Comments on the California Consumer Privacy Act (CCPA)

International Center for Law & Economics

Authored By:

Kristian Stout, Associate Director
Alec Stapp, Research Fellow

ICLE | 2117 NE Oregon St. Suite 501 | Portland, OR 97232 | 503.770.0076
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Before the

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

Sacramento, CA 94244

In the Matter of the California Consumer Privacy Act (CCPA)

COMMENTS OF THE INTERNATIONAL CENTER FOR LAW & ECONOMICS

December 6, 2019

Executive Summary

We thank the Attorney General's Office ("AG's Office") for the opportunity to comment on this timely and highly relevant policy discussion. We begin our analysis of the California Consumer Privacy Act ("CCPA") with a discussion of the standardized regulatory impact assessment (SRIA) prepared for the AG's Office by Berkeley Economic Advising and Research, LLC.[1] The bottom-line cost figures from this report are staggering: $55 billion in upfront costs and $16.5 billion in additional costs over the next decade.[2] The analysis includes large benefits as well, but as we will show below, the actual costs are even higher than the SRIA estimates and the benefits fall far short of making up for those costs.

Related, the AG's Office should take note of some of the early evidence of how the EU's General Data Protection Regulation ("GDPR") is faring.[3] After its first twelve month period in force, the compliance costs were astronomical; enforcement of individual "data rights" led to unintended consequences; "privacy protection" seems to have undermined market competition; and there have been large unseen — but not unmeasurable — costs in forgone startup investment.[4]

In one example of the ultimate scale of the compliance costs, Google reportedly spent "hundreds of years of human time" in order to be compliant with GDPR.[5] Nonetheless, France still found it noncompliant, levying a $57 million fine against the company for noncompliance.[6] A report by the Internet Association of Privacy Professionals estimated that roughly 500,000 firms in the EU registered a data protection officer.[7] Data protection officers can serve more than one organization, but the number of actual officers is undoubtedly large, and at an average salary of $88,000,[8] amount to a huge ongoing cost.

Consider this in the context of the SRIA's findings. The SRIA provides a very rough estimate of affected businesses based on assumptions about revenue per employee in order to arrive at a range

---

[1] Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf [hereinafter SRIA].

[2] *Id.*

[3] See, e.g., Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, TRUTH ON THE MARKET, May 24, 2019, https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/.

[4] *Id.*

[5] Ashley Rodriguez, *Google Says It Spent "Hundreds of Years of Human Time" Complying With Europe's Privacy Rules*, QUARTZ, Sep. 26, 2018, https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/.

[6] Tony Romm, *France Fines Google Nearly $57 Million for First Major Violation of New European Privacy Regime*, WASHINGTON POST, Jan. 21, 2019, https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

[7] *Approaching One Year GDPR Anniversary, IAPP Reports Estimated 500,000 Organizations Registered DPOs in Europe*, Internet Association of Privacy Professionals, May 16, 2019, https://iapp.org/about/approaching-one-year-gdpr-anniversary-iapp-reports-estimated-500000-organizations-registered-dpos-in-europe/.

[8] *Id.*

of between 9,858 and 570,066 affected businesses.[9] Already this rough estimate exceeds the number of firms that registered data protection officers in the EU, but the SRIA further opines that "[a] lack of data prevents us from estimating with precision the number of businesses that meet the other threshold requirements in the CCPA"[10] — suggesting that the actual compliance costs of all affected firms could be significantly higher. And this is just for firms within California, leaving aside the compliance costs to extraterritorial firms that reach the statutory thresholds for California customers or users.

Implementation of GDPR also led to a host of unintended consequences. Although GDPR was designed to reign in the power of large ad-tech companies, like Google and Facebook, it perversely resulted in smaller vendors suffering more harm than the large companies.[11] Venture funding also appears to have taken a hit, with a "17.6% reduction in the number of weekly venture deals, and a 39.6% decrease in the amount raised in an average deal following the rollout of GDPR."[12] And it is the latter sort of unintended consequence that should be most troubling to regulators, as all too often there do not even exist proxies like VC funding by which to judge the pro-social behavior (like starting new companies) that laws like GDPR and the CCPA silently deter.

Finally, despite the DC Circuit trimming the FCC's 2018 Restoring Internet Freedom Order ("RIF Order"),[13] the fact remains that the FCC still retains a conflict-preemption authority to specifically preempt state laws that are incompatible with its regulations.[14] To wit,

> Conflict preemption applies to "state law that under the circumstances of the particular case stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that 'obstacle' goes by the name of conflicting; contrary to; repugnance; difference; irreconcilability; inconsistency; violation; curtailment; interference, or the like."[15]

The DC Circuit only limited the FCC's ability to *generally* preempt all potentially conflicting state laws, requiring that each preemption be challenged in a fact-intensive inquiry.[16]

---

[9] *See* SRIA, *supra*, note 1, pp. 20-21 and Table 2.

[10] *Id.* at 20.

[11] *See, e.g.*, Greg Ip, *Beware the Big Tech Backlash*, WALL STREET JOURNAL, Dec. 19, 2018, https://www.wsj.com/articles/beware-the-big-tech-backlash-11545227197.; *see also* Jessica Davies, *'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers*, DIGIDAY, June 4, 2018, https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

[12] Jian Jia, Ginger Zhe Jin, and Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. 25248 (2018) *available at* https://www.nber.org/papers/w25248

[13] Mozilla Corp. v. Fed. Commc'ns Comm'n, 940 F.3d 1, 18 (D.C. Cir. 2019).

[14] *Id.* at 81.

[15] *Id.*

[16] *Id.*

Similarly, it is also possible that the broad extent of the CCPA's rules, and their impositions on firms outside of California's borders could lead to Dormant Commerce Clause challenges.[17] Activities that "inherently require a uniform system of regulation" or that "impair the free flow of materials and products across state borders" violate the Dormant Commerce Clause.[18] As the FCC noted in its RIF Order, Internet-based communications is such a type of activity.[19]

Recommendations

The AG's Office should take great care in implementing the CCPA as both the known and the unknown costs are very large, and the law, if incorrectly implemented, will be subject to serious federal challenge. There are a handful of modifications that we believe may help navigate these shoals. Each suggestion is discussed in more depth, *infra*.

1- Clarify the definition of "personal information" so that it is not overinclusive of incidental information and also does not allow third-parties to claim rights over others' data;
2- Stress that the "valuation" of data is a difficult exercise, and the requirements to value data when offering different tiers of service shall be interpreted liberally;
3- Clarify that the definition of a "business" does not mean that *any* firm that "receives for the business's commercial purposes" an individual's personal information includes firms that merely "receive" information on consumers as a normal part of operations. For example, a website that logs a user's behavior through its site "receives" location, IP Address, and other information about that user, but *should not* be included in such a broad definition;
4- Delay implementation until there is a broadly available means of ensuring that firms can reliably ascertain the validity of user data requests (i.e. that, as is happening under the GDPR, third-parties are not able to obtain information on the customers of firms by representing themselves as those customers); and
5- Use the authority granted by the CCPA to establish a necessary exception in order to comply with applicable federal law to temporarily delay implementation until (1) it is determined that the law does not violate the Dormant Commerce Clause, and (2) the AG's Office has the opportunity to consult with the FCC and ensure that the CCPA is not subject to conflict-preemption in light of the FCC's authority over Internet communications.

---

[17] *See, e.g.,* Jennifer Huddleston and Ian Adams, P*otential Constitutional Conflicts in State and Local Data Privacy Regulations*, Regulatory Transparency Project (2019) *available at* https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf ; *see also* Graham Owens, Fede*ral Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail*, TechFreedom (2018) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216665. Better cite: https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf

[18] Ark. Elect. Co-op. Corp. v. Arkansas Pub. Serv. Comm'n, 461 U.S. 375, 384 (1984).

[19] *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, FCC 17-166 (Jan. 4, 2018) *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf [hereinafter RIF Order].

I. The SRIA analysis shows costs exceeding benefits

To start, there is a lot of uncertainty in estimating the benefits of privacy regulations to consumers, as well as the costs of compliance. Among other things, no one actually knows how many businesses the CCPA will cover, even though it will go into effect in less than a month. Indeed, the SRIA estimates that somewhere between 9,858 and 570,066 California businesses will be covered by the new law.[20] That is, to say the least, quite a margin of error. Such uncertainty inevitably chills business activity and can even pose rule of law issues (e.g., a conscientious entrepreneur may reasonably believe their business falls outside the scope of the CCPA when in fact it does not).

As Daniel Castro and Alan McQuinn point out, these higher estimates arise because, in addition to gross annual revenue thresholds, "businesses with websites that receive traffic from an average of 137 unique Californian IP addresses per day could be subject to the new rules."[21] Even the Notice of Proposed Rulemaking Action ("NPRMA") in this matter demonstrates the ambiguity in the law. In its summary of the law, the NPRMA describes one of the categories of businesses subject to CCPA requirements as those that **"[b]uy[], receive[], or sell[]** the personal information of 50,000 or more consumers, households, or devices[.]"[22] And, according to the text of the law, the statute applies to any firm that

> Alone or in combination, annually **buys, receives** for the business's commercial purposes, **sells**, **or shares** for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.[23]

Yet, later in the NPRMA, the same class of businesses is described as "businesses that **buy, sell, or share** the personal information of more than 50,000 consumers, households, or devices per year[.]"[24]

It may seem a minor distinction, but the difference between a business that merely "receives" consumer information and one that "buys," "sells," or "shares" consumer information is *very* different and goes back to Castro and McQuinn's point. A website that passively logs information on all of its visitors for completely innocuous purposes certainly "receives" information on consumers. But this is very different than a website that actively scrapes user information, purchases it for integration with data sets, or sells large amounts of consumer data as part of its regular course of business. Yet, under the highly ambiguous definitions in the law, these behaviors are treated equally.

---

[20] *SRIA, supra,* note 1 at 22.

[21] Daniel Castro and Alan McQuinn, *Comments on the California Consumer Privacy Act, Assembly Bill 375, Rulemaking Process*, Information Technology & Innovation Foundation 4, Mar. 8, 2019, *available at* http://www2.itif.org/2019-comments-ccpa.pdf

[22] Notice of Proposed Rulemaking Action, California Department of Justice, 3 (Oct. 11, 2019) *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf (emphasis added) [hereinafter NPRMA].

[23] California Consumer Privacy Act, California Civil Code § 1798.140(c)(1)(B).

[24] *Id.* (emphasis added)

Notably, the SRIA uses the conservative, low end of its range for its "baseline" estimates. But the report also includes estimates for scenarios in which up to thirty times more companies are covered than in the conservative baseline. For reference, according to a survey by the International Association of Privacy Professionals ("IAPP"), 79 percent of respondents believe their employer must comply with the CCPA, so the higher end of the range is likely closer to reality than the lower end.[25] Also, it must be noted, the report looks at only the incremental effects of the CCPA. So, all of these costs are in addition to — not in lieu of — the costs companies already incur to comply with privacy rules.

A. Direct Costs

According to the SRIA, the CCPA will impose on California businesses approximately $55 billion in initial compliance costs, or 1.8 percent of California's 2018 Gross State Product (GSP):

> Assume that smaller firms (<20 employees) will incur $50,000 in initial costs (the median of the lowest cost category), 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.[26]

In addition, the CCPA will impose on California businesses up to another $16.45 billion in costs over the next decade, as this table from the SRIA shows:

[25] *Ready or Not, Here It Comes: How Prepared are Organizations for The California Consumer Privacy Act?*, Internet Association of Privacy Professionals, 8 (2019) *available at* https://www.onetrust.com/wp-content/uploads/2019/04/onetrust-iapp_ccpa-benchmarking-report.pdf.

[26] SRIA, *supra*, note 1 at 11.

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

While these cost estimates are indeed significant, there remains one major problem with the SRIA analysis. As the report itself notes, none of these estimates includes the costs incurred by the hundreds of thousands of companies outside of California to which the regulation applies:

> 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.[27]

Interestingly, an independent analysis by IAPP estimated that 507,280 businesses (including those outside of California) would be liable under the CCPA — about the same as the report's high-end, California-only number.[28] The reality is likely higher given IAPP's conservative calculations. And, of course, neither of these estimates counts non-US firms. Most importantly, the foregoing includes only *direct* costs; there are large *indirect* costs as well that need to be taken into account.

---

[27] *Id.* at 21.

[28] Rita Heimes and Sam Pfeifle, *New California Privacy Law to Affect More Than Half A Million US Companies*, Internet Association of Privacy Professionals, Jul. 2, 2018, *available at* https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/

B. Indirect Costs

The SRIA points to GDPR compliance for reference, noting that, in addition to a substantial increase in IT budgets, the GDPR has also likely led to reduced productivity:

> 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).[29]

The report provides some estimates of the CCPA's likely macroeconomic effects but dismisses them as "completely negligible in relation to the economy as a whole."[30] But are they really negligible? Here is the relevant table from the SRIA:[31]

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

This table shows that, over the next ten years, the CCPA could result in a loss of $4.6 billion in gross state product (GSP), 14,000 jobs, and $9.3 billion in output, investment, and income. Given California's size, these estimates are small on a relative basis but large on an absolute basis. And, in

[29] SRIA, *supra*, note 1 at 12.

[30] *Id.* at 39.

[31] *Id.*

comparison to the low value consumers place on privacy,[32] the costs to productivity and employment are unacceptably high.

The SRIA also does not count the higher costs of advertising and lost advertising revenue. A compelling estimate by Catherine Tucker, a professor of marketing at the Massachusetts Institute of Technology, and Avi Goldfarb, a professor of marketing at the University of Toronto — based on their research on the effects of EU privacy regulations on advertising effectiveness — suggests this cost is also well into the billions of dollars:[33]

> [S]eeing one plain banner ad increases purchase intent by 2.63 percent-age points. The introduction of privacy laws in the EU was associated with a decrease in this effectiveness of 1.71 percentage points, or around 65%. **Therefore, for an advertiser to achieve the same lift in likely intent as they did prior to the law, they would have to buy 2.85 times as much advertising.**
>
> Currently in the United States, $8 billion is spent per year on the type of display-related advertising that we study (Interactive Advertising Bureau (IAB) 2010). If prices and demand of advertising did not change, that would mean that advertisers would have to spend $14.8 billion more than they are currently doing to achieve the same increase in purchase intent after the introduction of privacy regulation.[34]

This is a positive result for the incumbent advertising platforms, which have the resources necessary for compliance and the direct relationship with end users necessary to secure consent. As Antonio García Martínez wrote recently,

> Facebook and Google ultimately are not constrained as much by regulation as by users. **The first-party relationship with users that allows these companies relative freedom under privacy laws comes with the burden of keeping those users engaged and returning to the app**, despite privacy concerns.[35]

The benefits to dominant advertising platforms come at a high cost to consumers and advertisers. Moreover, this kind of differential impact is anathema to the goals of public policy. Regulatory benefits accruing to particular firms — at the expense of consumers — are anti-competitive in nature and

---

[32] See discussion, *infra*, at notes 45 –55 and accompanying text; *see also* Will Rinehart, H*earing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation*, American Action Forum, Oct. 24, 2019, *available at* https://www.americanactionforum.org/testimony/hearing-on-data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation/

[33] N.B., further data is needed to reach a more precise estimate.

[34] Avi Goldfarb and Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 1 MANAGEMENT SCIENCE 57, 68, *available at* https://pdfs.semanticscholar.org/41dd/8ae2799fbeaa00d3e0af3a16d994a2dcd928.pdf (emphasis added)

[35] Antonio García Martínez, *Why California's Privacy Law Won't Hurt Facebook or Google*, WIRED, Aug. 31, 2018, https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/ (emphasis added)

can become self-reinforcing, biasing market competition in favor of incumbents and against new entrants.

C. Benefits

First, researchers still debate the degree to which consumers actually value privacy, so assessing the benefits under the CCPA is difficult. The bulk of the empirical research on the economics of privacy shows that, while consumers' privacy valuations are highly context-dependent, they tend to be extremely low and often pale in comparison to other considerations such as cost and convenience.[36]

Furthermore, the measurement problems with this endeavor are significant, with the SRIA even acknowledging the extreme uncertainty of any estimates of the regulation's benefits. Nevertheless, it offers a couple of possible measures for benefits: $1.6 to $5.4 billion based on consumers' willingness to pay ("WTP") for more app privacy; $169 million based on the implied value of firms' WTP for consumers' basic information; $9.7 billion based on the implied value of firms' WTP for more-sensitive information; and $12 billion based on the average revenue per user ("ARPU") of personal information used for advertising in California.

Despite the report's assumption to the contrary, other than the first of these, none of these metrics estimates the value *to consumers* of increased privacy regulation. Rather, they estimate the value *to firms* of the underlying data. In no sense does the CCPA somehow transfer this value to consumers. Some of the CCPA's costliest rules require disclosure, but this does not inherently preserve value. It might trigger additional expense to claw data back, but it does not simply confer its value on consumers.

Indeed, much of the value of this data — and presumably all of its value to businesses — arises from its use by businesses. Therefore, keeping it out of firms' hands does not transfer that value to consumers — it *destroys* that value. The CCPA's opt-out rules will impede firms' ability to offer targeted ads and publishers' ability to finance content with advertising. This limitation will likely lead to significant consumer costs, including higher product prices, less information flow, and subscription fees.[37]

All of these issues are ignored by the SRIA.

Based on the report's one arguably valid measure of the regulation's benefits (i.e., consumer WTP for more privacy), the CCPA would confer between $1.6 to $5.4 billion per year in benefits at a cost — including both annualized up-front costs and ongoing costs over ten years — of $7.2 billion per year. Even ignoring the problems with these estimates, this is a poor outcome for California consumers.

---

[36] *See, infra*, at notes 38– 55 and accompanying text.

[37] *See generally* Avi Goldfarb and Catherine E. Tucker, *supra*, note 34.

II. The economics of valuing user data

Under § 1798.125, businesses are permitted to discriminate between consumers that allow data collection and those who choose to opt-out.[38] There is an important proviso, however. Nothing in the CCPA, "prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, **if that difference is reasonably related to the value provided to the consumer by the consumer's data.**"[39]

The manner in which the AG's Office plans to interpret this rule is potentially problematic and requires careful consideration of the economics of user data. The AG's Office proposes to require the following pursuant to § 1798.125:

> To estimate the value of the consumer's data, a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall use one or more of the following:
>
> (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
>
> (2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
>
> (3) Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value;
>
> (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information;
>
> (5) Expenses related to the sale, collection, or retention of consumers' personal information;
>
> (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;
>
> (7) Profit generated by the business from sale, collection, or retention of consumers' personal information; and
>
> (8) Any other practical and reliable method of calculation used in good-faith.[40]

[38] California Civil Code 1798.125 (a)(2).

[39] *Id.* (emphasis added).

[40] Proposed California Consumer Privacy Act Regulations § 999.337. Calculating the Value of Consumer Data, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

There are, broadly speaking, two classes of "calculation" this rule contemplates: one performed by firms that explicitly traffic in data as a commodity (e.g. data brokers, and, possibly, some advertising networks) on the one hand, and firms that otherwise use data as part of their operations (everyone else).

A. Valuing data for data brokers and ad networks

Data as a commodity is worth very little — so little it is potentially onerous to generally require firms to maintain an accounting of it. Moreover, it is very difficult to actually put a price on data.[41] When data brokers and other intermediaries in the digital economy do try to value data, the prices are almost uniformly low. For example, according to the Financial Times,

> [g]eneral information about a person, such as their age, gender and location is worth a mere $0.0005 per person, or $0.50 per 1,000 people. A person who is shopping for a car, a financial product or a vacation is more valuable to companies eager to pitch those goods. Auto buyers, for instance, are worth about $0.0021 a pop, or $2.11 per 1,000 people… Knowing that a woman is expecting a baby and is in her second trimester of pregnancy, for instance, sends the price tag for that information about her to $0.11… For $0.26 per person, buyers can access lists of people with specific health conditions or taking certain prescriptions… [T]he sum total for most individuals often is less than a dollar.[42]

The reason for these low valuations is because data is a specific asset, meaning it has "a significantly higher value within a particular transacting relationship than outside the relationship."[43] Data only appears valuable because the firms that *use* the data are so valuable. In reality, it is the combination of high-skilled labor, large capital expenditures, and cutting-edge technologies (e.g., machine learning) that makes those companies so valuable.[44] Yes, data is an important component of these production functions. But, in reality, it makes little sense to claim that the data possessed by firms have little, if any, independent value.

Thus, where data itself is a commodity the price is close to zero.

---

[41] Will Rinehart, *How Do You Value Data? A Reply To Jaron Lanier's Op-Ed In The NYT*, THE TECHNOLOGY LIBERATION FRONT, Sep. 23, 2019, https://techliberation.com/2019/09/23/how-do-you-value-data-a-reply-to-jaron-laniers-op-ed-in-the-nyt/.

[42] Emily Steel, *Financial worth of data comes in at under a penny a piece*, FINANCIAL TIMES, June 12, 2013, https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de

[43] Benjamin Klein, *Asset Specificity and Holdups* in THE ELGAR COMPANION TO TRANSACTION COST ECONOMICS (Peter G. Klein & Michael E. Sykuta, eds.) *available at* http://masonlec.org/site/files/2012/05/WrightBaye_klein-b-asset-specificity-and-holdups.pdf

[44] *See, e.g.,* Dan Gallagher, *Data Really Is the New Oil*, WALL STREET JOURNAL, Mar. 9, 2019, https://www.wsj.com/articles/data-really-is-the-new-oil-11552136401

B. Valuing data for general firms

Although the proposed allowance for "[a]ny other practical and reliable method of calculation used in good-faith"[45] allows the AG's Office a degree of latitude when confronted with the inevitably vast differences across use cases for data that will surely arise, even such an extremely liberal *potential* allowance will do little to mitigate the chilling effect that this regulation will impose on general firms.

When data, as noted above, either eludes valuation or is practically worthless in isolation, firms face a stark choice: collect only the minimum data required to operate in an effort to comply with the CCPA, or take a legal risk by collecting more than is strictly necessary where that data *might* be useful to later innovations developed by the firm.

If the problem is framed strictly from the perspective of maximizing a social value of privacy, this may not sound like a problem at all. But, of course, the real world is not so simple. "Privacy" is only *one* value in a network of competing values that are implicated by technology and the use of data.

To begin with, there are clear benefits to information sharing that must be taken into account. Since the dawn of the Internet, free digital services have created significant consumer surplus and this trend continues today: Recent research using both survey and experimental methodologies has consistently found substantial benefits for consumers from sharing information in exchange for free (or subsidized) digital products.

Allcott et al., for example, studied the price that Facebook users were willing to accept in order to abstain from using the service for four weeks.[46] In the study, the median willingness-to-accept ("WTA") from participants was $100.[47] The WTA estimate means that "[a]ggregated across an estimated 172 million US Facebook users, the mean valuation implies that four weeks of Facebook generates $31 billion in consumer surplus in the US alone."[48]

Corrigan et al. reported similar results of "a series of three non-hypothetical auction experiments where winners are paid to deactivate their Facebook accounts for up to one year."[49] In their conclusion, the researchers said, "Though the populations sampled and the auction design differ across the experiments, we consistently find the average Facebook user would require more than $1,000 to deactivate their account for one year."[50]

Brynjolfsson et al. reviewed the benefits of "several empirical examples [of technology that implicates privacy concerns] including Facebook and smartphone cameras" and then "estimate[d] their valuations

---

[45] Proposed California Consumer Privacy Act Regulations § 999.337(b)(8).

[46] Hunt Allcott, Luca Braghieri, Sarah Eichmeyer, and Matthew Gentzkow, *The Welfare Effects of Social Media*, NBER Working Paper No. 25514 (2019).

[47] *Id.* at 5. Note, this was not just cheap talk—the study followed through and paid a randomly-selected portion of the users to deactivate their accounts for four weeks. *Id.*

[48] *Id.*

[49] Jay R. Corrigan et al., H*ow much is social media worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (2018).

[50] *Id.*

through incentive-compatible choice experiments."[51] The study found considerable benefits that are currently excluded from national accounts: "For example, including the welfare gains from Facebook would have added between 0.05 and 0.11 percentage points to GDP-B growth per year in the US."[52]

In a literature review of the economics of privacy, Acquisti et al. concluded that:

> Extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: the optimal balancing of privacy and disclosure is very much context-dependent, and it changes from scenario to scenario.[53]

Moreover, what we think of as privacy is actually an umbrella covering many related concepts, each with their own separate complicating factors.[54] As some economists have aptly pointed out:

> If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing.[55]

With this in mind, digital privacy regulations can have important unintended consequences that could significantly harm consumer welfare in the long run. These include misunderstanding consumer preferences, requiring excessive data protection, mandating business models, imposing compliance costs that potentially exceed benefits of those regulations, crowding out superior privacy offerings stemming from the private sector, and protecting some companies' market power.

Further, it's important to underscore that, even in the face of all the potential innovation that can come from new uses of data, it is typically out of the reach of firms to be able to actually place a value on any piece of data. The studies noted above refers to a WTA as expressed by *consumers*. The asymmetry of the relationship between consumers and providers means that providers generally will not have access to any particular user's WTA.

But more to the point, as noted above, it is the combination of the business's processes with data that enable it to generate value, and that revenue generation will not be even across all users' data. Some data will end up being more valuable in a given business process, and other data valuable in a different context. Thus, the actual value of the data won't actually emerge until the data is employed.

---

[51] Erik Brynjolfsson et al., *GDP-B: Accounting for the Value of New and Free Goods in the Digital Economy*, NBER Working Paper No. 25695 (2019).

[52] *Id.*

[53] Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 52(2) J. ECON. LIT. 48 (2016) (emphasis added).

[54] Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 443 (2016).

[55] *Id.* at 462.

The implications for the present regulation are complicated. In some cases, firms will be able to produce outputs with data inputs that are very valuable, and in other cases the data will never end up being valuable at all. Thus, in order to anticipate *potential* value that *might* be realized, a firm faces two choices. First, it can report average revenue per user, and smooth the differences in revenue generation over its entire user base where it expects large outliers (extremely high value and extremely low value users) to be rare. Second, if it anticipates that a small group of users will end up generating a large amount of its revenue, it has a reasonable incentive to report a very large "valuation" of every piece of data, despite the fact that *most* of its users' data will be nearly worthless.

The choice is essentially arbitrary from the firm's perspective and doesn't actually provide real information about a particular user's data. Nonetheless, regulators should be careful not to read too much into the numbers, and likely, should treat an extremely wide range of potential valuations as having been reasonably made in "good faith."

III. Recommendations

We offer the following suggestions as points where implementation of the CCPA could be improved.

A. Modify the definition of "personal information"

Under the CCPA protected "personal information"

> means information that identifies, relates to, describes, **is capable of being associated with, or could reasonably be linked, directly or indirectly**, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[.][56]

As Professor Goldman has observed, under this definition "what doesn't qualify as personal information in the CCPA?"[57] Outside of one narrow exception for information provided publicly by the government, essentially *all* information remotely related to an individual qualifies as "personal information" because every such piece of information is "capable of being associated with, or could reasonably be linked" with that individual.

Moreover, since the definition of "personal information" includes both information about an individual as well as information about his or her household, conflicts in how to apply the law are inevitable. Different individuals in a single household do not always (or usually) have strictly aligned interests.[58] Therefore, the AG's Office needs to carefully consider how to avoid allowing one member of a household to access or modify the private information of other members of the household.

---

[56] California Civil Code § 1798.140(o) (1) (emphasis added).

[57] Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, Santa Clara Univ. Legal Studies Research Paper 3 (2019) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013

[58] *Id.* ("These people's interests may diverge, such as with separating spouses, multiple generations under the same roof, and roommates").

In order to avoid overinclusive enforcement, as well as data breaches and privacy invasions by members of households against each other, the definition of "personal information" needs to be interpreted more narrowly.

If the definition is to have a reasonable meaning, it cannot be interpreted to mean *any* information at all that could remotely be used to identify an individual. For example, entries of user activity in various web site logs, and other observational data about the behavior of website users should not be interpreted as "personal information." At the same time, the AG's Office should clarify that different members of households do *not* have access or modification rights to the information of *other* members of the household. Further, and related to the broader point about over-inclusivity, a household member's web activity that generates observations about, for instance, the behavior of certain IP Addresses should not be treated as the "personal information" of all members of the household.

B. Liberally interpret the "value" of data

As noted above, placing a realistic estimate of value on any particular piece of data is a fraught exercise. In proposed regulation 999.337 ("Calculating the Value of Consumer Data") the AG's Office should include an acknowledgement that any estimates provided will be understandably imprecise. Further, given the highly imprecise nature of performing such calculations, the AG's Office should emphasize that it will interpret "good faith" compliance liberally.

C. Clarify the definition of "business"

The difference between a business that merely "receives" consumer information and one that "buys," "sells," or "shares" consumer information is large. Further, even the ostensibly large threshold of "50,000 or more consumers" is trivial to reach under the existing interpretations. Any service that passively recorded information on at least 137 residents of California per day becomes subject to the law. There should be a meaningful distinction between firms that buy and sell information as a commodity, and those that merely collect information about user behavior as an aspect of their business.

Therefore, the AG's Office should clarify that § 1798.140(c)(1)(B) does not mean that any firm that "receives for the business's commercial purposes" an individual's personal information includes firms that merely "receive" information on consumers as a normal part of operations. For example, a service that logs a user's behavior through a site "receives" location, IP Address, and other information about that user, but should not be included in such a broad definition.

D. Ensure there exists reliable user verification methods

In order to work properly, the CCPA depends on the AG's Office requiring that firms use systems that can validate "verifiable consumer requests."[59] A "verifiable consumer request" is defined as

> a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify... to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer... if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General... that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.[60]

This is a critical piece of the law. If the verification procedures are not carefully designed, the CCPA transforms from a law designed to protect privacy into a law that facilitates identity theft, hacking, and fraud. And, particularly given the very broad definition of "personal information" noted above, businesses will have a difficult time verifying many consumer requests without requiring consumers to disclose *more* information about themselves to the firms.

For example, if the broad definition of a business that merely "receives" information remains as-is, and the broad definition of "personal information" similarly remains, websites with little or no direct relationship with a given individual have no internal means for validating a particular consumer's request. Faced with this dilemma, businesses either need to require that consumer to provide extensive enough documentation to allow validation — thus paradoxically requiring consumers to expose *even more* sensitive information to discover if any information on them exists at all — or the businesses need to err on the side of disclosure. But erring on the side of disclosure introduces the risk of leaking information to malicious third parties.

This is a very real concern. In the wake of GDPR, faced with ambiguity around validating users requesting data, some firms have been shown to improperly provide information on their users. In one highly publicized incident, a security researcher set about to find out how much of his fiancée's information he could fraudulently obtain using GDPR requests.[61] Although large tech companies tended to field his requests as expected, mid-sized businesses with less resources to handle GDPR requests performed poorly.[62] Ultimately, out of 83 firms that the researcher attempted to exploit:

---

[59] *See* California Civil Code § 1798.100(c).

[60] California Civil Code § 1798.140(y).

[61] Leo Kelion, *Black Hat: GDPR Privacy Law Exploited to Reveal Personal Data*, BBC NEWS, Aug. 8, 2019, https://www.bbc.com/news/technology-49252501

[62] *Id.*

- 24% supplied personal information without verifying the requester's identity
- 16% requested an easily forged type of ID that he did not provide
- 39% asked for a "strong" type of ID
- 5% said they had no data to share, even though the fiancée had an account controlled by them
- 3% misinterpreted the request and said they had deleted all her data
- 13% ignored the request altogether[63]

California would be well advised to avoid exposing the information of its citizens to similar data security risks. The AG's Office should therefore delay implementation of the CCPA until such time as it can verify that there are adequate, widely available means for firms of all sizes to validate consumer information requests. At the same time, it would be advisable to seek amendments from the California legislature that create better guidelines around how such verification procedures should work given the troubling evidence emerging from the EU around its similar privacy program.

E. Delay implementation until jurisdictional boundaries are clear

Finally, despite the DC Circuit trimming the FCC's 2018 Restoring Internet Freedom Order,[64] the fact remains that the FCC still retains a conflict-preemption authority to specifically preempt state laws that are incompatible with its regulations.[65] To wit,

> Conflict preemption applies to "state law that under the circumstances of the particular case stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that 'obstacle' goes by the name of conflicting; contrary to; repugnance; difference; irreconcilability; inconsistency; violation; curtailment; interference, or the like."

The DC Circuit only limited the FCC's ability to *generally* preempt potentially conflicting state laws, requiring that each preemption be challenged in a fact-intensive inquiry.[66]

Similarly, it is also possible that the broad extent of the CCPA's rules, and their impositions on firms outside of California's borders could lead to Dormant Commerce Clause challenges.[67] Activities that "inherently require a uniform system of regulation" or that "impair the free flow of materials

---

[63] *Id.*

[64] Mozilla Corp. v. Fed. Commc'ns Comm'n, *supra*, note 13.

[65] *Id.* at 81.

[66] *Id.*

[67] *See, e.g.*, Graham Owens, *supra*, note 17.

and products across state borders" violate the Dormant Commerce Clause.[68] As the FCC noted in its Restoring Internet Freedom Order, Internet-based communications is such a type of activity.[69]

Therefore, the AG's Office should consider using its authority to "[e]stablish[] any exceptions necessary to comply with state or federal law"[70] to temporarily delay implementation of the CCPA until latent federal preemption issues can be resolved. In particular, the AG's Office should determine that (1) the contemplated implementation of the CCPA does not violate the Dormant Commerce Clause and (2) the AG's Office has the opportunity to consult with the FCC and ensure that the implementation of the CCPA is not subject to conflict-preemption in light of the authority of the FCC's over Internet communications.

On a related note, the AG's Office should also consider harmonizing implementation of the law with other broadly applicable privacy laws, even where not legally compelled to do so. With the current structure of the CCPA, for example, businesses are not able to recycle their GDPR compliance programs.[71] If there must be a state level data protection law, then it would be desirable to harmonize it with existing regulations elsewhere (in a manner that is less — not more — restrictive) in order to promote efficiency and clarity for consumers.

IV. Conclusion

Attached is a comment our center submitted to the National Telecommunications and Information Administration on the subject of developing a regulatory approach to privacy. The comment goes into the law and economics of privacy regulation in depth, but some high-level thoughts are appropriate to note here as the AG's Office considers its implementation of the CCPA.

Although the US does not have a single, omnibus privacy regulation, this does not mean that the US does not have "privacy law." In the US, there already exist generally applicable laws at both the federal and California level[72] that provide a wide scope of protection for individuals, including consumer protection laws that apply to companies' data use and security practices, as well as those that have been developed in common law (property, contract, and tort) and criminal codes.

---

[68] Ark. Elect. Co-op. Corp. v. Arkansas Pub. Serv. Comm'n, 461 U.S. 375, 384 (1984).

[69] RIF Order, *supra,* note 19, ¶ 200.

[70] California Civil Code § 1798.185(3)

[71] Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, Internet Association of Privacy Professionals, Jul. 2, 2018, https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/

[72] *See, e.g.,* California Civil Code § 1798 et seq. (California data breach law).

In addition, there are specific regulations pertaining to certain kinds of information, such as medical records,[73] personal information collected online from children,[74] credit reporting,[75] as well as the use of data in a manner that might lead to certain kinds of illegal discrimination.[76]

Getting regulation right is always difficult, but it is all the more so when confronting evolving technology, inconsistent and varied consumer demand, and intertwined economic effects — all conditions that confront online privacy regulation. Given this complexity, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Federal Trade Commission has historically taken: case-by-case examination of actual privacy harms, without ex ante regulations, coupled with narrow legislation targeted at problematic uses of personal information.

Many (if not most) services on the Internet are offered on the basis that user data can, within certain limits, be used by a firm to enhance its services and support its business model, thereby generating benefits to users. To varying degrees (and with varying degrees of granularity), services offer consumers the opportunity to opt-out of this consent to the use of their data, although in some cases the only way effectively to opt-out is to refrain from using a service at all.

U.S. privacy regulators have generally evidenced admirable restraint and assessed the relevant tradeoffs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of ex ante privacy principles across industries is a fraught exercise as each firm faces a different set of consumer expectations about its provision of innovative services, including privacy protections.

This does not mean that privacy regulation should never be debated, nor that a more prescriptive regime should never be considered. But any such efforts must begin with the collective wisdom of the agencies, scholars, and policy makers that have been operating in this space for decades, and with a deep understanding of the business realities and consumer welfare effects involved.

Thank you again for the opportunity to comment on these timely and important topics.

---

[73] *See, e.g.,* The Health Information Portability and Accountability Act ("HIPAA"), 45 CFR Parts 160 and 164.

[74] *See, e.g.,* Children's Online Privacy Protection Act ("COPPA"), 16 CFR Part 312.

[75] *See, e.g.,* Gramm–Leach–Bliley Act, 15 USC § 6801.

[76] *See. e.g.,* Civil Rights Act of 1968, Title VIII ("Fair Housing Act"), 42 U.S.C. 3601, et seq.