STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations

Prepared for: Attorney General's Office
California Department of Justice

Prepared by: Berkeley Economic Advising and Research, LLC

August 2019

California Department of Justice

Primary Author(s):

David Roland-Holst
Samuel Evans
Drew Behnke
Samuel Neal
Liam Frölund
Yao Xiao

Berkeley Economic Advising and Research
1442A Walnut St. Suite 108
Berkeley, CA 94709
Phone: 510-220-4567
www.bearecon.com

Contract Number: 18-255U

Prepared for:

Attorney General's Office

Stacey D. Schesser
Supervising Deputy Attorney General
Consumer Law Section - Privacy Unit

David Roland-Holst
Project Manager

DISCLAIMER

This report was prepared as the result of work sponsored by the California Department of Justice (DOJ). It does not necessarily represent the views of the DOJ, its employees, or the State of California. The DOJ, the State of California, its employees, contractors, and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Department of Justice passed upon the accuracy or adequacy of the information in this report.

Contents

Abbreviations

AB – Assembly Bill
AG – Attorney General of California
BEAR - Berkeley Economic Advising and Research
CCPA – California Consumer Privacy Act
CGE – Computable General Equilibrium
DOF – California Department of Finance
DOJ – California Department of Justice
FY – Fiscal Year
GDPR - General Data Protection Regulation
PI – Personal Information
SRIA – Standardized Regulatory Impact Assessment

1 Introduction

California is the fifth-largest economy in the world, with a sizeable market leading the development of new technologies. The state is also home to many businesses that have capitalized on the collection of private data from consumers. With the sophistication and scope of technology and data increasing daily, so has the extensive and intensive collection of consumer information by businesses. Neither state nor federal law have kept pace with these developments in ways that enable consumers to exert control over the collection, use, and protection of their personal information (PI). Survey research from the Pew Research Center demonstrates that consumers do not trust that their personal data is secure and would like to be in control of what information is available and who has access to it. For example, a 2015 survey found that only 7% of respondents were confident that their records would remain private and 90% of respondents would like to be in control of what personal data is available (Madden & Rainie 2015). Consumers are also unaware of how and what data is being collected about them when they use the internet, their smart phones, or other interactive devices. They are wary about how their data is used and sold to third parties, often without their knowledge or control, as well as lack of transparency, compounded by confusing terms of service that govern everyday online services, including social media platforms, e-commerce sites, and internet search engines.

Despite these concerns, the vast majority of consumers continue to use free services, which rely upon and monetize consumer personal information. This situation appears to be the result of a lack of understanding over how to control data collection, i.e. the majority of internet users (62%) do not know how to limit information that is collected about them by a website (Purcell 2012). Not only do many consumers lack the technical ability to protect their data, but the market power of many internet companies and interactions between others leave consumers few options to surrendering their privacy. This “privacy market failure” supports a general case for intervention in the public interest, a primary impetus for legislation such as the groundbreaking California Consumer Privacy Act (CCPA). As part of the CCPA, the California legislature tasked the Attorney General’s office with adopting regulations to implement many elements of the statute. This Standardized Regulatory Impact Assessment (SRIA) evaluates the impacts of these proposed regulations on the California economy.

1.1 Background and Summary of Proposed Regulations

The CCPA arose from a consumer-led, statewide ballot initiative that was headed for the November 2018 election. The goal was to empower consumers with the ability to learn what data businesses were collecting on them and vest them with the ability to stop the sale of their personal information. Before reaching the ballot however, the California legislature offered AB 375 in exchange for the withdrawal of the ballot measure. On June 28, 2018, AB 375 passed unanimously and was signed into law. The law offers the following privacy protections to consumers:

- **Right to Know**: Grants consumers the right to be informed about a business's practices regarding the collection, use, disclosure, and sale of PI, and also to be informed, in response to a verifiable consumer request, of the specific pieces of their PI held by the business.

- **Right to Delete:** Grants consumers to the right to request that a business delete any PI that the business has collected from the consumer, as well as direct any service providers to delete the PI, unless excepted.

- **Right to Opt-Out:** Grants consumers the right to direct a business that sells a consumer's PI to no longer sell their PI. For minors between the ages of 13 – 16, a business may not sell their personal information without affirmative authorization. For consumers under 13, the affirmative authorization to sell must be granted by the parent or legal guardian.

- **Right to Non-Discrimination**: A business cannot discriminate against the consumer for exercising any of the above rights. This includes denying goods or services, charging different prices, or providing a different level or quality of service. However, a business is able to offer a consumer's different rates (or service) if that difference is reasonably related to the value of the consumer's data.

The CCPA applies to all businesses in California that meet one or more of the following three thresholds: (1) has annual gross revenues in excess of twenty-five million dollars ($25,000,000). (2) buys, sells, or shares the personal information of 50,000 or more consumers, households, or devices. (3) derives 50% or more of its annual revenue from selling consumers' PI.

The CCPA tasks the Attorney General with both exclusive enforcement of the law and rulemaking authority in furtherance of the CCPA. With respect to regulations, the law sets forth areas that require immediate rulemaking by July 1, 2020 (See Civil Code, § 1798.185, subd. (a)), and provides for ongoing, future rulemaking authority "as necessary

to further the purposes of this title" (id. at subd. (b)). Thus, the Legislature may have intended for rulemaking to commence on the specific, outlined areas in section 1798.185(a) so that the CCPA would be workable for businesses and consumers alike. In undertaking the preliminary rulemaking activities as required by the CCPA and the Administrative Procedure Act, the Attorney General solicited broad public participation at seven statewide forums and highlighted the list of areas in section 1798.185(a) for public comment. For this first-round of rulemaking, forthcoming regulations will address these priority areas, including how businesses shall respond and handle consumer requests, how consumers may submit verifiable consumer requests, and how businesses may offer financial incentives without discriminating against consumers who exercise their rights under CCPA. Future rulemaking may address any areas that require additional guidance.

As enacted, the CCPA mandates new obligations on businesses that would apply even without the force of the Attorney General's regulations. For example, businesses would have to update privacy policies and develop a mechanism for providing notice to consumers at or before the point of collection. Some businesses may already have these mechanisms in place in light of other existing legal frameworks, including federal and international privacy laws. Businesses must also comply with the newest right afforded to consumers—the right to opt-out of the sale of PI—as these requests do not mandate any verification by the business. Thus, while the Attorney General's forthcoming regulations will provide clarity on the operability of some of CCPA's provisions, businesses will be subject to and must comply with many requirements of the law when it goes into effect on January 1, 2020.

1.2 Major Regulation Determination

A proposed regulation is determined to be a major regulation if the estimated economic impact of the regulation is expected to exceed $50 million per year once fully implemented. Both the direct compliance costs and direct benefit of the proposed regulation are independently expected to exceed this threshold. Our preliminary estimate of direct compliance costs is estimated to be $467-$16,454 million over the next decade (2020-30), depending on the number of California businesses coming into compliance (details below). Therefore, DOJ implementation of CCPA qualifies as a major regulation, requiring a complete SRIA.

1.3 Public Outreach and Input

DOJ held seven public forums statewide to solicit broad public participation as part of its preliminary rulemaking activities for CCPA. DOJ also set up a dedicated portion of its website to keep the public informed of various CCPA rulemaking activities, including the

transcripts from each of the public forums. In total, DOJ received input from over 110 speakers at the public forums and over 300 written comments, which were also posted on DOJ's CCPA website.

1.4 Regulatory Baseline

The CCPA will result in both benefits to consumers and costs to businesses, but for the purposes of this SRIA, we are tasked with identifying the additional costs and benefits from the regulations needed to successfully implement the law. An assessment of the economic impacts of the proposed regulations requires identifying the incremental impacts of the regulation beyond what would have happened in the absence of the regulation. This counterfactual, the absence of the regulation, is referred to as the regulatory baseline and is developed in detail in this section.

As noted in the introduction, while the CCPA gives the California DOJ broad authority to write implementing regulations, many of the benefits and costs are likely to be incurred regardless of the specific regulations. Some of these economic impacts, whether compliance costs to businesses or benefits to California consumers, are part of the regulatory baseline and not directly attributable to the proposed regulations. This interpretation is supported by evidence showing that businesses are making large up-front investments in CCPA compliance strategies, based on their review of the statutory text, ahead of the issuance of the first round of regulations.[1] For consumers, the law, not the regulations, establishes the main privacy rights and benefits, which are therefore also assumed to largely be a part of the regulatory baseline.

The incremental regulatory impacts, for which we analyze the economic impacts in this SRIA, include regulatory actions proposed by DOJ that differ from how a regulated business might interpret the CCPA in the absence of guiding regulations. In other words, we assume that in the regulatory baseline, businesses either follow exactly what the CCPA requires or utilize full discretion in areas where the CCPA does not provide explicit guidance. In areas where this distinction is not clear, we default to assuming that the economic impacts are fully attributable to the regulation. We also include a detailed discussion of the baseline costs and benefits that we assume to be attributable to the CCPA. The intent of this is to highlight the potential costs attributable to the CCPA along with the potential incremental costs directly attributable to DOJ's regulations.

[1] The 2019 analysis, published by TrustArc Inc, found that 84% of respondents had started CCPA compliance efforts and 56% had begun implementing their CCPA compliance plans.

1.4.1 Baseline Costs to Businesses

The California Consumer Privacy Act of 2018 requires qualifying businesses operating in California to take a number of compliance actions that go beyond standard business practices prior to passage of the privacy law. New systems must be put into place to respond to requests from consumers exercising their rights under the law. In general, compliance costs associated with the CCPA fall into four categories:

1. **Legal**: Costs associated with interpreting the law so that operational and technical plans can be made within a business.

2. **Operational**: Costs associated with establishing the non-technical infrastructure to comply with the law's requirements.

3. **Technical**: Costs associated with establishing technologies necessary to respond to consumer requests and other aspects of the law.

4. **Business**: Costs associated with other business decisions that will result from the law, such as renegotiating service provider contracts and changing business models to change the way personal information is handled or sold.

Total CCPA compliance costs are likely to vary considerably based on the type of company, the maturity of the businesses current privacy compliance system, the number of California consumers they provide goods and services to, and how personal information is currently used in the business. A recent survey by TrustArc of businesses expecting to need to undertake compliance actions for CCPA found that 29% of businesses expect to spend less than $100,000 (or nothing) on compliance, 32% expect to spend $100,000-$500,000, 20% expect to spend $500,000-$1,000,000, 15% expect to spend $1,000,000-$5,000,000, and 4% of businesses expect to spend more than $5,000,000. While these estimates of costs are quite large, the majority of these economic costs are attributable to the CCPA, not the DOJ's regulations. Furthermore, the survey was only sent to businesses with more than 500 employees. Nearly 99% of California businesses have fewer than 500 employees.

The first cost category for CCPA compliance includes all legal fees incurred in preparing for the law. These costs can be quite large, ranging from $50,000 to $1,000,000, according to informal consultations. However, we assume that these costs are not attributable to the regulation, since businesses would need this legal advice regardless of the regulatory actions taken by DOJ.

Operational costs, which can include substantial labor costs as multiple departments in an organization coordinate a business' compliance strategy and workflow, are also almost

entirely attributable to the law. The CCPA is very clear about what rights consumers have and that businesses must respond to opt-out, deletion, and access requests. The majority of these costs, which are incurred even before the regulations are drafted, would be incurred regardless of how DOJ crafted the specific regulations. However, the operational compliance costs of the ongoing training requirements and some record-keeping requirements for firms with more than 4 million California consumers are directly attributable to the regulations and are therefore calculated in this assessment.

Technology costs, which cover the websites, forms, and other systems necessary to fulfill the CCPA compliance obligations, are also quite substantial due to passage of the CCPA. However, like operational costs, these are mostly attributable to the law, not the regulation. As an example, consider the "Do Not Sell My Personal Information" link required by the law. All CCPA-compliant companies must include this link on their webpages; however, the DOJ regulations will give them guidance on what must be included on the webpage to which the link directs consumers. While there might be some design costs that could be attributed to DOJ's requirements, the vast majority of the cost of including the link is attributable to that requirement in the law.

For the areas of incremental economic impact that we have described above, the SRIA calculates, to the extent possible, an estimate of this cost for California businesses. To reiterate, these are the costs that we assume are directly attributable to DOJ's regulations, not the CCPA overall.

To put these incremental costs in perspective, we generate a back of the envelope cost of CCPA compliance, including both the statute's baseline costs and the incremental costs attributable to the regulations, using estimates from the TrustArc survey cited above. Assume that smaller firms (<20 employees) will incur $50,000 in initial costs (the median of the lowest cost category)[2], medium-sized firms (20-100 employees) incur an initial cost of $100,000 (the maximum of the lowest cost category in the survey), medium/large firms (100-500 employees) incur an initial cost of $450,000, and firms with greater than 500 employees incur, on average an initial cost of $2 million. Also assume that 75% of all California businesses will be required to comply with the CCPA (see Section 2.1 for detailed estimates of the number of firms affected by firm size and industry). The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately $55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018.

[2] The TrustArc survey only sampled privacy professionals from firms with at least 500 employees. Therefore, it is very possible that we are overestimating the compliance costs for smaller firms. However, in the absence of reliable compliance cost information for this category of businesses, applying the TrustArc estimates provides an upper bound on the total compliance costs.

1.4.2 Precedence from European Standards

The most comparable existing privacy regulation enacted is the European Union's General Data Protection Regulation (GDPR). While the CCPA is narrower in scope – it only applies to California businesses meeting specific criteria (described in Section 2.1) whereas the GDPR applies to all businesses that process data of EU citizens – both regulations are designed to improve protections on consumers' personal information and alter the way that personal data is collected and sold. In fact, standards and compliance for the GDPR have already imposed costs on many firms that operate in California. This reduces their expected cost of CCPA compliance and may offer useful guidance regarding the costs of enterprise adaptation to California standards. The EU's impact assessment of the GDPR estimated average incremental compliance costs of approximately 5,700 Euros per year (European Commission 2012, Annex 9). This is consistent with other compliance cost estimates ranging from 3,000 to 7,200 Euros per year (Christensen et al 2013). Collectively, these costs represent a 16-40% increase in annual IT budgets (Christensen et al 2013). In addition to compliance costs, there is also evidence that the GDPR's stricter data policies have reduced firm productivity in sectors that rely heavily on data (Ferracane et al 2019) with the biggest impacts found in firms devoted to data profiling (Cave et al 2012).

The GDPR also applies to many companies in California and, according to a recent survey by TrustArc, 83% of companies that have GDPR compliance requirements are expected to leverage some of their compliance programs for CCPA. For these companies, the work done on GDPR compliance will lower the compliance cost of CCPA, however given that the two privacy laws are not identical, businesses will not likely be able to fully apply their GDPR compliance systems to California consumers.

1.4.3 Baseline Benefits to Consumers

The CCPA's benefits to consumers derive from the privacy protections granted by the law. These protections, described in the previous section, give consumers the right to assert control over the use of their personal information. The economic value to consumers of these protections can be measured as the total value of consumers' personal information, which they can choose to prevent the sale of or even delete. Although the subjective value of this information to consumers is generally agreed to be great, it is extremely difficult to quantify the precise value of consumers' personal information in the marketplace and estimates can vary substantially. There is, for example, no universal method for pricing personal information. It is frequently argued that the value of personal information faces too many barriers to be accurately priced. Either data is dependent on trade secrets and algorithms, is too context-specific, or the underlying value, such as privacy, is intangible. Indeed, even companies who use

personal information as primary strategic asset typically have difficulty assigning value (Short and Todd 2017). That being said, assigning value to personal data is not impossible. Although there is not a single universal value, there are several approaches that have been used to price information.

One approach to estimating the value of consumers' personal information is to carry out experiments where participants are given options to pay different prices for different levels of privacy protections. Using this approach, one experiment found that consumers assigned $1.19-$4.05 of value per app to personal information collected by smartphone apps (Savage and Waldman 2017). Scaling this up to the approximate number of apps downloaded by Californians in 2017[3] suggests the aggregate value of consumers' private information on the app marketplace to be $1.6 – 5.4B.

An alternative approach to measuring the value of CCPA's protections of personal information is to estimate the price businesses are willing to pay for it. Several efforts have been undertaken to collect and publish the price that data brokers charge for a typical consumer's data. For example, *The Financial Times* collected data on prices companies pay for different types of basic personal information (age, gender, marital status, etc.). Using this data, they published a calculator that allows individuals to estimate the value of a one-time sale of their basic personal data.[4] General information about a person such as their age and gender were found to be worth $0.0005 per person. However, milestones in peoples' lives such as marriage, buying a car, getting divorced, etc. were worth more. The price of information that a woman is pregnant, for example, was priced at $0.11 per person. Collectively, the total value of the 61 basic information items examined sums up to approximately $4.83 for the average person. Other analogous efforts have examined more detailed private data, including financial history, and estimated a value of $277.65 per person for the one-time sale of these pieces of personal information.[5] These estimates can be used to calculate the aggregate value of consumers' personal information. There are approximately 35M internet users in California,[6] therefore using the Financial Times estimates the implied total value of consumers' basic information under protection would be approximately $169M while the implied total of consumers' more sensitive personal information according to the SWIPE tool would be $9.7B. These numbers illustrate that while, on an individual level, most personal information is at most moderately valuable, the aggregate value to consumers

[3] Americans had approximately 11.3B app downloads in 2017 [www.statista.com/statistics/249264/countries-ranked-by-number-of-app-downloads/]. Given Californians are 12% of the U.S. population, and assuming Californians download apps at the same rate as other Americans, these numbers suggest Californians downloaded approximately 1.1B apps in 2017.

[4] https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R; Steele et al 2013.

[5] http://turbulence.org/Works/swipe/swipe_data_cal.html

[6] Census 2015 Supplementary Survey/American Community Survey (C2SS/ACS) (U.S. Census Bureau, 2010).

is large. Given the thousands of pieces of personal information collected by businesses, it is not realistic for these estimates to be comprehensive of all personal information. Instead, these estimates can be viewed as lower bound estimates on the value of basic, and more detailed, personal information that indicate the magnitude of the value of consumer data that the CCPA covers.

A final approach estimates the value of personal data based on financial records on a per-user or per-record basis. Common financial records include market capitalization, revenue, or net income. Revenue, and especially advertising revenue, is the most robust indicator as it reflects the market value for access to personal data. While finding the average revenue per user (ARPU) is relatively straightforward, decisions must be made about what firms to include. Typically, large tech companies that derive the majority of their revenue from personal data are used to price the value of personal data. However, the per-company approach is piecemeal and although large tech companies represent the majority of advertising revenue, they do not capture all of it. We therefore instead choose to focus on total digital advertising revenue, which is reported annually by the Interactive Advertising Bureau (IAB) trade-group. This measure reports all internet/mobile/online advertising revenue in the United States. Unlike traditional advertising, where all customers receive the same ad, online advertising is defined by its use of targeted (i.e. personal) ads. Therefore, this measure arguably captures the market value of personal data in the United States.

The IAB reports total advertising revenue split between desktop and mobile. Each of these categories are further subdivided between an additional four categories: Search, Banner, Video, Other. Of these categories, we assume search, banner, and video advertising all rely on personal data to target ads. The other category is comprised of classifieds, lead generation, and audio (podcasts), whose use of personal data is less clear. With estimates for total online advertising revenue for search, banner, and video the challenge becomes matching these estimates to the number of desktop and mobile phone users in the United States. Using ACS data, we are able to find the total number of internet users with both a computer and mobile, or only mobile, or only computer. With these estimates we are then able to estimate that ARPU for Mobile and Desktop online advertising. To reach estimates for the total value of personal data for California consumers we then take the ARPU estimates and multiply by the relevant number of computer and/or mobile users in California.

We find that the 2018 ARPU for search, banner, and video adds are $135.71 (desktop) and $266 (mobile). With an estimated 30.9 million desktop users and 31.7 mobile users in California this represents a total value of $4.2 billion and $8.4 billion respectively.

Overall, this would suggest that value of personal information used for advertising in California is over $12 billion annually.

The above estimates suggest that the aggregate value of personal data that falls under the CCPA is large, likely on the order of magnitude of tens of billions of dollars. Each of these effects should be considered cumulatively as well. The value of personal information based on data brokers is separate from that of digital advertising. Therefore, combining those estimates suggests the total value of personal data would exceed $20 billion annually. Furthermore, since personal data is non-rival, the sale of one personal data profile does not preclude the sale of an additional one. This means that not only can specific data brokers sell the same profile numerous times, but that different companies can sell a profile representing the same individual as well. Thus, these above estimates represent a lower bound and should be taken as conservative values for personal information.

That being said, consumers only receive maximal benefits if they choose to exercise the privacy rights given to them and not everyone is likely to do so, although, available evidence indicates that a substantial portion of consumers have preferences that align with exercising rights provided by the CCPA. In a 2012 survey from the Pew Research Center, roughly two-thirds of consumers (68%) reported that they did not like targeted advertising because they did not want to have their online behavior tracked and analyzed (Purcell 2012). Moreover, a 2015 Pew survey found that 90% of respondents preferred to be in control of what personal information is available and being utilized by businesses (Madden & Rainie 2015). The CCPA provides consumers the opportunities to exercise these preferences by becoming informed of how their personal information is being collected and used, limiting the sale of this information, and requesting that it be deleted.

1.4.4 Equity considerations

The CCPA will introduce differential benefits for consumers largely related to wealth and income. While the CCPA increases the ease with which consumers can access, control, delete, and stop the sale of their data, some users may be unable to navigate the procedures required to access these rights. The CCPA requires that businesses make it straightforward for an average consumer to exercise their privacy rights. However, there is no guarantee that all consumers will be able to understand how to manage these processes. Insofar as other personal characteristics correlate with computer literacy, there may be equity concerns whether disadvantaged groups disproportionately do not exercise the privacy rights afforded to them by the CCPA. Furthermore, the stipulation that businesses can charge consumers for their services means that low-income groups may be more likely to give up their personal information in exchange for services while high-income groups are more likely to pay the service fee to protect their data.

Furthermore, there are serious equity considerations related to the ability for consumers to pay for a digital service using either money or data. When paying with data, users consent to allow businesses to use their data in return for services. Conversely, the payment option would allow users to make some type of monetary payment (either one-off or monthly) to use a service and explicitly forbid businesses to use their data. This suggests that low-income groups may be more likely to give up their personal information in exchange for services while high-income groups will pay the service fee to protect their data. In turn, the CCPA could create a system of two-tiers, where higher socio-economic groups are able to protect their personal information and disadvantaged groups have no choice but to allow their data to be used.

1.5 Incremental Impacts of the Proposed Regulation

In this section we identify provisions in the proposed regulation that are assumed to have incremental economic impacts that deviate from the regulatory baseline. For each article in the proposed regulation, we briefly describe the general purpose of the article and in instances where no incremental impact is assumed, we provide a justification for this assumption.

1.5.1 Article 2: Notices to Consumers

This section of the proposed regulation establishes rules regarding how businesses must notify consumers about their rights under the CCPA. There are four general notification requirement regulations developed by DOJ:

1. **Notice at Collection of Personal Information** - The regulations detail requirements for businesses to provide a notice communicating to consumers what type of information is being collected and for what purpose.

2. **Notice of the Right to Opt-Out of the Sale of Personal Information** - The regulations detail notification requirements for businesses that sell consumers' personal information and provide guidance on how businesses must communicate to consumers that they can opt out of the sale of their information to third parties.

3. **Notice of Financial Incentive** - The regulations detail notification requirements for businesses to clearly notify the consumer of financial incentives or price differentials being offered in exchange for using (internally or through sale) the consumer's personal information.

4. **Privacy Policy** –The regulations detail requirements for businesses to disclose in a privacy policy their online and offline practices regarding the collection, use,

disclosure, and sale of personal information, and of the rights of consumers regarding their PI.

We assume that none of the economic impacts associated with these notification requirements are directly attributable to the proposed regulation. Because notification requirements are required under the CCPA, the economic impacts of developing these notifications are part of the regulatory baseline. The DOJ regulations provide guidance to businesses on how they must structure the notification requirements but the resources required to do this are not likely to be different than what businesses would otherwise do to meet CCPA requirements.

1.5.2 Article 3: Business Practices for Handling Consumer Requests

This section of the proposed regulation establishes rules about how businesses must respond to personal information requests from consumers.

Establishing processes to respond to consumer requests is likely to require businesses to incur substantial costs. Most of these costs are attributable to the CCPA and not to DOJ's implementing regulations; however, there are certain aspects in Article 3 of the proposed regulation where DOJ had considerable flexibility to exercise discretion in drafting the regulations and these areas are assumed to have economic impacts attributable to the regulations rather than the CCPA. The incremental impacts include costs and/or benefits associated with:

1. Additional technology and operational costs for establishing systems for businesses and service providers to respond to consumer requests.

2. Notification to third parties to whom personal information was sold within the past 90 days, if a consumer makes an opt-out request.

3. Training requirements for employees in businesses that handle the personal information of more than 4 million consumers.

4. Recording-keeping requirements for businesses that handle the personal information of more than 4 million consumers.

All other economic impacts associated with language in Article 3 are assumed to be attributable to the CCPA and are therefore included in the regulatory baseline.

1.5.3 Article 4: Verification of Requests

Article 4 of the proposed regulation establishes rules about how business must go about verifying the identity of consumers making personal information requests. This is an area

where the CCPA gives DOJ considerable discretion in crafting the regulations. DOJ has chosen to separate verification of consumer requests into two categories: verification of consumers who have a password-protected account with a business and consumers who do not have a password-protected account with a business.

For consumers that have a password-protected account with a business, if the business is following existing privacy laws then the password authentication process is likely sufficient for verifying a consumer's identity. In this case, we assume that the regulations will have little or no incremental economic impact for consumer verification.

However, for consumers who exchange personal information with a business but do not have a password-protected account, the business must verify the identity of the consumer to either a reasonable degree of certainty or a reasonably high degree of certainty depending on the nature of the request. This may require matching at least two data points provided by the consumer to information maintained by the business, or three pieces of PI provided by the consumer with information maintained by the business and a signed declaration under penalty of perjury. The economic impact associated with this verification process is assumed to be attributable to the regulation and thus is addressed in this analysis.

1.5.4 Article 5: Special Rules Regarding Minors

The CCPA specifies that if a business collects personal information from minors 16 years or younger, it must obtain the affirmative authorization of the minor (if 13-16 years of age), or their parent or guardian (if the minor is under 13 years of age), to sell that information. The DOJ regulations outlined in Article 5 specify the process for opting-in. DOJ's regulations are meant to allow businesses to build on existing processes and systems they use for verifying parental consent under the Children's Online Privacy Protection Act (COPPA). However, COPPA requires consent for collection of data, whereas the CCPA requires consent for sale. Therefore, the DOJ regulations will require that additional notification of consent for sale. Any impacts associated with this can be directly attributable to the regulations.

1.5.5 Article 6: Non-Discrimination

The non-discrimination regulations proposed by DOJ attempt to clarify language in the CCPA about business practices that treat consumers who exercise their rights under the CCPA differently, such as by providing financial incentives or differential services/prices. The CCPA's anti-discrimination clause says that businesses cannot discriminate against consumers for exercising their CCPA rights (opt-out, right to know, and right to delete); however, a business can offer a financial incentive or a price or service difference if it is reasonably related to the value of the consumer's data to the business. While these

provisions are included in the CCPA, and are therefore part of the regulatory baseline, the CCPA directs DOJ to provide guidance to businesses on exactly how a business should determine the value of a consumer's data. We assume that there are economic impacts associated with how this definition of value is determined that are directly attributable to the DOJ regulations and thus should be included in the SRIA.

Table 1: Incremental Economic Impacts from DOJ's CCPA Regulations

Section of the Regulation	Incremental Economic Impacts
Article 2: Notices to Consumers	None attributable to regulation
Article 3: Business Practices for Handling Consumer Requests	(1) Fraction of technology and operational costs of implementing systems for handling requests. (2) 90-day third-party notification of opt-out requests. (3) Training requirements (4) Record-keeping requirements
Article 4: Verification of Requests	(5) Cost of verifying identity for non-accountholders
Article 5: Special Rules Regarding Minors	(6) Additional notification and verification requirement beyond COPPA.
Article 6: Non-Discrimination	(7) Impact associated with how the value of personal information can be calculated by businesses.

2 Impacts on California Businesses

In terms of measurable direct costs, the most consequential aspect of CCPA will be investments in compliance activity by enterprises operating in California. This section describes the incremental compliance cost estimates used in this SRIA, representing each of several categories of incremental impact identified in the regulatory baseline.

2.1 How many firms are impacted by CCPA?

Not all businesses that handle the personal information of California residents are required to comply with the CCPA. The law established three thresholds, each of which would trigger compliance requirements if reached. They are:

1. A business has annual gross revenues of more than $25 million,
2. A business buys, sells, or shares the personal information of more than 50,000 consumers, households, or devices per year,
3. A business derives 50% or more of its annual revenue from selling consumers' personal information.

As a lower-bound estimate of the number of businesses that will be required to comply with CCPA, we use 2017 Survey of U.S. Businesses (SUSB) data from the U.S. Census Bureau. This data reports the number of firms by sector and number of employees for California. Because the data does not include data on business revenue, we assume that the average employee generates approximately $100,000 in annual revenue. Based on this assumption, firms with more than 250 employees will meet the $25 million CCPA threshold. Employee size categories in the SUSB data are reported for businesses with 100-499 employees and businesses with 500 or more employees. We assume that all businesses with 500+ employees will be subject to the CCPA and 37.5% of businesses in the 100-499 employee category will need to comply with the law.

A lack of data prevents us from estimating with precision the number of businesses that meet the other threshold requirements in the CCPA. However, it is likely that the 50,000 PI requirement and the 50% annual revenue requirement will apply to many businesses with annual revenues less than $25 million. For example, any firm that collects personal information from more than 137 consumers or devices a day will meet the 50,000 threshold. To provide an upper bound on the number of firms potentially affected by the CCPA regulations, we consider two alternative assumptions. We assume that either 50% or 75% of all California businesses that earn less than $25 million in revenue will be covered under than CCPA. A survey completed by the International Association Privacy

Professionals (IAPP) found that 8 out of 10 surveyed businesses believed that they would need to take compliance actions as a result of the CCPA. Because the survey went only to businesses in certain sectors likely to be covered by the law, the 50-75% upper-bound compliance range is reasonably supported by empirical evidence.

The SRIA requires an analysis of the impact of proposed major regulations on California businesses. However, the CCPA will also affect businesses that provide goods and services to California consumers. There are likely to be many businesses that are not located in California (and therefore not captured in SUSB statistics) but serve California customers. The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.

Table 2 shows the total number that would either exceed the $25 million annual revenue threshold or require compliance under the 50% and 75% scenarios. While the law says that medical information is not covered as personal information under the CCPA, we assume that large firms in the health care sector will still likely need to comply with the law as they collect other non-medical personal information on consumers. We also show the number of firms with greater than 500 employees, which will be used for assessing certain compliance costs later in the analysis.

The lower bound estimate of the number of businesses affected by the proposed regulations is 15,643. The upper bound estimates, depending on whether one assumes 50% or 75% of businesses will be impacted, ranges from 383,323 to 570,066. This large range of potentially impacted businesses will have important implications for the total compliance costs of the proposed regulations.

The SRIA requires an analysis of the impact of proposed major regulations on California businesses. However, the CCPA will also affect businesses that provide goods and services to California consumers. There are likely to be many businesses that are not located in California (and therefore not captured in SUSB statistics) but serve California customers. The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.

Table 2: Number of California Businesses Meeting the $25 Million CCPA Revenue Threshold

NAICS Code	Description	>$25 million revenue threshold	50% Threshold	75% Threshold	Firms with 500+ Employees
11					21
21	Mining, Quarrying, and Oil and Gas Extraction	71	310	434	61
22	Utilities	46	285	408	40
23	Construction	573	35,592	53,256	264
31-33	Manufacturing	1,612	18,352	27,016	1,025
42	Wholesale Trade	1,657	26,134	38,658	1,087
44-45	Retail Trade	1,079	35,382	52,746	656
48-49	Transportation & Warehousing	832	10,154	14,923	615
51	Information	678	8,579	12,634	469
52	Finance and Insurance	818	14,843	21,962	606
53	Real Estate, Rental, Leasing	461	21,628	32,289	304
54	Professional, Scientific, and Technical Services	1,728	58,404	87,038	1,137
55	Management of Companies and Enterprises	1,537	2,196	2,708	1,171
56	Administrative/Support/Waste Mgmt. Svs.	1,120	19,100	28,290	722
61	Educational Services	411	6,386	9,479	202
62	Health Care and Social Assistance	1,165	46,078	68,842	550
71	Arts, Entertainment, and Recreation	281	11,806	17,634	151
72	Accommodation and Food Services	986	33,024	49,301	470
81	Other Services (except Public Administration)	550	34,133	51,046	307
99	Industries Not Classified	0	1,473	2,210	0
Total		15,643	383,328	570,066	9,858

2.2 Article 3 Costs – Business Practices for Handling Consumer Requests

There are four specific incremental costs for businesses complying with DOJ's Article 3 regulations that are assumed to be directly attributable to the regulation. These are:

a) The small fraction of technology and operations costs that will directly exceed an average businesses or service provider's interpretation of the CCPA due to the specificity of the regulations.

b) The costs of complying with DOJ's 90-day lookback requirement for firms selling personal information to third parties.

c) The more detailed training requirements for firms handling the personal information of more than 4 million California consumers.

d) The more detailed record-keeping requirements for firms handling the personal information of more than 4 million California consumers.

2.2.1 Operations and Technology Costs

We assume that a small fraction of the operational and technology costs associated with the CCPA are likely to be attributable to the regulation. Operational costs are predominantly a one-time cost of establishing workflows, plans, and other inter-departmental non-technical systems to determine the business' best compliance pathway under the CCPA. These costs are largely labor costs associated with meetings and compliance planning. For illustrative purposes we assume that for large companies, a separate employee from three different departments in an organization will need to coordinate with weekly meetings (2 hours each) for 6 months. For the value of these employees' time, we assume the 2018 median annual salary of a data privacy officer ($123,050). We assume that 10% of these costs are directly attributable to the regulation, with the rest attributable to the CCPA baseline. The total annual cost attributable to the regulation for a representative firm is therefore $959 in the initial year of compliance. Applied to all firms with revenue greater than $25 million per year, the total compliance costs for operational compliance is approximately $15 million. Applying this incremental cost using the 50% and 75% thresholds increases the total operational costs attributable to the regulation to $368 million and $547 million.

Costs associated with developing technological systems to comply with the CCPA are also likely to be significant and will vary considerably by firm and sector. For large firms, many are likely to allocate in-house engineering resources to develop specialized systems. Firms that handle less personal information and that are not using that personal information as a key aspect of their business models are not likely to develop complicated

technological platforms to respond to CCPA requests, especially in the early phase of CCPA compliance. New technologies may develop over time to provide businesses with technological platforms that do provide these services. Because of considerable variation and uncertainty in technology costs prior to CCPA implementation, we assume that 25% of total expected compliance costs reported by firms are likely to be for the technology requirements necessary to respond to CCPA requests. Based on the TrustArc firm survey cited above, we assume a central value of for technology costs of $75,000 per firm, 10% of which we assume is directly attributable to the DOJ regulations.

If a consumer contacts a service provider with a request to know or request to delete, according to the DOJ regulations, the service provider must provide the consumer with the contact information of the business on whose behalf the service provider processes the information when feasible. The CCPA requires that service providers comply with businesses' direction to delete/stop selling personal information but does not provide guidance on whether or how a service provider should respond directly to consumers. The regulatory requirement that service providers respond to consumer requests by providing the contact information for the primary PI-collecting business will likely require the service provider to build out a process for responding to requests and identifying which business it is servicing. It is not possible to quantify this cost ex ante since there are no data sources that identify the number of service providers located in California. However, we would expect it to be a small fraction of the costs incurred by businesses handling personal information directly from consumers as these companies build out the technology and operational systems necessary to respond to consumer requests.

2.2.2 90-Day Lookback Costs

The DOJ's CCPA regulations specify that if a consumer makes an opt-out of sale request, the business must notify any third party that was sold the consumer's information in the past 90 days that the consumer has withdrawn their consent to sell the data. These third parties are then no longer allowed to sell the data. The CCPA did not specify that the third party who had received the data up to 90 days prior must discontinue further sales of the data. The law could instead have been interpreted as saying that after an opt-out request is made, the firm could no longer make additional sales of the data, but that previous sales of personal information were not covered.

The incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible. Reliable data was not available to quantify this impact, which would require knowing how many businesses sell personal information to third parties. However, businesses that do sell personal information will need to retain records to track these sales and must allocate resources to communicating with third parties once an opt-out request is made. For larger

companies, it is quite plausible that this notification process will be built into automated systems so that additional staff resources are not required. If this is the case, the incremental compliance cost will be cost associated with building this capacity into the data mapping strategy and back-end technologies.

2.2.3 Training Requirements

The CCPA requires that individuals within a business that handle consumer inquiries are aware of the provisions of the law. There is no detailed guidance stating how these individuals will be made aware of the law and a plausible interpretation by a business would be to assume that privacy professionals are aware without any formal training. Under such an interpretation, the regulatory baseline would have no costs associated with employee training.

The DOJ regulations specify that firms collecting, buying, selling, or sharing the personal information of more than 4 million California consumers (approximately 10% of the State's population) must "establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA." We assume that there are additional costs associated with this training policy that are directly attributable to the regulations.

For simplicity, we assume that all firms with more than 500 employees will fall under the training requirements. This assumption is purely speculative since there is no detailed data on how many California consumers all companies in the State have. Industries are likely to fall into this compliance category if they are located in California, have little competition for their goods or services in the State, and collect personal information. For example, large electric power utilities are likely to use personal information from many California consumers for business purposes. Technology and social media companies that have large-scale adoption of their services are also likely to fall into this category.

To calculate the cost of training, we assume that the training will consist of requiring data professionals to read prepared training documents on the CCPA law and regulations. We assume that for large firms, there will be a team of approximately 5 privacy professionals that may handle consumer requests or be responsible for the business's CCPA compliance. Each individual will require two hours to complete the training and that the cost to the business is the opportunity cost of these employees' time. Assuming an average wage of $123,050 ($61.50/hour), the total cost per business is assumed to be $615/year ($61.5/hr x 2 hours x 5 individuals). The total compliance cost for the 9,858 businesses with more than 500 employees is $6.062 million per year.

2.2.4 Record-Keeping Requirements

Similar to the training requirements, the DOJ specifies additional record-keeping requirements for firms that collect, buy, sell, or share the personal information of more than 4 million California consumers. These businesses must compile a number metrics on consumer requests and business responses from the prior year. For example, the business must estimate the number of requests to know, requests to delete, and requests to opt out that were (1) received, (2) complied with, and (3) denied. The business must also compile the number of days that the business took to substantively responded to requests to know/delete/opt out.

For estimating the incremental cost of this recording-keeping requirement, we make several assumptions. First, because the businesses affected by this record-keeping requirement are already likely to have mature systems for identifying, processing, and analyzing personal information from their data mapping and consumer response systems, we assume that there is no incremental cost of actually collecting this information. We do assume that there is a labor cost associated with processing and reporting the information in a format in the businesses privacy policy that is in compliance with the DOJ regulations. We assume that this activity will take approximately two (2) days of time (16 hours) from a data privacy professional. Assuming a rate of $61.5/hour, each firm will incur a labor cost of $984/year. The total cost for businesses assumed to exceed the 4 million consumer threshold is $9.7 million per year. This cost is likely to be ongoing since the metrics must be reported every year.

2.3 Article 4 Costs – Verification of Requests

As noted in the regulatory baseline, there may be some additional compliance costs attributable to the regulation from a business needing to confirm the identity of consumers without accounts making CCPA requests. In theory, the costs associated with this compliance action could be calculated as follows:

Cost per firm = Number of California Consumers Doing Business with the Firm
x % of the Consumers Without an Account
x % of Consumers Making a CCPA Request
x Incremental Cost per Person of Verification

Each of these factors is likely to vary considerably from business to business and there are no data points that would allow an estimation of this impact ex ante. However, if businesses build out efficient systems for complying with other aspects of the CCPA related to handling consumer requests, the incremental cost of matching the identity of a consumer to personal information that the business already has is likely to be quite low. For companies that routinely handle personal information and have sophisticated privacy

systems in place, this verification process is likely to be automated. There will be an upfront cost of integrating this verification into the larger privacy ecosystem but marginal cost for an additional consumer verification could be close to zero. On the other end of the spectrum, for businesses that attempt to manually verify consumers without an account, the marginal cost would be the labor cost associated with having staff dedicated to this verification process. In this case, the cost would depend on the number of verification requests being made and the variable cost is likely to be quite high relative to any initial investments in developing the systems for automating verification.

2.4 Article 6 Costs – Non-Discrimination

The CCPA states that DOJ should adopt regulations regarding financial incentive offerings. The DOJ chose to outline eight broad methodological approaches that businesses could use to determine the value of consumer data for financial incentive offerings. For example, a business can use either the marginal or average value of a typical consumer's PI to the business. They can also base their determination of value on revenues, profits, or costs associated with the PI. As a final category, the regulations say that the business can use any other method of estimating the value, so long as it is made in good faith. Essentially, DOJ is telling businesses that they can use whatever method they prefer, so long as there is an actual method developed that is reasonable. The cost associated with this provision is simply the cost to develop the method for businesses that are using financial incentives. There is therefore an initial labor cost associated with developing and documenting the method. The various methods are likely to become standard business practice and therefore we assume that a business will likely need to devote about 1 day (8 hours) towards developing a methodological approach. Assuming an average hourly rate of $61.50, the average cost for a typical business will be approximately $492. Applied to the 15,646 businesses with revenue greater than $25 million per year, the total cost would be $7.7 million. Applied to the 383,382 and 570,066 businesses in the 50% and 75% compliance scenarios, costs associated with developing these methodologies would be $188.6 million and $280.5 million, respectively.

2.5 Total Enterprise Compliance Costs

Table 3 shows the total estimated costs by sector for the proposed regulations. Costs are estimated for each of the three thresholds used to assess the number of potentially affected firms. The most conservative estimate is for firms that exceed the $25 million annual revenue threshold, while the 50% and 75% threshold reflect assumptions that many additional firms would be subject to DOJ's CCPA regulations. It is important to note

that these costs only reflect quantified compliance costs. Some compliance costs noted in the previous sections did not have enough empirical evidence to support a compliance cost estimate. Furthermore, the novel nature of the CCPA and uncertainty regarding the expected compliance actions by firms across a diverse set of sectors should cause the reader to interpret these compliance costs estimates with caution.

Table 3: Total Estimated Compliance Costs (million 2019$)

NAICS Code	Description	>$25 million revenue threshold	50% Threshold	75% Threshold
11				40.5
21	Mining, Quarrying, and Oil and Gas Extraction	2.1	9.0	12.6
22	Utilities	1.4	8.3	11.8
23	Construction	16.9	1,026.8	1,536.1
31-33	Manufacturing	48.1	530.8	780.7
42	Wholesale Trade	49.5	755.3	1,116.5
44-45	Retail Trade	32.2	1,021.3	1,522.0
48-49	Transportation & Warehousing	25.0	293.8	431.3
51	Information	20.3	248.1	365.1
52	Finance and Insurance	24.6	429.0	634.3
53	Real Estate, Rental, Leasing	13.8	624.2	931.6
54	Professional, Scientific, and Technical Services	51.6	1,686.0	2,511.6
55	Management of Companies and Enterprises	46.2	65.2	80.0
56	Administrative/Support/Waste Mgmt. Svs.	33.5	551.9	816.9
61	Educational Services	12.2	184.5	273.7
62	Health Care and Social Assistance	34.5	1,329.6	1,986.0
71	Arts, Entertainment, and Recreation	8.3	340.7	508.7
72	Accommodation and Food Services	29.2	953.0	1,422.4
81	Other Services (except Public Administration)	16.4	984.8	1,472.5
Total		466.9	11,069.4	16,454.2

2.6 Incentives for Innovation

The CCPA will generate incentives for innovation across a range of new privacy products and services for consumers. Firms have already begun announcing new features intended to assist consumers with managing their private data while using the firm's products. These types of innovations are likely to accelerate. In addition to product specific features, there will also be incentives for provision of new services assisting consumers with utilizing CCPA protections to monitor and manage their data across products. Because consumers are required to communicate with each business individually, there is potential demand for a service that allows consumers to manage these many requests through a single interface and advises consumers on how best to utilize their rights to privacy overall.

Like consumers, firms will also demand new products and services in relation to the CCPA. New businesses or services are likely to be developed in order to assist firms with CCPA compliance. While initial efforts may focus on helping individual firm compliance, there will likely eventually be a relatively cheap standardized compliance assistance product developed analogous to software services designed to help individuals fill out their tax returns. Because of the large number and wide range of firms affected by the CCPA, there will be strong incentives to offer a relatively inexpensive product that can be marketed to a wide variety of firms, including smaller businesses, that do not have the internal capacity to manage compliance.

The CCPA will fundamentally change how firms work with personal data. Some industries will be forced to completely revise their business models to incorporate the newly required data protections. Data brokers, for example, will need to fundamentally change the way they operate. Adapting to the new privacy conditions will require innovations in the way firms use data. New data management systems that ensure privacy standards will need to be developed along with new techniques to extract useful information from data with obscured identifying personal information. The CCPA may, somewhat counterintuitively, also provide firms with new opportunities to expand data-based research and products. If the CCPA increases consumers' trust of data protections it could actually *increase* the amount of data that consumers are willing to share with firms. Despite the additional controls put on data use, increased access to users' data could help improve business' capacity to produce and bring research to market as well as increase firm capacity for product innovation.

2.7 Small Business Impacts

Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. Conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms that derive the majority of their revenue from personal data, however evidence from the EU suggests the opposite may be true. Over a year after the introduction of the GDPR, concerns regarding its impact on larger firms appear to have been overstated, while many smaller firms have struggled to meet compliance costs. Resources explain this dichotomy as large technology companies are often several steps ahead of both competitors and regulators. In fact, some have even argued that the GDPR has provided a competitive advantage to large firms as their significant in-house regulatory resources have allowed them to adjust quicker, while smaller competitors have struggled to adapt (Scott et al. 2019).

Small firms in California will face similar pressures. Large technology firms that are already GDPR-compliant will likely find it easier to become CCPA-compliant. Furthermore, with more revenue, large companies are better suited to absorb up-front compliance costs. Another significant risk to small businesses is uncertainty. Even after the roll out of regulations, interpretation and implementation present additional challenges to ensure full compliance for small enterprises. In the example of the GDPR, some firms report struggling with understanding compliance requirements, which has made compliance harder for small firms (Scott et al 2019).

These concerns will present real challenges for small businesses in the short term. In the long term however, the differential impacts will be smaller as third-party service providers enter the market to offer small businesses low-cost tailored compliance solutions. Although some small businesses will use in-house resources to become compliant, we expect that many others will outsource this work to dedicated firms. As competition in this new market increases, we expect overall costs to fall, limiting the differential impacts between small and large businesses in the long run.

2.8 Competitive Advantage/Disadvantages for California Businesses

For firms that operate within the state of California, the regulation will provide a competitive disadvantage relative to firms that operate only outside of the state. This is purely a reflection of compliance costs as firms that are subject to the regulation will face higher costs than those that are not. The most affected firms are those that have over $25 million in revenue that have competitors of a similar size operating only outside of California. These firms will be at a disadvantage when competing in markets outside of California, as they will be faced with higher compliance costs relative to their competitors.

We anticipate the competitive disadvantage to be small, however. Given the size of the California economy, previous legislation that was unique to California has in turn set national standards as firms find it easier to adopt California's requirements to all products and services rather than provide differentiated services. Furthermore, there is likely limited direct competition between firms that would be subject to the regulation and those that would not. Either the firm is small and localized and would not compete directly with outside firms or is large enough that outside competitors have a California component to their business already and would be subject to the regulation as well.

On the other hand, the regulation may also provide a future competitive advantage for affected firms that are required to come into CCPA compliance now by creating additional barriers to entry for future competitors considering entering into the California market. Moreover, if the CCPA is a precursor for future privacy regulations at the additional state or federal level, then firms already in compliance with the CCPA will have a competitive advantage over firms that are not. Indeed, this already appears to be the case as legislators in nine states have introduced bills that would follow either all or part of the model established in the CCPA. Therefore, firms that become CCPA-compliant now will be better positioned to adapt to future privacy protection regulations.

3 Impacts on California Consumers

As its name implies, the primary impetus for CCPA is to improve the wellbeing of California consumers. While much of the policy dialog on individual privacy emphasizes non-pecuniary benefits, this economic assessment confines itself to measurable economic benefits that could reasonably be expected to accrue to private individuals from CCPA implementation. This section discusses the incremental pecuniary benefits for the state's consumers in the main categories of incremental impact identified in the regulatory baseline.

3.1 How many consumers are impacted by the CCPA?

The personal information of all Californians is covered by the CCPA. According to the American Community Survey, there are 35M people in California that have internet access, either with a computer or a mobile phone. While the CCPA covers online and offline businesses, these online consumers will be the primary beneficiaries of the privacy protections afforded by the law.

3.2 Article 2 Benefits – Notice to Consumers

While the CCPA requires that businesses notify consumers about their CCPA rights, the proposed regulation establishes additional specifics regarding the format of these notifications. The incremental benefit of the regulation, therefore, includes the effects from the additional understanding of privacy rights *that would not have been achieved under notifications constructed without the regulation's guidelines*. This additional understanding could lead to more consumers exercising their CCPA rights and, in turn, protecting their personal information which has a positive value to consumers. However, given all of the uncertainties, it is not possible to quantify the magnitude of this benefit.

3.3 Article 3 Benefits – Business Practices for Handling Consumer Requests

3.3.1 90-day Lookback Requirement

Article 3 specifies that if a consumer makes an opt-out of sale request, the business must notify any third party that was sold the consumer's information in the past 90 days that the consumer has withdrawn their consent to sell the data. These third parties are then no longer allowed to sell the data further. The incremental benefit to consumers is stopping data sales among third parties to whom their data was sold in the past 90 days. The economic value of this benefit will depend on the value of the data types sold, the number of third party data transactions, and the number of consumers that request

businesses stop selling their data. However, because we do not reliable information on the volume of third party data sales, it is not possible to quantify this benefit.

3.3.2 Training Requirements

The DOJ regulations specify that firms collecting, buying, selling, or sharing the personal information of more than 4 million California consumers must "establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA." The benefit to consumers of additional business training will be an incrementally higher likelihood that businesses will follow the stipulations in the CCPA and that consumers' personal information will be accurately given the protections provided by the CCPA.

3.3.3 Record Keeping

The regulation specifies additional record-keeping requirements for firms that collect, buy, sell, or share the personal information of more than 4 million California consumers. These businesses must compile a number metrics on consumer requests and business responses from the prior year. The benefit to consumers is increased transparency with respect to business compliance of consumer requests to access, delete, and opt out of data sales. While this benefit is not easily quantifiable, the transparency requirements make it more likely that consumers' requests to exercise their CCPA provided protections will be fulfilled completely and in a timely manner.

3.4 Article 4 Benefits – Verification of Requests

The regulation provides additional requirements for confirming the identity of consumers without accounts making CCPA requests. This will benefit consumers by limiting the possibility that someone posing as them gains access to or affects the privacy of their personal information through a fraudulent CCPA request. While this is expected to benefit consumers, the magnitude of the benefit is not easily quantifiable.

3.5 Article 5 Benefits – Special Rules Regarding Minors

The CCPA specifies that if a business collects personal information from minors to sell, the minor (if 13-16 years of age) or their parent or guardian (if under 13 years of age) must explicitly opt-in to the sale of that information. Article 5 of the proposed regulation specifies the process for opting-in. A benefit will accrue to minors who do not want their personal information sold, but who might have opted in with the CCPA (but without the proposed regulation), and who would not opt in under the proposed regulation. We do not have sufficient information on the number of minors in this group to quantify this benefit.

3.6 Article 6 Benefits – Non-Discrimination

The non-discrimination regulations proposed by DOJ attempt to clarify language in the CCPA about business practices that involve providing financial incentives or differential services/prices for consumers who exercise their rights under the CCPA. The CCPA directs DOJ to provide guidance to businesses regarding financial incentive offerings and the proposed regulation provides guidance on how businesses should calculate the value of consumer date for that purpose. The impact of the proposed regulation on consumers will therefore depend on the difference between how businesses would have calculated the value of consumer data absent the proposed regulation and how they will calculate the value of consumer data given the additional guidelines. Because businesses are allowed to charge consumers who exercise CCPA privacy rights for services at a price equivalent to the value of their personal information, we assume that the value of personal information calculated by businesses under the additional guidelines in the proposed regulation will be lower than they would have been absent the proposed regulation. If this is the case then the quantity of consumer benefits will be derived from the difference in prices charged with and without the proposed regulation. However, we do not have enough information to quantify this benefit.

4 Macroeconomic Impacts

4.1 Methodology

The economy-wide impacts of the proposed CCPA regulation will be evaluated using the BEAR forecasting model. The BEAR model is a dynamic computable general equilibrium (CGE) model of the California economy. The model explicitly represents demand, supply, and resource allocation across the California economy, estimating economic outcomes over the period 2015-2030. For this SRIA, the BEAR model is aggregated to 60 economic sectors, with detailed representation of the construction sectors most likely affected by the CCPA.

The current version of the BEAR model is calibrated using 2017 IMPLAN data for the California economy (BEAR: 2016b). Both the baseline and policy scenarios use the Department of Finance conforming forecast from June 2019. The conforming forecast provides assumptions on GDP growth projections for the State and population forecasts.

4.2 Scenarios

The macroeconomic impact results are based on the expected changes in compliance costs attributable to the *regulatory implementation of* CCPA (rather than the letter of the statute). The main scenario, *Proposed*, represents the expected impact on the overall California economy of this compliance. As discussed in previous sections, the direct CCPA compliance costs are subject to considerable uncertainty. We attempt to quantify the macroeconomic consequences of this uncertainty by considering three versions of the *Proposed* scenario, differing the scope of enterprise coverage. As in Table 2 above, we consider cases where 25%, 50%, or 75% of all California businesses that earn less than $25 million in revenue will be covered under than CCPA. A survey completed by the International Association Privacy Professionals (IAPP) found that 8 out of 10 surveyed businesses believed that they would need to take compliance actions as a result of the CCPA. Because the survey went only to businesses in certain sectors likely to be covered by the law, the 50-75% upper-bound compliance range is reasonably supported by empirical evidence. Results for all scenarios are presented relative to the Baseline reference scenario that assumes CCPA law and pre-existing regulations remain in place.

Table 4 shows the direct costs that are measured for this analysis for the proposed regulation and the two regulatory alternatives. Costs are shown for all three methods of measuring how many firms may need to comply with the CCPA. These costs reflect total compliance spending over the entire analysis period (2020-2030) and have not been annualized. For the less stringent regulatory alternative, costs are approximately 25%

lower than the proposed regulations, regardless of how the number of compliant firms is measured. For the more stringent alternative, costs are 34%-39% higher than the proposed regulation.

Table 4: Decadal Compliance Costs For Proposed Regulation and Regulatory Alternatives (2020-30, $ million)

	Low Firm Threshold	50% Firm Threshold	75% Firm Threshold
Proposed			**16,454**
Less Stringent	**356**	**8,353**	**12,415**
More Stringent	**626**	**15,344**	**22,819**

4.3 Inputs to the 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 CCPA compliance costs as the primary inputs for the impact assessment (see Section 1.5). These compliance costs are broken into two categories: reflecting incremental costs for labor and technology. Labor costs pertain to compliance associated with operational planning costs and other human resource needs arising from CCPA, such as training and record-keeping. These costs will raise enterprise costs for skilled labor in each sector of the model that incurs CCPA compliance obligations. Technology costs are assumed to comprise 10% of CCPA costs attributable to design and/or purchases for technological infrastructure necessary to respond to consumer requests. These costs are modeled as an increase in sectoral purchases of goods and services from the information technology sector.

Cost for a representative scenario (50% firm compliance) and a representative year (2025) are shown in Table 5. While the macroeconomic model used for this analysis has 60 economic sectors, the table aggregates these costs to 2-digit NAICS codes for simplicity of exposition. Within NAICS codes, costs were allocated to BEAR sectors based on base year shares of output.

Table 5: Macroeconomic Inputs by Sector for a Representative Year (2025) and Scenario

	Labor Cost		Tech Cost		Total Compliance Cost	
Sector						% of Output
Agriculture, Forestry, Fishing, Hunting	0.870	0.001%	1.610	0.002%	2.480	0.004%
Mining, Quarrying, Oil-Gas Extraction	0.290	0.002%	0.530	0.003%	0.820	0.005%
Utilities	0.210	0.000%	0.390	0.001%	0.600	0.001%
Construction	32.680	0.017%	60.660	0.031%	93.340	0.048%
Manufacturing	16.950	0.002%	31.290	0.004%	48.240	0.007%
Wholesale Trade	24.120	0.011%	44.550	0.021%	68.670	0.033%
Retail Trade	32.550	0.018%	60.310	0.033%	92.860	0.051%
Transportation and Warehousing	9.400	0.008%	17.310	0.015%	26.710	0.023%
Information	41.510	0.004%	76.790	0.007%	118.300	0.011%
Professional, Scientific, and Tech Serv	55.900	0.013%	103.300	0.024%	159.200	0.037%
Educational Services	5.880	0.020%	10.890	0.037%	16.770	0.057%
Health Care and Social Assistance	42.330	0.018%	78.540	0.033%	120.870	0.051%
Arts, Entertainment, and Recreation	41.200	0.024%	76.410	0.045%	117.610	0.070%
Other Services (except Public Admin)	31.340	0.013%	58.180	0.024%	89.520	0.037%

4.4 Results

For the three comparison cases in our main, *Proposed* CCPA regulatory scenario, Table 6 presents impacts on the overall California economy over the period 2020-2030. A variety of macroeconomic metrics are listed, including real Gross State Product (GSP)[7], total Full Time Equivalent state employment, gross state Output and Investment (at purchaser prices), and total Household Income. All financial indicators are discounted for inflation to a 2015 base year.

Although the magnitude of impacts varies over time and across comparison cases, the salient macroeconomic finding is that CCPA will impose small but consistently positive net costs on the economy. The simple reason for this is that CCPA compliance occasions costs for firms and other institutions that are not offset by pecuniary benefits to themselves or other California stakeholders. It must also be noted that we have made no attempt to

[7] GSP is the state-level counterpart of GDP, or the total value added of all formal sector activities in the state economy.

value the benefits to consumers of these new protections, which could be considerable and would directly offset the net costs we present here. Thus, our net cost estimates are relatively pessimistic, but even in this case, it must be emphasized that the magnitude of these costs is very small in comparison to Baseline economic activity.

It is estimated (Table 6) that by 2030, California's real GSP will be $5.6 trillion dollars, meaning the largest impact in the most inclusive scenario (75% Threshold) would be (-4.6/5600<0.1%) less than one tenth of one percent of GSP. Although the relative magnitude of adjustment costs could be substantially higher for some groups and individual enterprises, the expected net total cost of CCPA is completely negligible in relation to the economy as a whole.

Table 6: Economy-Wide Impacts of CCPA Regulations
(billion$ differences from baseline, 2015 dollars unless otherwise noted)

	$25 Million Revenue Threshold		
			2030
Real GSP	-0.070	-0.110	-0.140
Employment (1,000 FTE)	-0.180	-0.310	-0.430
Real Output	-0.070	-0.120	-0.170
Investment	-0.030	-0.030	-0.040
Household Income	-0.040	-0.060	-0.080
	50% Threshold		
			2030
Real GSP	-1.680	-2.380	-3.090
Employment (1,000 FTE)	-4.550	-7.190	-9.520
Real Output	-1.560	-2.630	-3.740
Investment	-0.590	-0.690	-0.770
Household Income	-0.890	-1.310	-1.750
	75% Threshold		
			2030
Real GSP	-2.500	-3.530	-4.600
Employment (1,000 FTE)	-6.770	-10.690	-14.150
Real Output	-2.320	-3.900	-5.560
Investment	-0.880	-1.030	-1.140
Household Income	-1.320	-1.950	-2.610

More detailed examination of the main macroeconomic scenarios reveals that impacts vary in same direction as the scope of enterprise coverage, but not in a linear way. This is because the size distribution of California firms is quite heterogeneous. The $25 million threshold qualifies only a small share of the state's enterprise population (the largest ones) for compliance. The two population share thresholds include many more and, as expected, moving compliance from 50% to 75% coverage raises aggregate adjustment costs by about half. Also intuitive is the intertemporal pattern of adjustment costs, which are basically rising with the Baseline expansion of the economy. These results indicate that aggregate impacts attributable to CCPA could not materially influence California's baseline growth dynamics. Again, however, this finding should not discount the importance of attention to adjustment needs for particular stakeholder groups such as small businesses.

5 Fiscal Impacts

An additional regulatory cost of the CCPA will come from staffing requirements needed to monitor compliance. Specifically, the DOJ has requested an additional 23 full time positions at an estimated cost of approximately $4.5M per year. The DOJ currently enforces privacy rights through its Consumer Law Unit and Privacy Unit, a small subsection of attorneys comprised of one Supervising Deputy Attorney General (SDAG) overseeing four Deputy Attorney Generals (DAG). The CCPA will create new operational challenges in the enforcement of the framework that must be addressed through additional funding and staffing. To ensure adequate enforcement the DOJ has requested the following additional positions:

- Unfair Competition Law Fund
  - $2,912,000 in FY 2019-20 and $2,808,000 in FY 2020-21 and ongoing.
  - 9 Permanent Positions
    - 1 SDAG
    - 5 DAG
    - 3 Associate Governmental Program Analyst (AGPA)
    - $250,000 annually for expert consultants
- General Fund
  - $1,827,000 in FY 2019-20 and $1,746,000 in FY 2020-21 and ongoing
  - 14 Permanent Positions
    - 3 DAG
    - 5 AGPA
    - 6 Legal Secretary
- Total Positions: 23
- Total Funding: $4,739,000 in FY 2019 – 20, $4,554,000 FY 2020 – 21 and ongoing

6 Economic Impacts of the Regulatory Alternatives

As required for major regulations, this SRIA considers two regulatory alternatives to the proposed regulation. For this analysis, the proposed scenario reflects results assuming DOF's projected growth rates for all relevant sectors.

First, a more stringent regulatory alternative considers an alternate approach to mandating a more prescriptive CCPA compliance pathway for eligible firms, by requiring more detailed training and record-keeping practices for all firms that must be compliance with CCPA. Second, a less stringent regulatory alternative would, among other things, allow limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA are conformal in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs.

6.1 More Stringent Regulatory Alternative

The economic impacts of the more stringent regulatory alternative are modeled by assuming that all CCPA-compliant firms are required to have staff dedicated to both training and record-keeping mandated in the proposed regulation for firms that handle the personal information of more than 4 million California consumers. This requirement would be an additional requirement (beyond the proposed regulations) for potentially hundreds of thousands of California businesses and would impose substantial costs.

Reasons for rejecting: DOJ rejects this regulatory alternative in order to ease the compliance burden for smaller businesses that would trigger a CCPA-compliance threshold but do not necessarily have the resources to devote additional staff to handle CCPA-related tasks. While the CCPA requires training and record-keeping, the proposed regulation does not require all firms to hire dedicated staff for this purpose. Larger firms that handle more consumer data would be subject to the stricter training and record-keeping regulations in order to ensure that they have dedicated individuals that are familiar with the CCPA and associated requirements.

6.2 Less Stringent Regulatory Alternative

The economic impacts of the less stringent regulatory alternative are modeled by assuming that a fraction of CCPA-compliant firms will not need to allocate additional resources to the technology and operational costs associated with CCPA since they can fully leverage their GDPR compliance systems. We assume that 25% of CCPA-regulated

firms would fall into this category. For these firms, training, recordkeeping, and other ongoing costs associated with the regulation are still assumed to apply.

Reasons for rejecting: DOJ rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms of how the scope of personal information is defined and the right to opt-out of the sale of personal information (which is not required in the GDPR). While GDPR-compliant firms will certainly be able to leverage much of their compliance program for CCPA, the privacy regulations and statutes are different enough that an exemption would not ensure that all consumer rights under the CCPA are properly accommodated.

6.3 Macroeconomic Impacts

Like the *Proposed* scenario results presented in Table 6, macroeconomic impacts for the Regulatory Alternatives were evaluated for the three comparison cases of enterprise inclusion. Unlike its predecessor, however, Table 7 presents results only for the year 2030. This is done for simplicity only, since the results are still monotone over time. Even though impacts are greatest in the final year, it is clear that they remain economically insignificant to California as a whole, regardless of the regulatory alternative chosen. This suggests that the merits of the choice should be institutional, reflecting the comments in Section 6.2, rather than economic. In other words, neither alternative has a compelling economic case, and thus the *Proposed* regulation is preferred.

1442A Walnut Street, Suite 108
www.bearecon.com

Table 7: Economy-Wide Impacts of Proposed Regulation and Regulatory Alternatives in 2030
(billion$ differences from baseline, 2015 dollars unless otherwise noted)

	$25 Million Revenue Threshold		
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-0.140	-0.100	-0.190
Employment (1,000 FTE)	-0.430	-0.290	-0.500
Real Output	-0.170	-0.120	-0.250
Investment	-0.040	-0.030	-0.050
Household Income	-0.080	-0.050	-0.100
	50% Threshold		
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-3.090	-2.340	-4.670
Employment (1,000 FTE)	-9.520	-7.170	-12.520
Real Output	-3.740	-2.840	-6.140
Investment	-0.770	-0.580	-1.260
Household Income	-1.750	-1.320	-2.540
	75% Threshold		
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-4.60	-3.48	-6.95
Employment (1,000 FTE)	-14.15	-10.66	-18.61
Real Output	-5.56	-4.21	-9.13
Investment	-1.14	-0.86	-1.88
Household Income	-2.61	-1.97	-3.78

7 Summary of Economic Results

Assessment of the CCPA regulation indicates that it will have consistently positive net costs for the state economy, but the magnitude of these costs is negligible from a macroeconomic perspective. Certainly, more specific stakeholder groups, individual firms, and others, can be expected to face important adjustment costs, and complementary policies regarding special adjustment needs are worthy of consideration. Having said this, however, the overall impact estimated here for CCPA, excludes valuation of many offsetting non-pecuniary benefits and is therefore relatively pessimistic. The resulting impact amounts to a tiny fraction of overall economic activity.

For a regulation of CCPA's consequence for the state and one of its leading knowledge intensive industries, the direct costs present a notable, but hardly insurmountable challenge. For most other activities across this large and highly diversified and robust economy, impacts of CCPA will be nearly imperceptible.

With respect to regulatory alternatives, this SRIA presents two leading candidates with supporting and dissenting arguments for each. The estimates presented for these alternative scenarios indicate that economic differences between the policies, like the total impacts of the *Proposed* policy, are economically insignificant to California as whole. In other words, neither alternative has a compelling economic case, and thus the *Proposed* regulation, which offers significant benefits at reasonable costs, is preferred.

8 References

A.P.C., Kotterink, B., and S. Marcus. "Data Protection Review: Impact on EU Innovation and Competitiveness". Report carried out at request of the European Parliament's Committee on Industry, Research, and Energy (ITRE). December 2012.

BEAR (2016a). "Review of Standardized Regulatory Impact Assessments to Date." Report prepared for the California Energy Commission.

BEAR (2016b). "Berkeley Energy and Resources (BEAR) Model: SRIA Baseline Forecast for the California Economy." Report prepared for the California Energy Commission.

BEAR (2016c). "Economic Assessment for SB350: Economic Analysis." Report prepared for the California Independent System Operator, Volume 8, http://bearecon.com/portfolio-item/caiso-sb350/

BEAR (2016d). "Economic Assessment for SB350: Disadvantaged Community Impacts." Report prepared for the California Independent System Operator, Volume 10, http://bearecon.com/portfolio-item/caiso-sb350/

Cave, J., Schindler, H.R., Robinson, N., Horvath, V., Castle-Clarke, S., Roosendaal,

Christensen, L., Colciago, A., Etro, F., and G. Raftert "The Impact of the Data Protection

European Commission. "Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)". Brussels, 25.1.2012.

Ferracane, M.R., Kren, J., and E.V. Marel "Do Data Policy Restrictions Improve the Productivity Performance of Firms and Industries?". European Centre for International Political Economy DTE Working Paper 01. 2019.

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

Madden, Mary and Lee Rainie. "Americans' Attitudes About Privacy, Security, and Surveillance." Pew Research Center, 2015.

Purcell, Kristen, Joanna Brenner, and Lee Rainie. "Search Engine Use 2012." Pew Research Center's Internet & American Life Project, 2015.

Regulation in the E.U." Intertic Policy Paper. Inertic 2013.

Rickman, Dan S., and R. Keith Schwer. 1995. "A Comparison of the Multipliers of

Roland-Holst, David. "Cap and Trade and Structural transition in the California Economy," Research Paper 0707121, Center for Energy, Resources, and Economic Sustainability, University of California, Berkeley, September, 2007.

S. J. Savage and D. M. Waldman. Privacy tradeoffs in smartphone applications. Economics Letters, 137:171–175, 2015.

Savage S.J., D.M. Waldman "Privacy tradeoffs in smartphone applications." Economics Letters, 137:171–175, 2015.

Scott, Mark, Laurens Cerulus, and Steven Overly (2019). "How Silicon Valley gamed Europe's privacy rules." POLITICO. https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/

Short J.E., S. Todd (2017) What's Your Data Worth? MIT Sloan Management Review, 58 (3).

Short, J.E. and S. Todd. What's Your Data Worth? MIT Sloan Management Review, 58 (3). 2017.

Steele E., Locke C, Cadman E, Freese, B. "How much is your personal data worth?" Financial Times, 2013. Available at https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R

TrustArc. "CCPA and GDPR Compliance Report," 2019. Available at https://info.trustarc.com/Web-Resource-2019-03-18-CCPA-GDPRComplianceReport_LP.html

U.S. Census Bureau. Census 2010 Supplementary Survey (C2SS). Washington, D.C.: U.S. Bureau of the Census (2015).