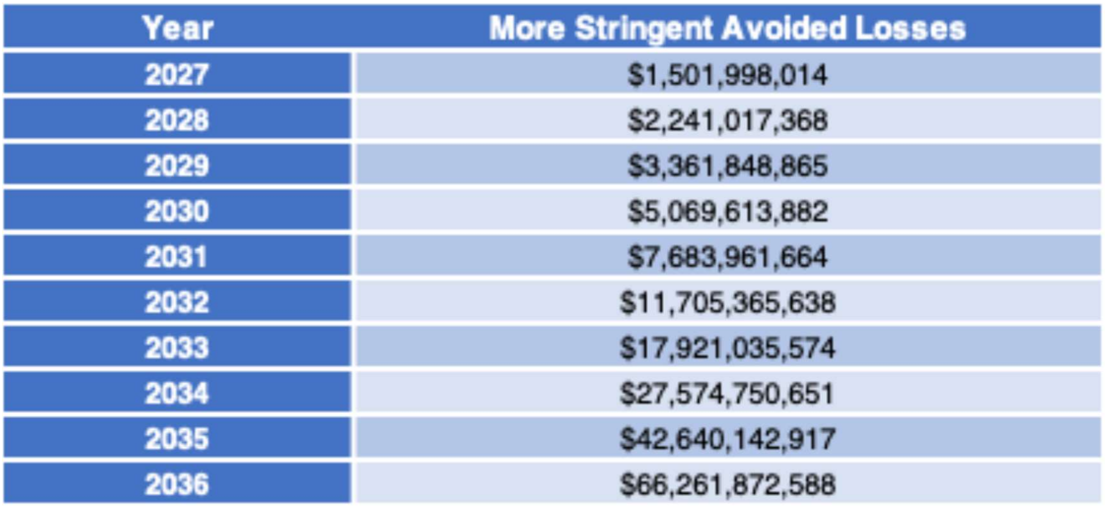
Table 6-14: Impacted Businesses Based on Number of Employees in More Stringent Alternative



Businesses with >500 Employees	Businesses with <500 Employees	Total Number of Impacted Businesses
1,602	50,724	52,326

Based on the number of impacted businesses, we estimate annual avoided losses in the more stringent alternative ranges over time from 2027 to 2036 as shown in Table 6-15 below.

Table 6-15: Annual Avoided Losses in the More Stringent Alternative (2027-2036)



Year	More Stringent Avoided Losses
2027	$1,501,998,014
2028	$2,241,017,368
2029	$3,361,848,865
2030	$5,069,613,882
2031	$7,683,961,664
2032	$11,705,365,638
2033	$17,921,035,574
2034	$27,574,750,651
2035	$42,640,142,917
2036	$66,261,872,588

Note: All figures in 2022 $

Expected annual avoided monetary losses in the more stringent alternative will be about **$1.5 billion** in 2027 and rise to about **$66.3 billion** by the year 2036. These quantified direct benefits estimates equal those for the proposed regulations due to the same maximum number of covered California businesses implementing CSAs, RAs, or both that reduce the risk of cybercrimes by $186 billion over the decade assessed. We expect the risk reduction will be greater under the more stringent alternative, when additional businesses conduct both CSAs and RAs. Due to a lack of information that allows separation of risk reductions associated with CSAs versus RAs versus both, quantified direct benefits remain tied to the number of businesses conducting CSAs or RAs. This limitation combined with a single source estimate of cybercrime risk reduction (12.6%) and a lack of quantifiable benefits of ADMT regulations, constrains the estimates for expected benefits of the more stringent alternative.

The combined number of impacted businesses in the more stringent alternative is equal to the maximum number of businesses covered by the CCPA (52,326) and estimated to achieve direct benefits of a 12.6% risk reduction in seven types of cybercrime. Combined, these estimates reflect the total quantified benefits for the More Stringent Alternative.

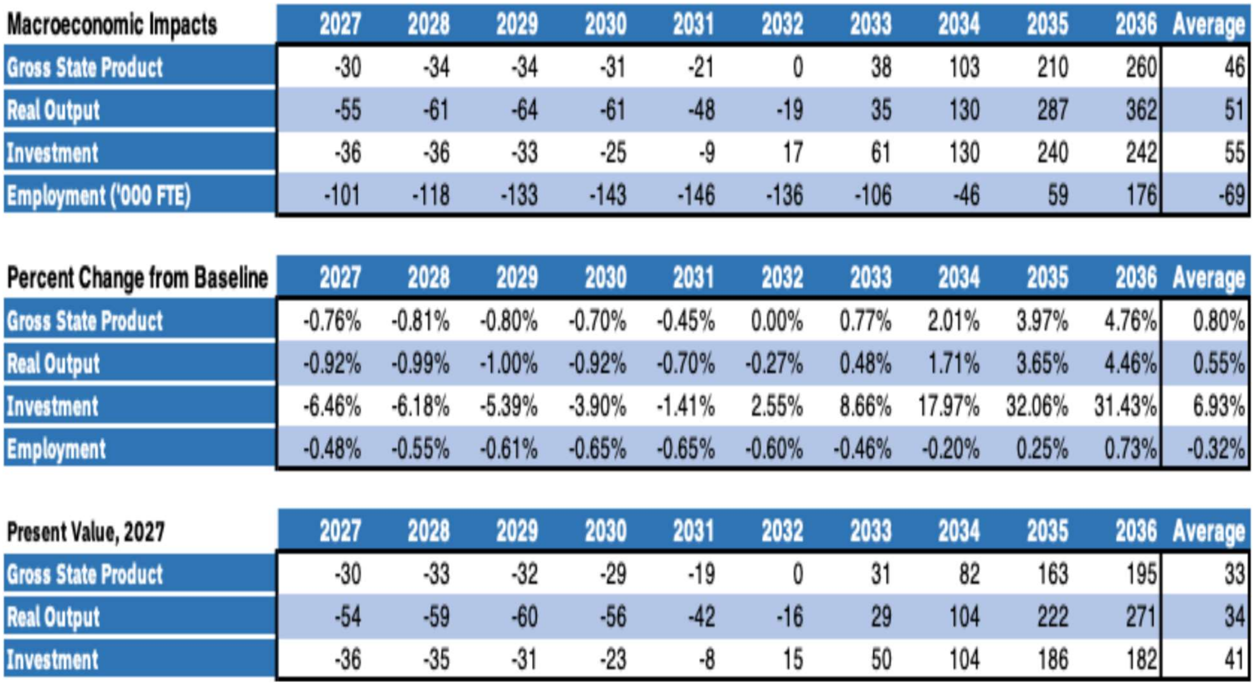
Analysis of these alternatives show that even when conservatively estimating the avoided monetary losses using a subset of cybercrimes in California, these avoided losses or direct benefits are expected to be significant. The economic benefits of avoided cybercrime losses will be long-term and grow substantially over time. Both the proposed regulations and alternatives considered will yield substantial benefits to California businesses and individuals through the increasing value of a percentage risk reduction associated with a subset of cybercrimes.

6.2.3 Macroeconomic Estimates for the More Stringent Alternative

Macroeconomic results for the more stringent alternative are presented below in Table 6-16. For regulatory packages with multiple alternative scenarios, the direct cost average is used as the input into the macroeconomic model. This presents a single more stringent alternative to assess the macroeconomic impacts.

To the extent that one expects deterrence of inadequate privacy protection of this magnitude can be achieved, as with proposed regulations, results for the more stringent alternative indicate that ensuring stronger protections for consumers' privacy can be a potent catalyst for growth when (as current trends indicate) losses of privacy are resulting in deadweight losses of many billions of dollars within California. In this way, both proposed regulations and the more stringent alternative suggests that regulations strengthening protection of consumer privacy, while imposing more compliance costs in the medium term, is compatible with more sustained and inclusive long-term growth.

Table 6-16: Macroeconomic Impacts of the More Stringent Alternative



Macroeconomic Impacts	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-30	-34	-34	-31	-21	0	38	103	210	260	46
Real Output	-55	-61	-64	-61	-48	-19	35	130	287	362	51
Investment	-36	-36	-33	-25	-9	17	61	130	240	242	55
Employment ('000 FTE)	-101	-118	-133	-143	-146	-136	-106	-46	59	176	-69

Percent Change from Baseline	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-0.76%	-0.81%	-0.80%	-0.70%	-0.45%	0.00%	0.77%	2.01%	3.97%	4.76%	0.80%
Real Output	-0.92%	-0.99%	-1.00%	-0.92%	-0.70%	-0.27%	0.48%	1.71%	3.65%	4.46%	0.55%
Investment	-6.46%	-6.18%	-5.39%	-3.90%	-1.41%	2.55%	8.66%	17.97%	32.06%	31.43%	6.93%
Employment	-0.48%	-0.55%	-0.61%	-0.65%	-0.65%	-0.60%	-0.46%	-0.20%	0.25%	0.73%	-0.32%

Present Value, 2027	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	Average
Gross State Product	-30	-33	-32	-29	-19	0	31	82	163	195	33
Real Output	-54	-59	-60	-56	-42	-16	29	104	222	271	34
Investment	-36	-35	-31	-23	-8	15	50	104	186	182	41

Notes: All figures in 2022 $ billions. Employment in FTE thousands.

The Agency finds that no alternatives were presented to or considered by the Agency that would be more effective in carrying out the purpose of these proposed regulations or would be as effective and less burdensome to affected private persons than these proposed regulations. Consistent with the above, while the more stringent alternative is associated with stronger protections for consumers' privacy, it is also associated with significantly higher compliance costs for businesses.

7 Summary of Economic Results

The Agency is proposing a set of related consumer privacy regulations. The proposed regulations do the following things: (1) update existing CCPA regulations; (2) clarify when insurance companies must comply with the CCPA; (3) operationalize requirements to complete an annual cybersecurity audit (CSA); (4) operationalize requirements to conduct a risk assessment (RA); and (5) operationalize consumers' rights to access and to opt-out of businesses' use of automated decision-making technology (ADMT). Based on a preliminary assessment using conservative approaches to combined direct economic costs and benefits (Table 4-1), the regulatory direct costs and benefits of these proposed regulations are estimated to be almost $5 billion in the first year and $66.7 billion in the tenth year following implementation starting in 2027. The net impacts to the California economy will be adverse in the early years and achieve higher than baseline growth by the middle of the decade. The annual average aggregate of costs and benefits is over $19.6B. Thus, it is our determination that the proposed regulations will easily exceed the $50 million threshold for performing a Standardized Regulatory Impact Assessment.

Macroeconomic estimates accounting for direct, indirect, and induced economywide impacts indicate that the regulatory impact will follow a similar trajectory, extending from relatively small (<1%) negative effects (against the growing baseline) in the first year to strongly positive (>5%) incremental growth in the tenth year, averaging $46 billion higher real GSP annually over the same decade.

In terms of economywide impacts, three salient findings deserve emphasis. First, when net direct costs are positive, the proposed regulations are understandably adverse to baseline or "business as usual" economic activity in the state's PI dependent sectors. This translates to lower profit, investment, output, and employment for established enterprises and allied activities. Second, cumulative impacts are much stronger than direct ones because the investment is reacting to the marginal change in profit, which is much higher than the marginal revenue effect. Finally, despite the investment shock combined direct, indirect, and induced effects are still a small percentage of baseline levels.

As is emphasized throughout this assessment, these impacts are completely overwhelmed by baseline aggregate growth. Even in the aggregate, we see a relatively small net impact on the state's multi-trillion-dollar economy, reducing average annual real GSP relative to the baseline reference by less than 1% in most years, until the net growth benefits compound in the final years to amplify baseline growth. This means the results are negative only relative to the baseline without proposed regulations, and the California economy and the sector itself can otherwise continue the robust trend growth it has enjoyed for two generations.

Impacts on sector and state competitiveness suggest that, as demand falls less than supply in a given year, some business is being diverted across California's border to available alternatives in other jurisdictions. While this is to be expected, the net slowing of growth for commerce remains modest. Relative impacts (as a percent of revenue) for the sector are of course more substantial than in comparison to the statewide economy, but they remain modest. With respect to investment, the proposed regulations exert pressure in both directions and is expected to have an ambiguous net effect.

Finally, empirical comparisons to more and less stringent alternatives suggest that the proposed regulations strike a good balance between the desire to strengthen consumer privacy and recognition of the importance of the information technology sector to the California economy. As PI protective practices and technologies proliferate, this adaptation can help reconcile higher levels of security and economic opportunity.

8 References

Acquisti, A. (2023). The Economics of Privacy at a Crossroads. *NBER Chapters*.

Acquisti, A., & Fong, C. (2020). An experiment in hiring discrimination via online social networks. *Management Science*, *66*(3), 1005-1024.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth?. *The Journal of Legal Studies*, *42*(2), 249-274.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes. *Proceedings of the ACM on human-computer interaction*, *3*(CSCW), 1-30.

Armitage, C., Botton, N., Dejeu-Castang, L., & Lemoine, L. (2023). Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers.

Aditya, B. R., Ferdiana, R., & Santosa, P. I. (2018, August). Toward Modern IT audit-current issues and literature review. In *2018 4th International Conference on Science and Technology (ICST)* (pp. 1-6). IEEE.

Belkhale, S., Cui, Y., & Sadigh, D. (2024). Data quality in imitation learning. *Advances in Neural Information Processing Systems*, *36*.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of management information systems*, *19*(1), 211-241.

California Department of Technology (2024). *Information Security Program Audit.*

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, *10*(1), 1-12.

Cisco (2024). Privacy as an Enabler of Customer Trust. *CISCO 2024 DATA PRIVACY BENCHMARK STUDY*.

Dubé, J. P., & Misra, S. (2023). Personalized pricing and consumer welfare. *Journal of Political Economy*, *131*(1), 131-189.

Ehrlinger, L., & Wöß, W. (2022). A survey of data quality measurement and monitoring tools. *Frontiers in big data*, *5*, 850611.

Eling, M., & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: mathematics and economics*, *75*, 126-136.

Ernst, & Young. (2015). How boards can help crack the cybereconomics equation. *Board Matters Quarterly*, September, 14-15.

Federal Trade Commission (2022). Trade regulation rule on commercial surveillance and data security.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial management & data Systems*, *106*(5), 601-620.

Frik, A., & Gaudeul, A. (2020). A measure of the implicit value of privacy under risk. *Journal of Consumer Marketing*, *37*(4), 457-472.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840.

Gordon, L. A., & Smith, R. (2007). Incentives for improving cybersecurity in the private sector: A cost-benefit perspective. *Congressional Testimony*.

Gauthier, M. P., & Brender, N. (2021). How do the current auditing standards fit the emergent use of blockchain? *Managerial auditing journal*, *36*(3), 365-385.

Godel, M., Landzaat, W., & Suter, J. (2017). Research and analysis to quantify the benefits arising from personal data rights under the GDPR. *Report, Department for Culture, Media & Sport, London, UK*.

Gordon, L. A (2007). Incentives for improving cybersecurity in the private sector: A cost-benefit perspective. *Congressional Testimony*.

Hagey, K. (2019). Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests. *The Wall Street Journal*, *29*.

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). The devastating business impacts of a cyber breach. *Harvard Business Review. https://hbr. org/2023/05/thedevastating-business-impacts-of-a-cyber-breach*.

IBM (2023). *Cost of a Data Breach Report 2023.* IBM Security.

IMPLAN, REMI, and RIMS II: Benchmarking Ready-Made Models for Comparison." The Annals of Regional Science 29 (4): 363–74, 2022.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, *33*(4), 377-409.

Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J., & Mullainathan, S. (2018). Human decisions and machine predictions. *The Quarterly Journal of Economics*, *133*(1), 237-293.

Kox, H., Straathof, B., & Zwart, G. (2017). Targeted advertising, platform competition, and privacy. *Journal of economics & management strategy*, *26*(3), 557-570.

Lang, K., & Spitzer, A. K. L. (2020). Race discrimination: An economic perspective. *Journal of Economic Perspectives*, *34*(2), 68-89.

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of information security and applications*, *19*(6), 321-330.

Lewis, J. A. (2013). Raising the bar for cybersecurity. Washington, DC: Center for Strategic & International Studies.

Madnick, S. E. (2023). The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase.

Mallory, C., Sears, B., Wright, E. R., & Conron, K. J. (2017). *The economic impact of stigma and discrimination against LGBT people in Georgia*. Williams Institute, UCLA School of Law.

Mustri, E. A. S., Adjerid, I., & Acquisti, A. (2022). *Behavioral advertising and consumer welfare: An empirical investigation*. Technical report, Carnegie Mellon University.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

Norfleet, Nicole (2022, April 29). Target pays $5 million in settlement over pricing accuracy allegations. *Star Tribune.* https://apnews.com/article/technology-business-lawsuits-california-target-corp-35db1e4f1ea1d43ef7a1f7f2b4630c41

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *Sage Open*, *11*(4), 21582440211061556.

PricewaterhouseCoopers. (2013). 10 Minutes on the stark realities of cybersecurity. April. Available at: http://www.pwc.com/us/en/10minutes/cybersecurity-realities.html

Roland-Holst, David “Technical Documentation of the BEAR Impact Assessment Model,” 2024.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

Sanchez-Garcia, I. D., Rea-Guaman, A. M., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2024). Cybersecurity Risk Audit: A Systematic Literature Review. *New Perspectives in Software Engineering*, 275-301.

Seele, P., Dierksmeier, C., Hofstetter, R., & Schultz, M. D. (2021). Mapping the ethicality of algorithmic pricing: A review of dynamic and personalized pricing. *Journal of Business Ethics*, *170*, 697-719.

Shiller, B. R. (2020). Approximating purchase propensities and reservation prices from broad consumer tracking. *International Economic Review*, *61*(2), 847-870.

Skatova, A., McDonald, R., Ma, S., & Maple, C. (2023). Unpacking privacy: Valuation of personal data protection. *Plos one*, *18*(5), e0284581.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548.

Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. *Information Systems and e-Business Management*, *20*(1), 57-78.

Starks, T. (2023). Cyber experts say regulators aren't going far enough with their rules. *Washington Post*.

Steinbart, P.J., Raschke, R.L., Gal, G., Dilla, W.N., (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Acc. Organ. Soc. 71, 15–29. https://doi.org/10.1016/j.aos.2018.04.005.

Swonk, D. (n.d.) Diversity and Economics. Leading Authorities Speakers. (n.d.). https://www.leadingauthorities.com/speakers/video/diane-swonk-diversity-and-economics

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795.

U.S. Government Accountability Office (2023). *Cybersecurity Program Audit Guide*, GAO-23-104705.

Verizon. (2014). Data Breach Investigations Report. Available at: http://www.verizonenterprise.com/DBIR/2014/

Verizon. (2015). Data Breach Investigations Report. Available at: http://www.verizonenterprise.com/DBIR/2015/

Vetrò, A., Torchiano, M., & Mecati, M. (2021). A data quality approach to the identification of discrimination risk in automated decision-making systems. *Government Information Quarterly*, *38*(4), 101619.

Vila, T., Greenstadt, R., & Molnar, D. (2004). Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market. *Economics of information security*, 143-153.

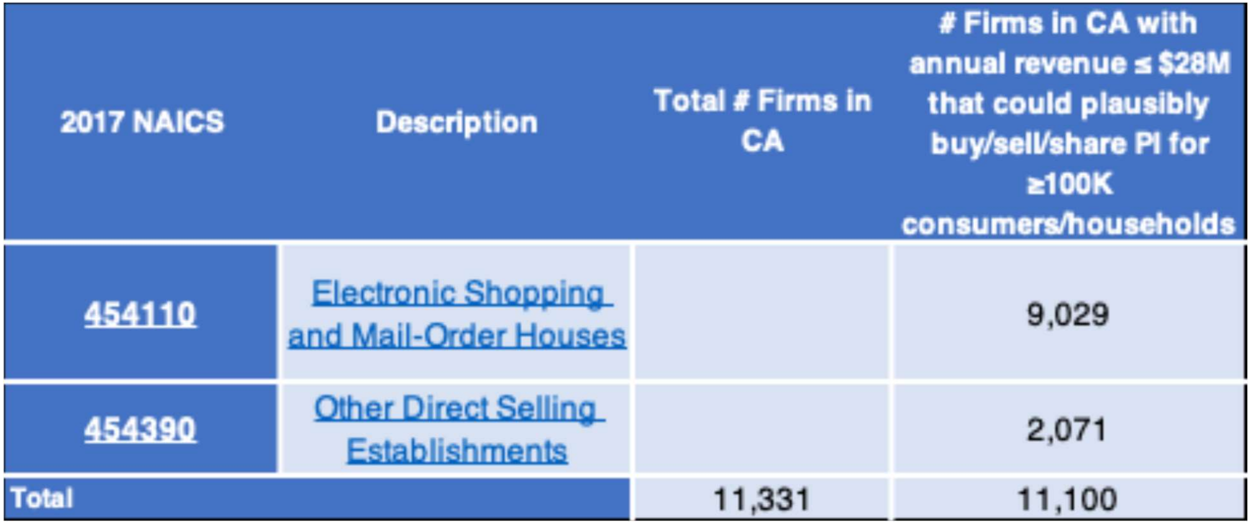
Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P. S., ... & Gabriel, I. (2021). Ethical and social risks of harm from language models. *arXiv preprint arXiv:2112.04359*.

Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. *Council of Europe, Directorate General of Democracy*, 42.

9 Appendix 1 – NAICS Used for Covered California Businesses

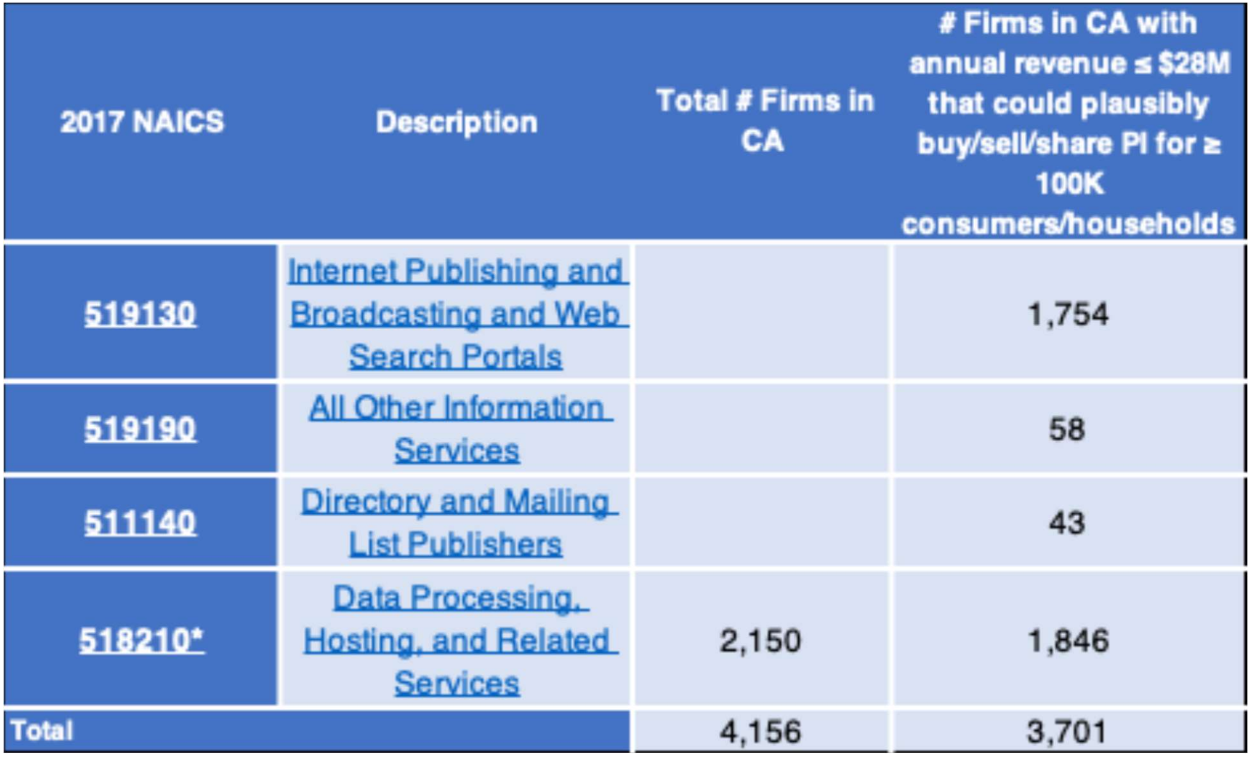
NAICS codes for which, in our assessment, businesses could plausibly buy/sell/share PI for ≥ 100K consumers or households.

Table 9-1: 44-45-Retail Trade



2017 NAICS	Description	Total # Firms in CA	# Firms in CA with annual revenue ≤ $28M that could plausibly buy/sell/share PI for ≥100K consumers/households
454110	Electronic Shopping and Mail-Order Houses		9,029
454390	Other Direct Selling Establishments		2,071
Total		11,331	11,100

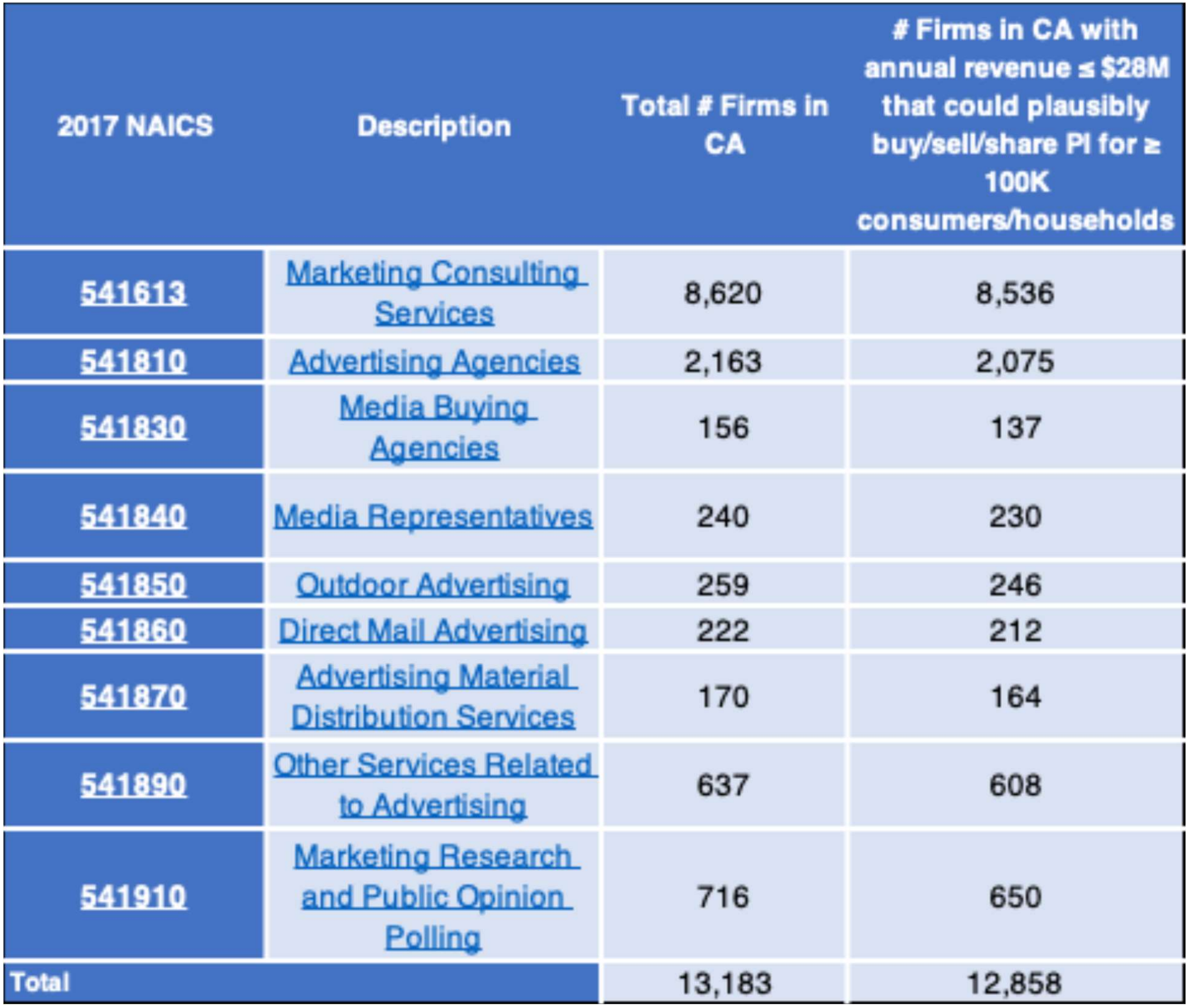
Table 9-2: 51-Information Services



2017 NAICS	Description	Total # Firms in CA	# Firms in CA with annual revenue ≤ $28M that could plausibly buy/sell/share PI for ≥ 100K consumers/households
519130	Internet Publishing and Broadcasting and Web Search Portals		1,754
519190	All Other Information Services		58
511140	Directory and Mailing List Publishers		43
518210*	Data Processing, Hosting, and Related Services	2,150	1,846
Total		4,156	3,701

* We assume data brokers registered with the Agency are classified by this NAICS code

Table 9-3: 54-Professional, Scientific, and Technical Services



2017 NAICS	Description	Total # Firms in CA	# Firms in CA with annual revenue ≤ $28M that could plausibly buy/sell/share PI for ≥ 100K consumers/households
541613	Marketing Consulting Services	8,620	8,536
541810	Advertising Agencies	2,163	2,075
541830	Media Buying Agencies	156	137
541840	Media Representatives	240	230
541850	Outdoor Advertising	259	246
541860	Direct Mail Advertising	222	212
541870	Advertising Material Distribution Services	170	164
541890	Other Services Related to Advertising	637	608
541910	Marketing Research and Public Opinion Polling	716	650
Total		13,183	12,858

10 Appendix 2 – Additional Methodological Details

10.1 Website Sampling for Businesses Covered by CCPA

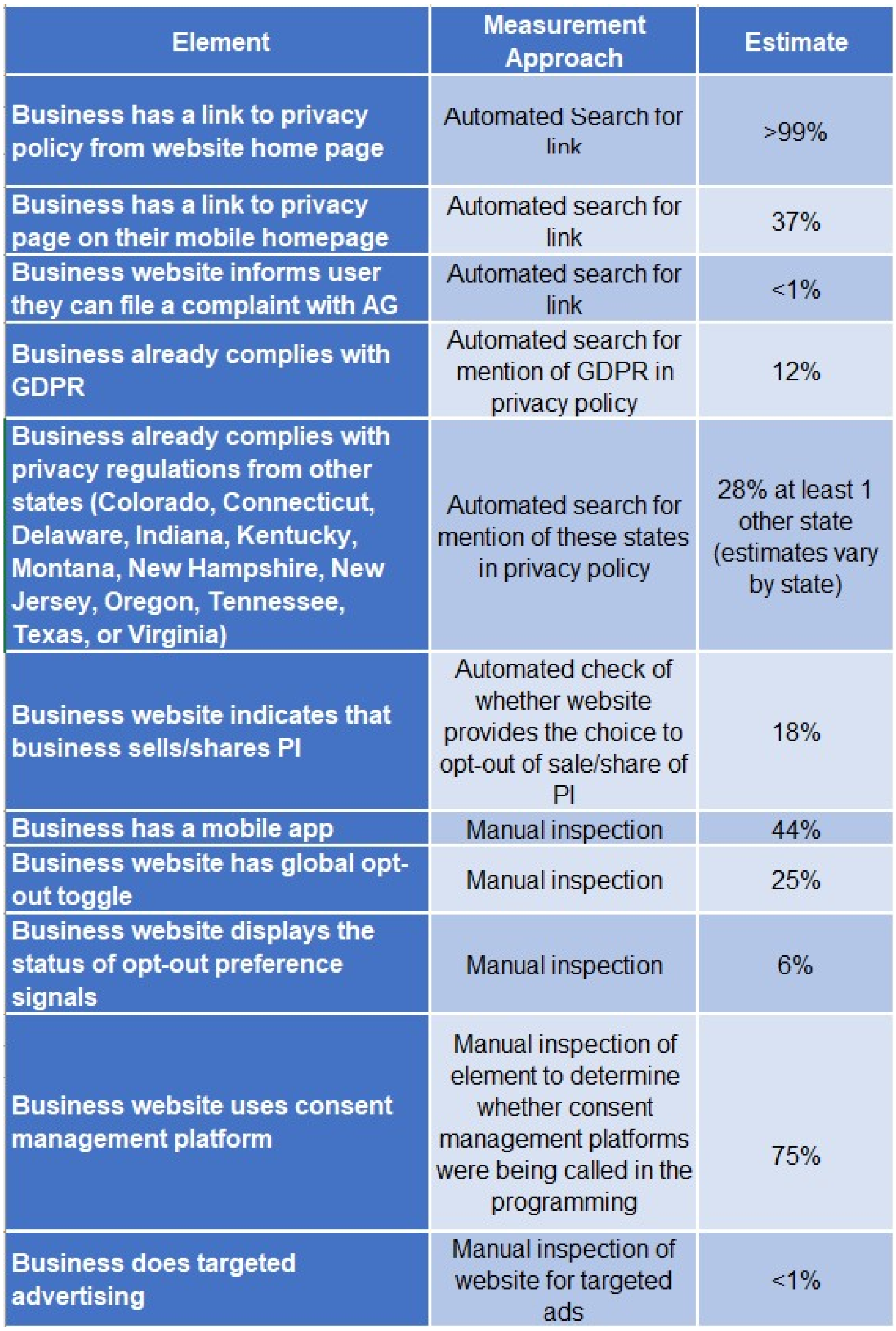
To inform our estimates of compliance costs to businesses we developed a process to randomly sample the websites for a subset of California businesses and evaluate the business websites for current privacy practices, compliance with other privacy regulations from other jurisdictions which could help mitigate costs associated with compliance with the proposed regulation, and to assess what share of businesses use data in ways that require compliance with the proposed regulations. Because it would not be feasible to automatically check for all features that we wanted to evaluate, we supplemented this process with manual evaluation of a subset of sampled businesses. This section describes the procedures used and information collected.

Data on California businesses was gathered from Business Finder (https://www.careeronestop.org/Toolkit/Jobs/find-businesses.aspx). Each possible 2-digit NAICS was coupled with the “California” for location to derive the complete list of Business Finder's 3,889,177 Californian businesses. Duplicates from the search were removed and compiled into a single list containing all Business Finder urls with the attributes of each business. We then randomly sampled 3,000 entries from this list, whose Business Name, Homepage url and 2-digit NAICS code were recorded. Businesses with no websites listed were ignored. Because various websites were outdated, did not exist (i.e., we received an error 404), or did not provide access, we were left with 2,139 websites in our sample covering all 2-digit NAICS codes.

To assess current privacy practices among this random sample of California businesses, a list of 16 key phrases involving variants of the phrase “privacy policy” were searched for on the homepage to determine whether the website provided any information on privacy. This process was repeated with iPhone headers to find the privacy policy links on the mobile versions of the homepages. The privacy policy page, if available, was extracted to be checked for the presence of key phrases such as ‘General Data Protection Regulation’ and ‘Colorado’ in order to assess whether the business was already complying with privacy regulations from other jurisdictions. Matches in long lists (preceding and succeeding new line characters) were ignored. Lastly, 6 key phrases involving variants of “cookies” and “my personal information” were searched for in the homepages to determine if the website sells or shares PI.

In the end we collected information on the following outcomes:

Table 10-1: Summary of Information Collected



Element	Measurement Approach	Estimate
Business has a link to privacy policy from website home page	Automated Search for link	>99%
Business has a link to privacy page on their mobile homepage	Automated search for link	37%
Business website informs user they can file a complaint with AG	Automated search for link	<1%
Business already complies with GDPR	Automated search for mention of GDPR in privacy policy	12%
Business already complies with privacy regulations from other states (Colorado, Connecticut, Delaware, Indiana, Kentucky, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, or Virginia)	Automated search for mention of these states in privacy policy	28% at least 1 other state (estimates vary by state)
Business website indicates that business sells/shares PI	Automated check of whether website provides the choice to opt-out of sale/share of PI	18%
Business has a mobile app	Manual inspection	44%
Business website has global opt-out toggle	Manual inspection	25%
Business website displays the status of opt-out preference signals	Manual inspection	6%
Business website uses consent management platform	Manual inspection of element to determine whether consent management platforms were being called in the programming	75%
Business does targeted advertising	Manual inspection of website for targeted ads	<1%

11 Appendix 3 – Department of Finance's Model Baseline Calibration

11.1 Introduction

The California Department of Finance requires that, for dynamic macroeconomic assessment work, a SRIA baseline scenario be calibrated to conform with its macroeconomic projections to the most recent projections (May Revision, accessed July, 2024).[1], [2], [3] This approach enables the SRIA to create accurate reference baselines for comparison to proposed regulations and alternatives considered by the agency.[4]

11.2 Macroeconomic Baseline Forecasts

There are three fundamental macroeconomic series of importance for baseline calibration: Population, Employment, and Personal Income. As it happens, population, baseline employment, and annual real GSP growth are exogenous (inputs) to the BEAR Model, though these two series are identical.

11.3 Baseline Calibration of the BEAR Model

The BEAR Model is calibrated to state real Personal Income growth rates, obtained from DOF and used to proxy real GSP growth. Using exogenous rates of implied growth in total factor productivity (TFP), the model computes supply, demand, and trade patterns compatible with domestic and state market equilibrium conditions. Equilibrium is achieved by adjustments in the relative prices of domestic resources and commodities, while international equilibrium is achieved by adjusting trade patterns and real exchange rates to satisfy fixed real balance of payments constraints.

The calibration procedure highlights the two salient adjustment mechanisms in the model (as well as the real economies), prices in California, U.S. domestic and international markets. General equilibrium price adjustments are generally well understood by professional economists but the degree of segmentation between state, national, and global markets depend on many factors.

Because CGE like this do not capture the aggregate price level or other nominal quantities, there are no pure inflationary or monetary effects in the sense of traditional macroeconomics or finance. Since there is no money metric in the model, all prices are relative prices. If there were financial assets in the model, one could define a nominal inflation and interest rates as the relative prices of financial assets (money, bonds, etc.). Without them, prices only reflect real purchasing power or the relative price of goods and services in terms of each other.

12 Appendix 4 - Technical Summary of the BEAR Model

The Berkeley Energy and Resources (BEAR) Model is in reality a constellation of research tools designed to elucidate linkages across the California economy. This section provides a brief summary of the formal structure of the BEAR Model.[5] For the purposes of this report, the 2013 California Social Accounting Matrix (SAM), was aggregated along certain dimensions. The current version of the Model includes 195 activity sectors, 22 occupations, and ten households aggregated from the original California SAM. The equations of the Model are completely documented elsewhere (BEAR: 2024), and for the present we only review its salient structural components.

12.1 Structure of the BEAR (CGE) Model

Technically, a CGE model is a system of simultaneous equations that simulate price-directed interactions between firms and households in commodity and factor markets. The role of government, capital markets, and other trading partners are also specified, with varying degrees of detail and passivity, to close the model and account for economywide resource allocation, production, and income determination.

The role of markets is to mediate exchange, usually with a flexible system of prices, the most important endogenous variables in a typical CGE model. As in a real market economy, commodity and factor price changes induce changes in the level and composition of supply and demand, production and income, and the remaining endogenous variables in the system. In CGE models, an equation system is solved for prices that correspond to equilibrium in markets and satisfy the accounting identities governing economic behavior. If such a system is precisely specified, equilibrium always exists, and such a consistent model can be calibrated to a base period data set. The resulting calibrated general equilibrium model is then used to simulate the economywide (and regional) effects of alternative policies or external events.

The distinguishing feature of a general equilibrium model, applied or theoretical, is its closed-form specification of all activities in the economic system under study. This can be contrasted with more traditional partial equilibrium analysis, where linkages to other domestic markets and agents are deliberately excluded from consideration. A large and growing body of evidence suggests that indirect effects (e.g., upstream and downstream production linkages) arising from policy changes are not only substantial but may in some cases even outweigh direct effects. Only a model that consistently specifies economywide interactions can fully assess the implications of economic policies or business strategies. In a multi-country model like the one used in this study, indirect effects include the trade linkages between countries and regions which themselves can have policy implications.

The Model we use for this work has been constructed according to generally accepted specification standards, implemented in the GAMS programming language, and calibrated to the new California SAM estimated for the year 2012. The result is a single economy model calibrated over the thirty-five-year interval time-path from 2015 to 2050. Using the very detailed accounts of the California SAM, we include the following in the present Model:

12.2 Production Sectors

All sectors are assumed to operate under constant returns to scale and cost optimization. Production technology is modelled by a nesting of constant-elasticity-of-substitution (CES) function.

In each period, the supply of primary factors — capital, land, and labor — is usually predetermined.[6] The Model includes adjustment rigidities. An important feature is the distinction between old and new capital goods. In addition, capital is assumed to be partially mobile, reflecting differences in the marketability of capital goods across sectors.[7] Once the optimal combination of inputs is determined, sectoral output prices are calculated assuming competitive supply conditions in all markets.

12.3 Consumption and Closure Rule

All income generated by economic activity is assumed to be distributed to consumers. Each representative consumer allocates optimally his/her disposable income among the different commodities and saving. The consumption/saving decision is completely static: saving is treated as a “good” and its amount is determined simultaneously with the demand for the other commodities, the price of saving being set arbitrarily equal to the average price of consumer goods.

The government collects income taxes, indirect taxes on intermediate inputs, outputs, and consumer expenditures. The default closure of the Model assumes that the government deficit/saving is exogenously specified.[8] The indirect tax schedule will shift to accommodate any changes in the balance between government revenues and government expenditures.

The current account surplus (deficit) is fixed in nominal terms. The counterpart of this imbalance is a net outflow (inflow) of capital, which is subtracted (added to) the domestic flow of saving. In each period, the Model equates gross investment to net saving (equal to the sum of saving by households, the net budget position of the government and foreign capital inflows). This particular closure rule implies that investment is driven by saving.

12.4 Trade

Goods are assumed to be differentiated by region of origin. In other words, goods classified in the same sector are different according to whether they are produced domestically or imported. This assumption is frequently known as the *Armington* assumption. The degree of substitutability, as well as the import penetration shares are allowed to vary across commodities. The Model assumes a single Armington agent. This strong assumption implies that the propensity to import and the degree of substitutability between domestic and imported goods is uniform across economic agents. This assumption reduces tremendously the dimensionality of the Model. In many cases this assumption is imposed by the data. A symmetric assumption is made on the export side where domestic producers are assumed to differentiate the domestic market and the export market. This is modelled using a *Constant-Elasticity-of-Transformation* (CET) function.

12.5 Dynamic Features and Calibration

The current version of the Model has a simple recursive dynamic structure as agents are assumed to be myopic and to base their decisions on static expectations about prices and quantities. Dynamics in the Model originate in three sources: i) accumulation of productive capital and labor growth; ii) shifts in production technology; and iii) the putty/semi-putty specification of technology.

12.6 Capital Accumulation

In the aggregate, the basic capital accumulation function equates the current capital stock to the depreciated stock inherited from the previous period plus gross investment. However, at the sectoral level, the specific accumulation functions may differ because the demand for (old and new) capital can be less than the depreciated stock of old capital. In this case, the sector contracts over time by releasing old capital goods. Consequently, in each period, the new capital vintage available to expanding industries is equal to the sum of disinvested capital in contracting industries plus total saving generated by the economy, consistent with the closure rule of the Model.

12.7 The Putty/Semi-Putty Specification

The substitution possibilities among production factors are assumed to be higher with the new than the old capital vintages — technology has a putty/semi-putty specification. Hence, when a shock to relative prices occurs (e.g., the imposition of an emissions fee), the demands for production factors adjust gradually to the long-run optimum because the substitution effects are delayed over time. The adjustment path depends on the values of the short-run elasticities of substitution and the replacement rate of capital. As the latter determines the pace at which new vintages are installed.

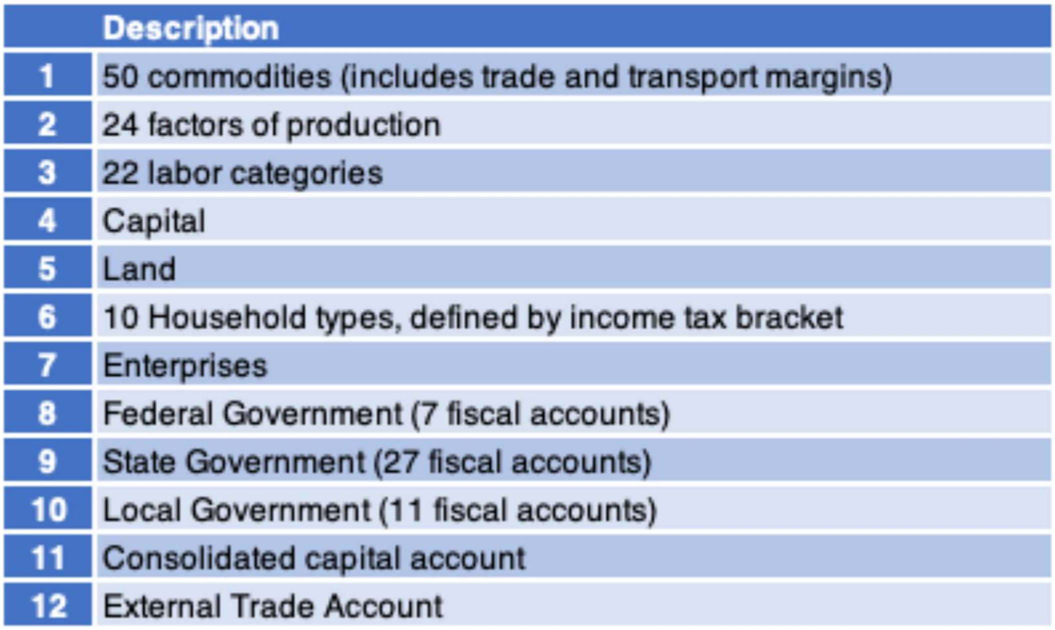
12.8 Profits, Adjustment Costs, and Expectations

Firms output and investment decisions are modelled in accordance with the innovative approach of Goulder and co-authors (2009). In particular, we allow for the possibility that firms reap windfall profits from events such as free permit distribution. We assume that these profits accrue to U.S. and foreign residents in proportion to equity shares of publicly traded US corporations (16% in 2009, Swartz and Tillman:2010). Between California and other US residents, the shares are assumed to be proportional to GSP in GDP (11% in 2009).

12.9 Dynamic Calibration

The BEAR Model is calibrated on exogenous growth rates of population, labor force, and GDP. In the so-called baseline scenario, the dynamics are calibrated in each region by imposing the assumption of a balanced growth path. This implies that the ratio between labor and capital (in efficiency units) is held constant over time.[9] When alternative scenarios around the baseline are simulated, the technical efficiency parameter is held constant, and the growth of capital is endogenously determined by the saving/investment relation.

Table 12-1: California SAM for 2013 – Structural Characteristics

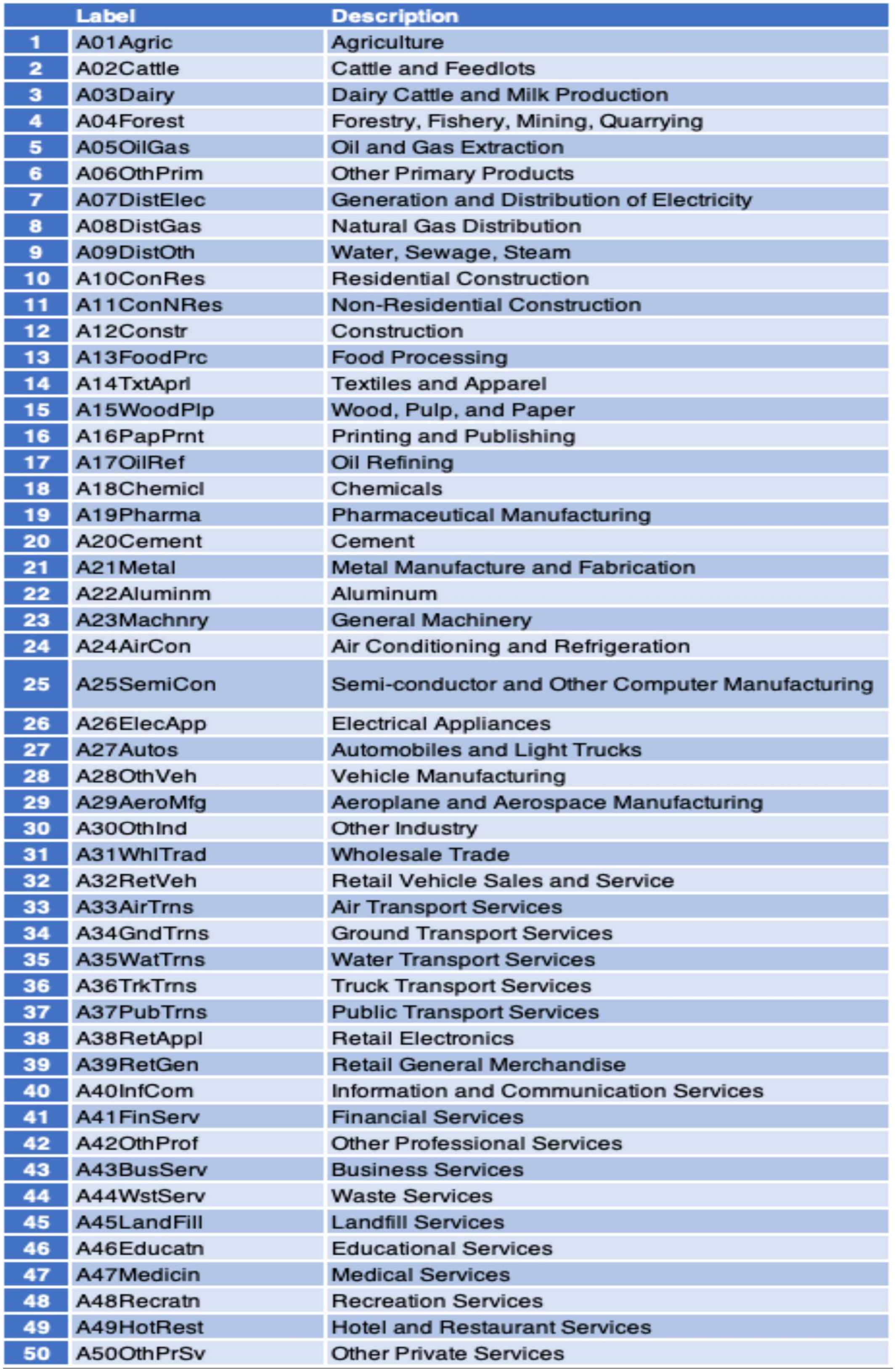


	Description
1	50 commodities (includes trade and transport margins)
2	24 factors of production
3	22 labor categories
4	Capital
5	Land
6	10 Household types, defined by income tax bracket
7	Enterprises
8	Federal Government (7 fiscal accounts)
9	State Government (27 fiscal accounts)
10	Local Government (11 fiscal accounts)
11	Consolidated capital account
12	External Trade Account

12.10 Sectoring Scheme for the BEAR Model

The 50 Production Sectors and Commodity Groups represent the aggregation of the 534 original sectors that were aggregated from a 2022 California Social Accounting Matrix (CGE) estimated by IMPLAN.

Table 12-2: Aggregate Accounts for the SRIA Assessment



	Label	Description
1	A01Agric	Agriculture
2	A02Cattle	Cattle and Feedlots
3	A03Dairy	Dairy Cattle and Milk Production
4	A04Forest	Forestry, Fishery, Mining, Quarrying
5	A05OilGas	Oil and Gas Extraction
6	A06OthPrim	Other Primary Products
7	A07DistElec	Generation and Distribution of Electricity
8	A08DistGas	Natural Gas Distribution
9	A09DistOth	Water, Sewage, Steam
10	A10ConRes	Residential Construction
11	A11ConNRes	Non-Residential Construction
12	A12Constr	Construction
13	A13FoodPrc	Food Processing
14	A14TxtAprl	Textiles and Apparel
15	A15WoodPlp	Wood, Pulp, and Paper
16	A16PapPrnt	Printing and Publishing
17	A17OilRef	Oil Refining
18	A18Chemicl	Chemicals
19	A19Pharma	Pharmaceutical Manufacturing
20	A20Cement	Cement
21	A21Metal	Metal Manufacture and Fabrication
22	A22Aluminm	Aluminum
23	A23Machnry	General Machinery
24	A24AirCon	Air Conditioning and Refrigeration
25	A25SemiCon	Semi-conductor and Other Computer Manufacturing
26	A26ElecApp	Electrical Appliances
27	A27Autos	Automobiles and Light Trucks
28	A28OthVeh	Vehicle Manufacturing
29	A29AeroMfg	Aeroplane and Aerospace Manufacturing
30	A30OthInd	Other Industry
31	A31WhlTrad	Wholesale Trade
32	A32RetVeh	Retail Vehicle Sales and Service
33	A33AirTrns	Air Transport Services
34	A34GndTrns	Ground Transport Services
35	A35WatTrns	Water Transport Services
36	A36TrkTrns	Truck Transport Services
37	A37PubTrns	Public Transport Services
38	A38RetAppl	Retail Electronics
39	A39RetGen	Retail General Merchandise
40	A40InfCom	Information and Communication Services
41	A41FinServ	Financial Services
42	A42OthProf	Other Professional Services
43	A43BusServ	Business Services
44	A44WstServ	Waste Services
45	A45LandFill	Landfill Services
46	A46Educatn	Educational Services
47	A47Medicin	Medical Services
48	A48Recratn	Recreation Services
49	A49HotRest	Hotel and Restaurant Services
50	A50OthPrSv	Other Private Services

These data enable us to trace the effects of policies at unprecedented levels of detail, tracing linkages across the economy and clearly indicating the indirect benefits and trade-offs that might result from comprehensive policies. In particular, cumulative indirect effects often outweigh direct consequences, and affected groups are often far from the policy target group. For these reasons, it is essential for policy makers to anticipate linkage effects like those revealed in a general equilibrium model and dataset like the ones used here.

It should be noted that the SAM used with the BEAR Model departs in a few substantive respects from the original 2012 California SAM. The two main differences have to do with the structure of production, as reflected in the input-output accounts, and with consumption good aggregation. To specify production technology in the BEAR Model, we rely on both activity and commodity accounting, while the original SAM has consolidated activity accounts. The difference is non-trivial and considerable additional effort was needed to reconcile use and make tables separately. This also facilitated the second SAM extension, however, where we maintained final demand at the full 119 commodity level of aggregation, rather than adopting six aggregate commodities like the original SAM.

End Notes

[1] California Code of Regulations, title 1, section 2003(b)

[2] https://www.dof.ca.gov/forecasting/demographics/projections/

[3] https://www.dof.ca.gov/Forecasting/Economics/

[4] We would like to express our thanks to the DOF Chief Economist and staff for their cooperation and data sharing to support this calibration exercise. Any errors implementing these inputs are solely the responsibility of the authors.

[5] See Roland-Holst (2024) for a complete model description.

[6] Capital supply is to some extent influenced by the current period's level of investment.

[7] For simplicity, it is assumed that old capital goods supplied in second-hand markets and new capital goods are homogeneous. This formulation makes it possible to introduce downward rigidities in the adjustment of capital without increasing excessively the number of equilibrium prices to be determined by the Model.

[8] In the reference simulation, the real government fiscal balance converges (linearly) towards 0 by the final period of the simulation.

[9] This involves computing in each period a measure of Harrod-neutral technical progress in the capital-labor bundle as a residual. This is a standard calibration procedure in dynamic CGE modeling.