ICLE International Center for Law & Economics

Comments on the California Consumer Privacy Act (CCPA)
December 6, 2019
Kristian Stout and Alec Stapp

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. 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. The analysis includes large benefits as well, but as we show in the full comments, the actual costs are even higher than the SRIA estimates and the benefits fall far short of making up for those costs.

We also draw on the the early evidence coming out of the EU related to GDPR enforcement and compliance to highlight some potential pitfalls that California is facing. In particular, after its first twelve month period in force, the compliance costs were astronomical; enforcement of individual "data rights" led to unintended con- sequences; "privacy protection" seems to have undermined market competition; and there have been large unseen — but not unmeasurable — costs in forgone startup investment.

Finally, we note that, despite the DC Circuit trimming the FCC's 2018 Restoring Internet Freedom Order, the fact remains that the FCC still retains a conflict-preemption authority to specifically preempt state laws that are incompatible with its regulations. 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. 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. 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. As the FCC noted in its RIF Order, Internet-based communications is such a type of activity.

We therefore offered the following suggestions:

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.

Continue reading the full comments

View Article