THE FREE STATE FOUNDATION
A Free Market Think Tank for Maryland.....Because Ideas Matter

Perspectives from FSF Scholars
October 28, 2019
Vol. 14, No. 35

California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption

By

Andrew Long *

I. Introduction and Summary

The California Consumer Privacy Act of 2018, the state's ambitious attempt to redefine radically how consumer privacy oversight is conducted in the United States, officially goes into effect in just a few months. The California Attorney General recently proposed implementing rules – the final piece of this highly proscriptive regulatory regime – and could initiate enforcement proceedings as early as next July. The California law is inconsistent with sound principles of privacy regulation. It creates regulatory uncertainty, prevents privacy protections from evolving over time, imposes significant and unjustified costs, diverts resources away from uses that benefit consumers, deters investment and innovation, and threatens the continued existence of the ad-supported online experience that consumers clearly prefer.

Without question, over the last several years we have witnessed some high-profile examples of the misuse of consumer information. The Federal Trade Commission, however, has proven itself more than capable of providing an adequate enforcement response. As such, the California Consumer Privacy Act of 2018's overly intrusive, rigid, and costly approach to privacy regulation – an abrupt departure from the flexible approach that has fostered unprecedented innovation and generated substantial consumer welfare – simply cannot be justified.

The undeniable and ongoing success of the digital services marketplace confirms that there is no reason to disturb the proven principles underlying the current approach to protecting consumer privacy. They include the following:

- Government oversight should be conducted by a single agency at the federal level – not by multiple states and localities competing to establish rules of the road that transcend jurisdictional boundaries. The inherent nature of the Internet is national – indeed, international – and domestic traffic flows intrinsically are interstate. Consistent with consumer expectations, one set of regulations should apply nationwide.
- Because the digital services marketplace is highly dynamic and defined by rapid technological innovation, consumers' interests are best served by the Federal Trade Commission's flexible, case-by-case approach to violations – not by rigid, proscriptive *ex ante* rules.
- The collection and use of non-sensitive information should be governed by a general "opt-out" approach – not an "opt-in" regime or a version of "opt-out" that is riddled with "opt-in" exceptions. "Opt-in" imposes additional operational burdens and excludes from targeted advertising the information of consumers who, though willing to provide it, fail to make their preferences known – which, in turn, threatens the continued availability of the "free" services that consumers value.
- Government decisionmakers should recognize that targeted advertising produces substantial benefits for consumers – and not impose burdensome regulations that jeopardize the continued viability of the digital services marketplace. Consumers clearly value their ability to exchange information for "free" content and services, and "anti-discrimination" provisions like the one included in the California law interfere with the efficient operation of these win-win transactions.

The California Consumer Privacy Act of 2018 roundly rejects these sound principles in favor of a highly restrictive regime that inevitably will lead to consumer dissatisfaction as well as a reduction in overall consumer welfare.

The size of California's economy, combined with the central role it plays in the tech and information services sectors, ensure that the harmful effects of the California Consumer Privacy Act of 2018 will be felt far beyond its borders. Absent further revisions to address the California law's most problematic aspects, it is critical that Congress pass a preemptive new law and the Federal Trade Commission take action in order to guarantee a consistent, responsive, and exclusively federal approach to consumer privacy oversight.

II. An Overview of the Burdensome Approach to Consumer Privacy Protection Set Forth in the CCPA and the Attorney General's Proposed Implementing Rules

On June 28, 2018, then-Governor Brown signed into law the California Consumer Privacy Act of 2018 ("CCPA"),[1] which will go into effect on January 1, 2020. The CCPA is an audacious attempt to redefine how consumer privacy concerns are addressed, not just in California, but throughout the United States.[2] The law (1) creates new privacy rights for consumers, (2) imposes intensely detailed compliance obligations upon businesses, (3) authorizes the Attorney General

[1] Cal. Civ. Code §§ 1798.100 *et seq*.
[2] *See, e.g.*, Marguerite Reardon, "California's new privacy law gets teeth with proposed regulations," *CNET* (October 11, 2019), available at https://www.cnet.com/news/california-proposes-regulations-to-enforce-new-privacy-law/ (highlighting that "California's law is meant to provide protection to California residents in the absence of federal law and to push the nation to offer more consumer protections.").

to impose civil penalties for violations,[3] and (4) establishes a private right of action, albeit one that is limited by a business' right to cure.[4]

It also directs the California Attorney General to (1) adopt implementing rules, and (2) enforce its provisions. The Attorney General may not initiate any enforcement actions, however, until July 1, 2020, or six months after publication of those rules, whichever comes later. Attorney General Xavier Becerra released proposed rules on Thursday, October 10, 2019.[5] The following day, Governor Newsom signed into law seven bills amending various aspects of the CCPA.[6]

The specific consumer privacy rights created by the CCPA are as follows:

The Right to Know: Consumers have the right to obtain a broad range of information regarding the data that businesses collect, such as: the pieces of personal information the business has collected about them specifically, as well as the general categories of personal information the business has collected or sold about consumers generally; the purpose for which the business collected or sold categories of personal information; and the categories of third parties to whom the business sold that personal information. While some of this information applies to all consumers and may be provided as part of the business' privacy policy, much of it is specific to the individual and is to be provided in response to a verifiable request.

The Right to Delete: Consumers have a right to ask that their personal information be deleted, subject to certain exceptions. Businesses must verify the identity of the requesting customer to a reasonable degree of certainty tailored to the sensitivity of the specific data to be deleted. For

---

[3] *See* Cal. Civ. Code § 1798.155(b) ("A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.").

[4] *See* Cal. Civ. Code § 1798.150(b) ("In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.").

[5] Cal. Code Regs. tit. 11, § 999.300 *et. seq.* (proposed October 11, 2019), available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf (*Proposed Regulations*). Comments are due on or before December 6, 2019. *See California Department of Justice, Notice of Proposed Rulemaking Action, Title 11. Law, Division 1. Attorney General* (published October 11, 2019), at 2, available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf (*CCPA NOPA*).

[6] Gretchen A. Ramos, "Governor Newsom Signs CCPA Amendments," *LEXOLOGY* (October 14, 2019), available at https://www.lexology.com/library/detail.aspx?g=ca6fc138-19e1-43a9-b8e3-11cd4cd43e2c (summarizing how the newly adopted legislation modifies the CCPA with respect to: the rights of certain categories of consumers, including employees and job candidates; methods for consumers to submit requests to online-only businesses; notice requirements in connection with business-to-business communications; the definitions of "personal information" and "publicly available;" notices regarding the categories of information collected about consumers; the types of data breaches for which class-action lawsuits may be brought; the types of information implicated in a data breach that trigger notification requirements; the transfer of information relating to vehicle warranties and recalls; and data broker registration). California's Attorney General "has indicated that he'll be amending the draft regulations to conform with the recent amendments to the law." Linn F. Freedman, "CCPA News: Amendments Signed into Law by the Governor and Draft Regulations Released by the Attorney General," *The National Law Review* (October 14, 2019), available at https://www.natlawreview.com/article/ccpa-news-amendments-signed-law-governor-and-draft-regulations-released-attorney.

example, businesses must go to greater lengths to confirm a consumer's identity before deleting photos than before deleting browsing history.

The Right to Opt-Out of Sale: Consumers who are 16 and older have the right to opt-out of the sale of their personal information. Businesses must provide a "Do Not Sell My Personal Information" button on their websites' homepage linked to a page via which they may opt-out. By contrast, a business may sell the personal information of consumers under the age of 16 only if they opt-in. Those aged 13 to 15 may opt-in themselves, but a parent or guardian must opt-in on behalf of those under the age of 13.

The Right to Non-Discrimination: A business may not discriminate against a consumer because he or she has exercised any of these rights. Discrimination is defined broadly and "includes, but is not limited to, denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, or suggesting that the consumer will receive a different price or quality of goods or services."[7]

At the same time, however, the CCPA states that businesses in fact "may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data."[8]

Businesses, as an inevitable consequence, face a host of new compliance-related obligations under the CCPA. These include:

Consumer Notices: Businesses must provide a number of notices to consumers, including: notice, at or before the time of collection of personal information, of "the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used"[9] ("Notice at Collection"); notice that a consumer may opt-out of the sale of his or her personal information, along with the inclusion of a "Do Not Sell My Personal Information" link/button on its homepage[10] ("Notice of Right to Opt-Out of Sale of Personal Information"); and notice regarding "each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate"[11] ("Notice of Financial Incentive").

Privacy Policy: A business' privacy policy must "provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure,

[7] *CCPA NOPA* at 5, referencing Cal. Civ. Code § 1798.125(a)(1).
[8] Cal. Civ. Code § 1798.125(b)(1).
[9] *Proposed Regulations* § 999.305(a)(1).
[10] *See generally Proposed Regulations* § 999.306.
[11] *Proposed Regulations* § 999.307(a)(1).

and sale of personal information and of the rights of consumers regarding their personal information."[12] Businesses must update their privacy policies at least once every 12 months.

Business Practices for Handling Consumer Requests: The CCPA proscribes detailed procedures specifying how businesses are to receive, verify, process, respond to, and document consumer requests.[13]

Training and Recordkeeping: All businesses must (1) train employees who deal with privacy-related inquiries on consumers' rights under the CCPA, and (2) retain records relating to consumer requests for at least 24 months. In addition, businesses that interact with the personal information of four million or more consumers must (1) compile metrics on consumer requests and include that data in their privacy policies, and (2) document, and take steps to ensure compliance with, their training policies.[14]

Given the radically intrusive nature of the CCPA, it is not surprising that one goal of the implementing rules recently proposed by the Attorney General is to "attempt to provide clarity around some of the questions business have been struggling to answer."[15] Unfortunately, however, those proposed rules just exacerbate that uncertainty by imposing still more detailed obligations.

Topics addressed and/or elaborated upon include: requirements regarding the content to be included within, and the manner of presentation of, consumer notices and the privacy policy; step-by-step instructions for submitting and responding to Requests to Know, Requests to Delete, and Requests to Opt-Out; training and recordkeeping requirements, including additional obligations for businesses with access to the personal information of 4 million or more consumers; requirements for verifying a requesting consumer's identity; opt-in methods for consumers under 16 years of age; further elaboration on the CCPA's anti-discrimination provision; and specific methods for calculating the value of a consumer's personal information in connection with a financial incentive program or other differential treatment of a consumer who has exercised his or rights under the statute.[16]

III. The CCPA Violates Sound Principles of Consumer Privacy Oversight

Other Free State Foundation scholars have described the following bedrock principles that undergird an optimized approach to protecting consumer privacy. Exclusive oversight at the federal level by the Federal Trade Commission ("FTC")[17] rather than a "patchwork" of state- and

---

[12] *Proposed Regulations* § 999.308(a)(1).
[13] *See generally Proposed Regulations* §§ 999.312 – 999.332.
[14] *See generally Proposed Regulations* § 999.317.
[15] "CCPA Update: Gov. Newsom Signs Amendments into Law; Attorney General Publishes Proposed Regulations," *Duane Morris Alerts and Updates* (October 18, 2019), available at https://www.duanemorris.com/alerts/ccpa_update_newsom_signs_amendments_law_attorney_general_publishes_proposed_regulations_1019.html.
[16] *See generally Proposed Regulations* §§ 999.305 – 999.337.
[17] *See, e.g.*, Theodore R. Bolema, "The FTC Has the Authority, Expertise, and Capability to Protect Broadband Consumers," *Perspectives from FSF Scholars*, Vol. 12, No. 35 (October 19, 2017), available at https://freestatefoundation.org//wp-content/uploads/2019/05/The-FTC-Has-the-Authority-Expertise-and-Capability-to-Protect-Broadband-Consumers-101917.pdf.

local-level statutes and rules.[18] A consistent approach to all digital service providers rather than the disparate treatment of competitors based upon inapposite and outdated regulatory classifications.[19] A flexible, case-by-case approach rather than overly proscriptive and fixed *ex ante* legislation or rules.[20] The efficiency of an "opt-out" regime for non-sensitive information rather than burdensome "opt-in" requirements that reduce the amount of information available to support targeted advertising – advertising that makes possible the "free" services that consumers demand.[21] An acknowledgement that consumers value the ability to make their own informed decisions about the exchange of personal information for "free" content and services rather than unreasonable government mandates that distort the efficient operation of the digital services marketplace.[22]

The CCPA does not fare well when evaluated against this model framework.

Before turning to its deficiencies, however, I want to highlight two ways in which the CCPA does align with these objectives. First, it treats all digital service providers alike, focusing on a business' interaction with personal information rather than its classification (edge provider, Internet Service Provider ("ISP"), telephone company, cable operator, etc.).[23] Second, it at least

---

[18] *See, e.g.*, Comments of the Free State Foundation, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration Docket No. 180821780-8780-01, (submitted November 9, 2018), at 14-16, available at https://freestatefoundation.org//wp-content/uploads/2019/08/FSF-Comments-to-NTIA-—-Developing-the-Administrations-Approach-to-Consumer-Privacy-110918.pdf.

[19] *See, e.g.*, Theodore R. Bolema, "Protecting Privacy on the Internet: Key Principles for Any Reform," *Perspectives from FSF Scholars*, Vol. 14, No. 9 (April 4, 2019), available at https://freestatefoundation.org//wp-content/uploads/2019/06/Protecting-Privacy-on-the-Internet-Key-Principles-for-Any-Reform-040419.pdf.

[20] *See, e.g.*, Comments of the Free State Foundation, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration Docket No. 180821780-8780-01, (submitted November 9, 2018), at 6-7, available at https://freestatefoundation.org//wp-content/uploads/2019/08/FSF-Comments-to-NTIA-—-Developing-the-Administrations-Approach-to-Consumer-Privacy-110918.pdf.

[21] *See, e.g.*, Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017), at 3-4, available at https://freestatefoundation.org//wp-content/uploads/2019/05/The-Right-Way-to-Protect-Privacy-Throughout-the-Internet-Ecosystem-032417.pdf. "Non-sensitive information" includes web-browsing and application-usage data but excludes things like health and financial information. *See, e.g.*, Comments of the Free State Foundation, *Competition and Consumer Protection in the 21st Century – "The Intersection between Privacy, Big Data, and Competition*," Federal Trade Commission Project Number P181201, (submitted August 20, 2018), at 3, available at https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0018-151998.pdf ("With regard to personally identifiable sensitive consumer information, like financial and health records, the FTC requires an affirmative "opt-in" choice for the collection and use of such data. With regard to non-sensitive consumer information, like web browsing or application usage, the FTC's policy is to allow opt-out as the default choice for the collection and use of such data.").

[22] *See, e.g.*, Comments of the Free State Foundation, *Competition and Consumer Protection in the 21st Century* – "*The Intersection between Privacy, Big Data, and Competition*," Federal Trade Commission Project Number P181201, (submitted August 20, 2018), at 2-3, available at https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0018-151998.pdf.

[23] *See* Comments of the Free State Foundation, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration Docket No. 180821780-8780-01, (submitted November 9, 2018), at 11-12, available at https://freestatefoundation.org//wp-content/uploads/2019/08/FSF-Comments-to-NTIA-—-Developing-the-Administrations-Approach-to-Consumer-Privacy-110918.pdf.

starts from the premise that an "opt-out" regime is the appropriate method for consumers to express their informed preferences with respect to the sale of non-sensitive personal information – although, as discussed below, exceptions to this rule found in various provisions of the CCPA and the proposed implementing rules threaten to produce inefficiencies similar to those that would result under an outright "opt-in" approach.

I will now address the numerous ways in which California's efforts to regulate consumer privacy are inconsistent with the principles identified above.

A. Consumer Privacy Oversight Should Take Place at the Federal Level

Consumer privacy, and in particular online consumer privacy, is a matter that transcends state borders. It is widely acknowledged that it is impractical, if not impossible, for ISPs to distinguish between interstate and intrastate online activity given the Internet's interconnected design and national traffic flows.[24] For the same reasons, it inherently is unreasonable to ask digital service providers with national (and international) operations to abide by different sets of privacy rules depending upon a consumer's state of residency, or perhaps location, at the time he or she chooses to share personal information. Moreover, consumers expect that consistent privacy protections will apply to their online activity regardless of where they, or the digital service provider with which they are transacting, happen to be. The CCPA, by contrast, purports to establish privacy regulations specific to the jurisdictional reach of the state of California.[25]

The possibility of a "patchwork" of privacy regimes threatens a number of harms. Technical and administrative costs associated with efforts – which, in the end, likely will fail – to tie specific Internet activity to the appropriate jurisdiction. Operational expenses arising from the need to develop and manage multiple compliance programs. Investment decisions distorted by the relative costs of doing business in one state versus another. Innovation deferred or delayed for all due to the most burdensome rules that apply only to some. Unresolvable conflicts between rival statutes and regulations.

B. The Dynamic and Technical Nature of the Digital Services Marketplace Requires the Flexible, Case-by-Case Approach of FTC Enforcement

The digital services marketplace is highly competitive and dynamic. Under current conditions, existing players and new entrants alike are free to innovate, and consumers reap benefits

---

[24] *See* Federal Communications Commission, *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order, WC Docket No. 17-108 (released January 4, 2018), at ¶ 200 ("Because both interstate and intrastate communications can travel over the same Internet connection (and indeed may do so in response to a single query from a consumer), it is impossible or impracticable for ISPs to distinguish between intrastate and interstate communications over the Internet or to apply different rules in each circumstance.").

[25] While the CCPA is a state-level law, once it takes effect its impact likely will be felt nationwide, as businesses may conclude that it is more cost effective to comply only with one set of rules. *See, e.g.*, Jeff John Roberts, "Here Comes America's First Privacy Law: What the CCPA Means for Business and Consumers," *Fortune* (September 13, 2019), available at https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/ (concluding that "since the data privacy law covers out-of-state merchants who sell to Californians – or even display a website in the state – the reality is that companies will comply with the CCPA, rather than step away from the world's fifth largest economy. And rather than create separate systems, lawyers are in consensus that companies will just apply the CCPA nationwide").

generated by this ongoing technological progress. Continued exclusive oversight of consumer online privacy by a single federal agency – specifically, the FTC – through case-by-case enforcement is the best way to ensure not only that digital services continue to develop under optimal conditions, but also that consumer privacy protections keep up as offerings evolve. FTC's actions in response to recent high-profile instances of the misuse of consumer information only confirm the wisdom of this approach.[26]

As Free State Foundation scholars explained in comments submitted last November to the National Telecommunications and Information Administration:

> [C]ase-by-case enforcement, based on the FTC's Section 5 authority and informed by agency enforcement precedents, addresses consumer privacy in a way that targets clear harms but allows for flexibility in digital service provider approaches to protecting privacy. The FTC's analytical approach and enforcement precedents constitute a developed body of law that providers can look to as a guide. Unlike a proscriptive regulatory approach relying on *ex ante* rules, a case-by-case approach allows for individualized examination of the type and use of consumer data involved as well as the underlying digital content, service, or application. By avoiding rigid and categorical restrictions, a case-by-case approach is hospitable to experimentation and innovation in new digital services and privacy protection measures.[27]

At the opposite extreme is the CCPA. It endeavors to codify in great detail not just new privacy rights, but also everything that businesses must do in order to comply, from how notices are drafted and provided, to the methods – both type and number – by which businesses accept requests, to how those requests are verified and processed, and countless steps in between. These burdensome and rigid requirements deny businesses the flexibility to pursue more efficient and practical means of compliance; impose unnecessary costs; create barriers to innovation and new entry; and will remain frozen in time, regardless of how the marketplace evolves, absent further legislative action and/or rulemaking activity.

---

[26] *See, e.g.*, Lesley Fair, "FTC's $5 billion Facebook settlement: Record-breaking and history-making," *Business Blog* (July 24, 2019), available at https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history ("If you've ever wondered what a paradigm shift looks like, you're witnessing one today. The FTC's $5 billion civil penalty against Facebook for violations of an earlier FTC order is record-breaking and history-making. In addition, the settlement requires Facebook to implement changes to its privacy practices, its corporate structure, and the role of CEO Mark Zuckerberg that are seismic in scope. Simply put, when it comes to the business of consumer privacy, it's no longer business as usual at Facebook.").

[27] Comments of the Free State Foundation, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration Docket No. 180821780-8780-01, (submitted November 9, 2018), at 7, available at https://freestatefoundation.org//wp-content/uploads/2019/08/FSF-Comments-to-NTIA-–-Developing-the-Administrations-Approach-to-Consumer-Privacy-110918.pdf. *See also* Thomas B. Pahl, "The View from the FTC: Overseeing Internet Practices in the Digital Age," panel discussion at the Free State Foundation's Ninth Annual Telecom Policy Conference (May 31, 2017), available at http://www.freestatefoundation.org/images/May_31_2017_FTC_Panel_Transcript_072017.pdf (explaining that "in fast-changing areas like online data security and privacy, regulations would need to be amended very often to remain current. Amending regulations is cumbersome and time consuming…. And so such amendments by agencies are very unlikely to keep up with the pace of change. Out-of-date rules can be very unclear in their application to new technologies and cause confusion and unintended consequences in the marketplace").

It is telling that, even before the CCPA could go into effect, the California legislature identified a number of highly specific provisions that warranted amendment. As one example, it was necessary to enact legislation in order to allow online-only businesses to provide only an email address for the receipt of consumer requests, rather than the minimum of two methods (including a toll-free number) explicitly required by the CCPA.[28] Further modifications are to be expected as real-world experience exposes additional gaps in the CCPA's all-encompassing regime.

Similarly, it is difficult to predict in advance the precise ways in which the CCPA's overbearing approach will constrain innovation and new entry. Nevertheless, as the digital services marketplace continues to evolve, it is unlikely that new offerings and new approaches to protecting consumer privacy in all cases will conform to the CCPA's highly detailed fixed guardrails. Moreover, significant compliance costs themselves will deter additional investment and competitive entry: the Attorney General estimates that the compliance costs associated with the proposed implementing rules themselves could exceed $16 billion in the first ten years alone.[29]

C. An "Opt-In" Regime for Non-Sensitive Information Imposes Unjustified Costs and Undermines Incentives to Provide Ad-Supported Content

An "opt-in" regime for the collection and use of non-sensitive consumer information harms consumer welfare in two significant ways. First, a requirement that businesses establish, manage, and monitor programs to elicit and store the preferences of every customer imposes significant costs, necessarily diverting resources away from more productive uses. Second, it imposes artificial constraints on the amount of data provided to advertisers, thereby reducing investment in the "free" content and services that consumers value. As mentioned above, the CCPA to its credit does not embrace "opt-in" for the collection and use of personal information. As a practical matter, however, the numerous exceptions to "opt-out" found within the statute and proposed implementing rules, collectively, could harm the digital services marketplace to a similar degree.

To be clear, the choice between "opt-in" and "opt-out" is not a choice between informed and uninformed consumer behavior. In either case, the rules of the road can be crafted to require that businesses provide consumers with the privacy disclosures necessary to facilitate well-reasoned decision-making. That is the current reality under the FTC's existing "opt-out" approach, which requires digital service providers to disclose their policies regarding the collection and use of personal information "clearly and prominently, immediately prior to the initial collection of or transmission of information, and on a separate screen from any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document."[30]

---

[28] *See* Gretchen A. Ramos, "Governor Newsom Signs CCPA Amendments," *LEXOLOGY* (October 14, 2019), available at https://www.lexology.com/library/detail.aspx?g=ca6fc138-19e1-43a9-b8e3-11cd4cd43e2c.

[29] *CCPA NOPA* at 12. *See also id*. at 11 (noting that the CCPA could impact up to 400,000 businesses), 14 (estimating the initial cost impact on a small business to be $25,000 (plus $1,500 each year thereafter) and on a larger business to be $75,000 (plus $2,500 each year thereafter)).

[30] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Federal Communications Commission WC Docket No. 16-106, (submitted May 27, 2016), available at

Thus, the issue is not whether consumers are able to evaluate whether it is in their best interest to provide personal information in exchange for ad-supported content and services, but whether the default response is "yes" or "no." Consumers clearly prefer exchanging personal information over providing financial consideration in order to access online content and services,[31] therefore "opt-out" is the more efficient approach. It adequately empowers consumers while avoiding the costly administrative and operational burdens associated with "opt-in."

The other major problem with "opt-in" is a practical one. One of the realities of human behavior is that people don't always take action, even when doing so would be in their own best interest and would not require tremendous effort. The fuel for the "free" online offerings that consumers value, meanwhile, is the personal information that enables targeted advertising – and so to the extent that businesses are denied access to that information due solely to the failure of consumers to make their preference known under an "opt-in" regime, consumer welfare suffers.

As Daniel A. Lyons explained in a 2017 Free State Foundation *Perspectives* piece:

> [C]onsumer information is the lifeblood of the Internet. It is the packaging of consumer information into advertising bundles that allows companies like Google to offer the "free" services that consumers have come to expect from the Internet experience, such as search results, email use and storage, and YouTube access. Shifting from opt-out to opt-in dries up the pool of information available for monetization, by removing any information from a consumer that does not make his or her consent known. With less information available, these companies will have fewer advertising dollars with which to subsidize their consumer-facing services. At the margin, this could lead companies to charge for services like gmail that they currently offer for free. And, importantly, a shift to a fee-based access model risks widening the digital divide, by putting Internet-based services beyond the reach of those who cannot or will not pay for them.[32]

With these concerns in mind, let's take a big-picture look at the CCPA. With respect to the sale of personal information, it takes the general position that consumers should be able to "opt-out" rather than be forced to "opt-in." At first glance, then, it would appear that the CCPA avoids the consumer welfare harms that an obligation to obtain affirmative consent would introduce. But upon closer inspection, a number of exceptions appear. So many, in fact, that they threaten to swallow the rule.

---

https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer- protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

[31] *See, e.g.*, Matt Nichols, "NAI Consumer Survey: Digital Advertising, Online Content, and Privacy," *Network Advertising Initiative* (April 9, 2018), available at https://www.networkadvertising.org/blog-entry/nai-consumer-survey-digital-advertising-online-content-and-privacy/ (reporting that 67.1% of consumers prefer online content and services to be financed through advertising).

[32] Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017), at 4, available at https://freestatefoundation.org//wp-content/uploads/2019/05/The-Right-Way-to-Protect-Privacy-Throughout-the-Internet-Ecosystem-032417.pdf.

For one, the CCPA requires "opt-in" whenever the intended use of personal information was not disclosed prior to its collection.[33] The not unreasonable goal motivating this provision, it would seem, is to ensure that businesses do in fact provide adequate and complete information to consumers. At the same time, however, it is important to recognize that, in the highly dynamic digital services marketplace, businesses regularly conceive of new ways to use personal information that produce benefits for consumers. The CCPA's bright-line rule requiring businesses to obtain explicit consent in all cases, rather than allowing them the flexibility to determine the most appropriate means to keep their customers informed, imposes unnecessary costs and impedes innovation.[34]

In addition, a business is required to obtain "opt-in" consent before it enrolls a consumer in a financial incentive program.[35] As I discuss in the next section, the CCPA's focus on non-discrimination, as well as the numerous regulatory restrictions it imposes on the operation of financial incentive programs, may lead businesses to conclude that any benefits derived from such offerings are not worth the associated risks. The obligation to obtain "opt-in" consent, and the administrative and operational costs that would entail, might make that conclusion even more likely.

Lastly, "opt-in" is required for those under the age of 16. Without question, there are sound policy reasons that justify imposing heightened protections with respect to children, particularly those that empower parents and guardians to monitor their activity and make decisions on their behalf. Notably, however, the CCPA requires "opt-in" by a parent or guardian only for children younger than 13; those aged 13 through 15 are able to "opt-in" on their own. Given the conclusion that those in this latter group are able to make privacy-related decisions for themselves, it is not immediately apparent why "opt-out" would not be appropriate for them, as well.

While these exceptions raise concerns of their own, the bigger issue is their potential collective impact. In each case, businesses will have to establish, operate, and monitor a standalone "opt-in" program. The total administrative and operational costs associated with all of these efforts will be substantial, perhaps as high as that of a comprehensive "opt-in" regime covering all customers. In addition, it is inevitable that a significant number of consumers falling within each exception will fail to make their consent known. This will result in the exclusion of their personal information from the pool available to advertisers, which will decrease the amount of

---

[33] *See Proposed Regulations* § 999.305(a)(3) ("A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.").

[34] This is not to say that there are no conceivable instances where the purpose for which a business intends to use previously collected personal information would not warrant obtaining explicit consent from customers. Rather, the point is that a rigid, blanket requirement denies businesses any flexibility to tailor their disclosure methods to the type and sensitivity of the information at issue, the value that the use of that information may provide to customers, the availability of alternative suitable methods of informing customers (*e.g.*, the distribution of revised privacy policies prominently describing such new uses and providing an opportunity to "opt-out"), and other considerations.

[35] *See* Cal. Civ. Code § 1798.125(b)(3) ("A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.").

resources available to fund ad-supported content and services – again, possibly to a similar extent as under a general "opt-in" requirement.

D. Anti-Discrimination Provisions Like the One Included in the CCPA Ignore Consumer Preferences and Threaten the Viability of Ad-Supported Content

I find the most problematic aspect of the CCPA to be the anti-discrimination provision, which states that "[a] business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) [d]enying goods or services to the consumer[;] (B) [c]harging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties[; or] (C) [p]roviding a different level or quality of goods or services to the consumer."[36]

Consumers have made their preference known, and the online experience that they prefer is one defined by the exchange of personal information for "free" content and services. Moreover, they want to make their own decisions in this regard.[37] The CCPA, however, proceeds from a markedly different assumption: that consumers are not capable of making informed decisions regarding the personal information they are willing to provide in the context of such transactions.

Critically, however, the CCPA's attempt to protect from "discrimination" consumers who "opt-out" of the sale of their personal information fails to take into account the real-world, practical impact that it will have on the continued viability of ad-supported content and services. By shielding these consumers from the economic consequences of their decision, the CCPA disincentivizes them from providing their personal information – without acknowledging the fact that, absent the value that personal information provides, businesses may choose to stop making content and services available at no cost. Instead, online providers may migrate to subscription-based offerings that allow them to recover those costs – or perhaps stop providing such offerings altogether. Either of these unintended (but likely) consequences will impact the quantity and quality of content available to consumers, and especially low-income consumers unable to pay for subscription-only services.

Thus, while the CCPA's drafters might like to assume that consumers can have their cake and eat it, too, the reality is that its anti-discrimination provision could lead instead to the end of free cake.

It is true, of course, that the CCPA tries to mitigate the impact of this language by creating an express exemption for differential treatment to the extent that it is "reasonably related to the value provided to the consumer by the consumer's data."[38] On its face, this carve-out would

---

[36] Cal. Civ. Code § 1798.125(a)(1)(A)-(C).

[37] *See, e.g.*, Matt Nichols, "NAI Consumer Survey: Digital Advertising, Online Content, and Privacy," *Network Advertising Initiative* (April 9, 2018), available at https://www.networkadvertising.org/blog-entry/nai-consumer-survey-digital-advertising-online-content-and-privacy/ ("When asked who should make the decision concerning opting a consumer out of targeted advertising, responders largely prefer themselves to be in control of this decision, with 79% indicating that "Individuals" should be in control.").

[38] Cal. Civ. Code § 1798.125(a)(2) ("Nothing in this subdivision 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."). The CCPA similarly allows businesses to provide financial incentives tied to the value of their personal data to consumers who

appear to moot the concerns I laid out above, as it provides businesses with the ability to charge those customers who "opt-out" an amount equal to the value of their data.

In practice, however, I suspect that a number of considerations – including (1) the prohibitive degree to which the statute and proposed implementing rules constrain businesses' ability to tailor that differential treatment (*e.g.*, requiring that they provide notice of such offerings and dictating the permissible methods of calculating the value of consumers' personal data),[39] and (2) the associated regulatory uncertainty and potential liability that could result – will prompt at least some businesses to make a rational decision not to do so. Accordingly, even in light of this exemption, it appears likely that the CCPA's anti-discrimination provision negatively will impact the continued availability of ad-supported offerings by creating a flawed disincentive for consumers to participate in targeted advertising.

IV. Conclusion

Sound time-proven principles of consumer privacy oversight counsel in favor of action at the federal level by a single agency; a flexible, case-by-case approach to enforcement; an "opt-in" regime for the collection and use of non-sensitive consumer information; and an understanding and appreciation of the important role that personal information plays in enabling a robust digital services marketplace.

The CCPA rejects these principles and instead imposes a highly proscriptive regime that creates regulatory uncertainty, prevents privacy protections from evolving over time, imposes significant and unjustified costs, diverts resources away from uses that benefit consumers, deters investment and innovation, and threatens the continued existence of the ad-supported online experience that consumers clearly prefer.

For the benefit of consumers nationwide – and absent further modifications to resolve the problems with the CCPA discussed above – it is critical that Congress pass new law and the FTC take preemptive action to guarantee a consistent, responsive, and exclusively federal approach to consumer privacy oversight.

* Andrew Long is an Adjunct Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland.

---

opt-in to such programs. *See* Cal. Civ. Code § 1798.125(b)(1) ("A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information").

[39] *See, e.g.*, *Proposed Regulations* § 999.337(b) (describing specific methods for calculating the value of consumer data); *see also Proposed Regulations* § 999.336(e) ("A business shall notify consumers of any financial incentive or price or service difference"), Cal. Civ. Code § 1798.125(b)(3) ("A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.").