FREE STATE FSF FOUNDATION

Perspectives from FSF Scholars
November 17, 2020
Vol. 15, No. 60

California Voters Approve the California Privacy Rights Act: A Detailed Analysis of Its Requirements and Impact

by

Andrew Long *

I. Introduction and Summary

On November 3, California voters, by a 56-44 percent margin, approved Proposition 24, the California Privacy Rights Act of 2020 (CPRA). The CPRA, which goes into effect at the beginning of 2023 and applies to data collected after January 1, 2022, layers further obligations upon businesses that – in the middle of a pandemic – are still struggling to determine exactly what is required of them under its predecessor, the California Consumer Privacy Act (CCPA), and its ever-evolving implementing rules. Adoption of Proposition 24 is problematic in many respects.

Online privacy should be regulated at the national, rather than the state, level. And a sound policy approach to protecting consumer privacy should incorporate certain principles: (1) consistent treatment of all marketplace rivals; (2) an "opt-out" model for non-sensitive personal information; (3) case-by-case enforcement by the FTC; (4) no private right of action; and (5) preemption of state and local laws.

The CCPA is at odds with many of these principles, but because it has been in effect for such a brief amount of time, the extent of its harmful impact is as yet unknown. Indeed, this is one of the primary reasons why additional legislation at this moment is such a bad idea. But voters have spoken and, as a result, the CPRA soon will make matters substantially worse than they already were.

The CPRA does so in the following specific ways: (1) it creates a new subcategory of data – "*sensitive* personal information" – and attaches heightened business obligations thereto; (2) it limits regulated entities' ability to engage in behavioral advertising by imposing limits on the "sharing" (as opposed to the CCPA's focus on the "sale") of data; (3) it establishes a new state agency that will take over enforcement and rulemaking responsibilities from the state Attorney General's office; (4) it expands the CCPA's private right of action in connection with data breaches; (5) it places limits upon the legislature's ability to amend its provisions; and (6) it denies lawmakers outright the authority to repeal it.

Congress should pass federal legislation that recognizes the interstate nature of Internet commerce; the positive role that online advertising plays in our economy, in general and especially as we struggle to recover from the impact of the COVID-19 pandemic; and the value that consumers obtain from ad-supported goods and services.

II. Online Privacy Demands a Reasoned, Flexible, and National Approach

When Americans engage in Internet commerce, rarely do they consider the physical location of the businesses with which they transact. Whether across town, two states away, or in a different country, consumers reasonably expect that a single set of rules will govern how those entities handle their personal information. Federal privacy legislation can and should provide that consistent and nationwide regulatory approach.

As broad matters of principle, and as I and other Free State Foundation scholars in the past have argued, federal online privacy law should apply in an equitable fashion to all businesses that collect personal information – not arbitrarily single out certain industry segments such as Internet service providers (ISPs) for differential treatment.[1] It should apply an "opt-out" model to non-sensitive personal information.[2] It should rely upon a case-by-case, dynamic approach to enforcement rather than restrictive *ex ante* rules. It should task the FTC with sole responsibility for policing violations, with perhaps a complementary supporting role for state attorneys general.[3] It should preempt state and local laws that inevitably would lead to a confusing and

[1] *See, e.g.*, Andrew Long, "Maine's ISP-Only Privacy Law Will Not Protect Consumers," *Perspectives from FSF Scholars*, Vol. 15, No. 17 (April 9, 2020), available at https://freestatefoundation.org/wp-content/uploads/2020/04/Maines-ISP-Only-Privacy-Law-Will-Not-Protect-Consumers-040920.pdf.
[2] *See* Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017), available at https://freestatefoundation.org//wp-content/uploads/2019/05/The-Right-Way-to-Protect-Privacy-Throughout-the-Internet-Ecosystem-032417.pdf.
[3] *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; Randolph J. May, "The Net Neutrality CRA Would Remove FTC Privacy Protections," *Perspectives from FSF Scholars*, Vol.

resource-wasting collection of incompatible regimes.[4] And it should prohibit a private right of action, which – to the detriment of the consumers whose interests are the proper focus of privacy regulation – would incentivize the plaintiffs' bar to pursue fee-generating class actions.[5]

To date, however, no such federal law exists. Lawmakers' progress has been stymied most notably by a failure to achieve consensus on the last two topics listed above, state preemption and a private right of action.[6] California, in 2018 and again via the recent ballot referendum, has filled that vacuum. One state, no matter how large, should not dictate the rules of the road that apply throughout the country. A patchwork of potentially inconsistent state and local laws is no better. But in the event that Congress still does not act, the country could find itself faced with both.

III. It Is Far Too Soon to Evaluate the Impact of the California Consumer Privacy Act

Adopted by referendum in the recent election, the California Privacy Regulation Act of 2020 (CPRA) will go into effect on January 1, 2023. Its provisions apply to data collected after January 1, 2022.[7] As was the case with the earlier, legislature-passed California Consumer Privacy Act (CCPA), enforcement will lag by six months, beginning on July 1.[8]

As I described in a May 2020 *Perspectives from FSF Scholars* the CPRA layers on additional regulation before the CCPA ink has dried – and during a pandemic whose economic impact has been mitigated in significant part by the online commerce that digital advertising fosters.[9] Although the CCPA was passed in June 2018 and became effective on January 1 of this year, Attorney General Xavier Becerra's office did not produce final implementing rules until August

---

13, No. 18 (May 9, 2018), available at https://freestatefoundation.org//wp-content/uploads/2019/05/The-Net-Neutrality-CRA-Would-Remove-FTC-Privacy-Protections-050918.pdf.

[4] *See* Andrew Long, "California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019), available at https://freestatefoundation.org/wp-content/uploads/2019/10/California's-Heavy-Handed-Approach-to-Protecting-Consumer-Privacy-–-Exhibit-A-in-the-Case-for-Federal-Preemption-102819.pdf.

[5] *See generally* Andrew Long, "A Privacy Private Right of Action Is Inferior to FTC Enforcement," *Perspectives from FSF Scholars*, Vol. 15, No. 4 (January 21, 2020), available at https://freestatefoundation.org/wp-content/uploads/2020/01/A-Privacy-Private-Right-of-Action-Is-Inferior-to-FTC-Enforcement-012120.pdf.

[6] *See* Andrew Long, "Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," *Perspectives from FSF Scholars*, Vol. 14, No. 42 (December 4, 2019), available at https://freestatefoundation.org/wp-content/uploads/2019/12/Federal-Privacy-Legislation-Bipartisan-Discussions-Devolve-into-Dueling-Drafts-120419.pdf.

[7] *See* The California Privacy Rights Act of 2020, § 31(a), available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf (*CPRA*).

[8] *See id*. at § 21 (adding subsection (d) to § 1798.185 of the CA Civil Code).

[9] *See generally* Andrew Long, "California Privacy Regulation Must Account for the COVID-19 Crisis," *Perspectives from FSF Scholars*, Vol. 15, No. 26 (May 27, 2020), available at https://freestatefoundation.org/wp-content/uploads/2020/05/California-Privacy-Regulation-Must-Account-for-the-COVID-19-Crisis-052720.pdf.

14, six weeks after it began enforcing the underlying statute.[10] Less than two months later, the Attorney General's office proposed still more changes to those rules.[11]

As businesses struggling to stay open were allocating scarce resources in order to come into compliance with the CCPA, the Attorney General's actions introduced unacceptable levels of uncertainty into the process.[12] Making matters worse, Californians for Consumer Privacy, the advocacy group whose 2018 ballot initiative led to the rushed passage of the CCPA, at the same time was working to place Proposition 24 before voters as part of the November 2020 election.

The CCPA itself is an unprecedented privacy statute, one that, as a practical matter and in the absence of a federal law, creates expansive rights for consumers and imposes burdensome obligations on businesses nationwide.

Those rights include: the right to know what data businesses collect; the right to request that their personal information be deleted; the right to opt-out of the sale of their personal information; and a right to non-discrimination for exercising any of the aforementioned rights.

Those obligations include: providing consumers with multiple notices as well as a privacy policy; detailed requirements for the handling of consumer requests; and training and recordkeeping obligations.[13]

It is far too early to appreciate the impact that the specific provisions of the CCPA will have on Internet commerce generally, to say nothing of our nation's ability to recover economically from the COVID-19 public health crisis.[14]

Nevertheless, state voters approved the CPRA – often referred to as the CCPA version 2.0 – on November 3. It is now California law.

IV. The California Privacy Regulation Act Raises a Number of Additional Concerns

The CPRA exacerbates the problems of the CCPA by creating still more consumer rights and business obligations. Among other things, it also defines an additional data category ("*sensitive*

---

[10] *See, e.g.*, Andrew Long, "Proposed Revisions to California's Privacy Law Create Additional Unwanted Uncertainty, Underline Need for Federal Legislation," *FSF Blog* (October 23, 2020), available at https://freestatefoundation.blogspot.com/2020/10/proposed-revisions-to-californias.html.

[11] *See* State of California, Department of Justice, Office of the Attorney General, "California Consumer Privacy Act (CCPA) Current Rulemaking Activities," available at https://www.oag.ca.gov/privacy/ccpa/current.

[12] *See, e.g.*, Andrew Long, "Privacy Recap: Another CCPA Update, Another COVID-19 Bill," *FSF Blog* (June 5, 2020), available at https://freestatefoundation.blogspot.com/2020/06/privacy-recap-another-ccpa-update.html; Andrew Long, "Will Enforcement of California's Privacy Law Precede Final Rules?," *FSF Blog* (April 13, 2020), available at https://freestatefoundation.blogspot.com/2020/04/will-enforcement-of-californias-privacy.html.

[13] For an in-depth discussion of the CCPA, *see* Andrew Long, "California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019), available at https://freestatefoundation.org/wp-content/uploads/2019/10/California's-Heavy-Handed-Approach-to-Protecting-Consumer-Privacy-–-Exhibit-A-in-the-Case-for-Federal-Preemption-102819.pdf.

[14] *See* Andrew Long, "State Online Advertising Laws: Wrong Policies, Wrong Time," *Perspectives from FSF Scholars*, Vol. 15, No. 22 (April 30, 2020), available at https://freestatefoundation.org/wp-content/uploads/2020/04/State-Online-Advertising-Laws-Wrong-Policies-Wrong-Time-043020.pdf.

personal data"), restricts the "sharing" of data for the purpose of cross-context behavioral advertising, establishes a new state agency, and expands the data breach private right of action. Perhaps most concerning, however, are the ways in which it imposes constraints upon the legislature's lawmaking authority.

First, the CPRA creates new consumer rights, in particular (1) the right to correct inaccurate personal information, and (2) the right to data minimization, which will require business to disclose for how long they retain personal information and prohibit them from retaining that data "for longer than is reasonably necessary."[15]

Second, the CPRA creates a new subcategory of data. "Sensitive personal information" is defined as a subset of "personal information" that includes social security, driver's license, and passport numbers; debit/credit card numbers and other information used to access financial accounts; precise geolocation information; racial or ethnic origin, religious beliefs, or union membership; the contents of mail, email, and text messages; genetic information; biometric data used to identify an individual consumer; and information concerning a consumer's sex life or sexual orientation.[16]

Businesses will be required to provide notice to consumers that (1) their sensitive personal information may be used or disclosed, and for what specific purposes, and (2) they at any time may opt out of the use or disclosure of their sensitive personal information.[17] To facilitate the latter, businesses will have to add a "Limit the Use of My Sensitive Personal Information" link to their websites.[18]

Third, whereas the CCPA focused exclusively on the "sale" of personal information, the CPRA attempts to limit the use of cross-context behavioral advertising by including restrictions on the "sharing" of data for that purpose.[19] Consumers will have the right to opt-out of the "sharing" of their personal information,[20] and businesses will be required to add the words "Or Share" to the "Do Not Sell My Personal Information" link that the CCPA requires them to display on their homepages.[21]

Fourth, the CPRA immediately creates new bureaucracy, the California Privacy Protection Agency (CPPA). The CPPA will: assume rulemaking responsibilities from the Attorney

---

[15] *See CPRA* § 4 (adding subsection (a)(3) to § 1798.100 of the CA Civil Code).
[16] *See id*. at § 14 (adding § 1798.140(ae) to the CA Civil Code). "Sensitive personal information" excludes "publicly available" information. *See id*. (revising § 1798.140(o)(2) of the CA Civil Code to exclude "publicly available information or lawfully obtained, truthful information that is a matter of public concern" from the definition of "public information" set forth in subsection (o)(1)).
[17] *See id*. at § 10 (adding § 1798.121 to the CA Civil Code).
[18] *See id*. at § 13 (adding subsection (a)(2) to § 1798.135 of the CA Civil Code).
[19] *See id*. at § 14 (adding subsection (ah)(1) to § 1798.140 of the CA Civil Code) ("'Share,' 'shared,' or 'sharing' means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.").
[20] *See id*. at § 9 (revising § 1798.120(a) of the CA Civil Code).
[21] *See id*. at § 13 (revising § 1798.135(a)(1) of the CA Civil Code).

General's office; "administer, implement, and enforce" the amended CCPA through administrative proceedings; appoint a Chief Privacy Auditor; investigate and conduct hearings regarding possible violations; issue cease and desist orders; and impose fines.[22] The CPRA allocates to the agency's budget a minimum of $5 million from the state General Fund in fiscal year 2020-21 and $10 million every year that follows.

Fifth, the CPRA expands the CCPA's data-breach private right of action in two respects. One, the CCPA authorized a private right of action only where exposed data was not encrypted or redacted, but the CPRA will allow consumers to sue where an email address and password or security question – credentials "that permit access to the account" – are revealed.[23] Two, the CCPA provided businesses with a thirty-day period in which to cure a security breach, but the CPRA clarifies that "[t]he implementation and maintenance of reasonable security procedures and practices … following a breach does not constitute a cure with respect to that breach."[24] A breach cure will continue to serve as a bar to a suit for damages, but only where "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."[25]

Sixth, and as noted above, similar to the European General Data Protection Regulation (GDPR),[26] the CPRA incorporates the concept of "data minimization," stating that, as a general principle, "[b]usinesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared."[27]

Seventh, the CPRA restrictively defines "consent" as:

> [A]ny freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent."[28]

---

[22] *See generally id*. at § 24 (adding §§ 1798.199.10 *et seq*. to the CA Civil Code).
[23] *See id*. at § 16 (revising § 1798.150(a)(1) of the CA Civil Code).
[24] *Id*. (revising § 1798.150(b) of the CA Civil Code).
[25] *Id*.
[26] *See* Regulation (EU) 2016/679 (General Data Protection Regulation), Chapter II, Article 5(1)(c) ("Personal data shall be … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[27] *CPRA* at § 3(B)(3).
[28] *Id*. at § 14 (adding a new subsection (h) to § 1798.140 of the CA Civil Code).

Finally, the CPRA in two ways proactively denies the legislature the ability to exercise its core lawmaking authority. First, it states that it "may be amended after its approval by the voters by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor, *provided that such amendments are consistent with and further [its] purpose and intent*."[29] Second, it includes the following language, which appears to deny lawmakers the ability to repeal it at a later date:

> The provisions of this Act shall prevail over any conflicting legislation enacted after January 1, 2020. Any amendments to this Act or any legislation that conflicts with any provision of this Act shall be null and void upon passage of this Act by the voters, regardless of the code in which it appears. Legislation shall be considered "conflicting" for purposes of this subdivision, unless the legislation is consistent with and furthers the purpose and intent of this Act ….[30]

Thus, should subsequent events call into question the wisdom of parts or all of the CPRA – as surely will be the case – then yet another ballot initiative would be required. As TechNet CEO Linda Moore recently noted, "[t]he legislature should be in charge, along with the governor, in setting privacy policy. This takes it out of the hands of the people who can work on this complicated issue."[31]

V. Conclusion

The CPRA ratchets up regulation of online advertising at a doubly inopportune moment: (1) well before the impact of its predecessor statute, the CCPA, can be evaluated, and (2) in the middle of an economic crisis whose harmful impact has been mitigated by the electronic commerce that the CCPA targets. Fortunately, businesses have until January 1, 2023, before they must comply with its provisions. In the meantime, the California Privacy Protection Agency will take over rulemaking and enforcement responsibilities from the state Attorney General's office.

By its terms, the CPRA denies the California legislature its constitutional role to make and revise law. The legislature may amend the CPRA only to the extent that such changes "are consistent with and further [its] purpose and intent" – and a repeal is barred outright. Only a subsequent ballot initiative or preemptive federal law can unwind that which voters recently approved.

Congress must seize this moment. Internet commerce is an interstate concern that demands a single set of privacy rules; a dynamic marketplace that calls out for a flexible, case-by-case approach rather than a patchwork of rigid *ex ante* state laws; and a powerful catalyst that buoys our economy and produces significant consumer benefits. Now more than ever, federal privacy legislation is required that preempts state laws, expressly denies the plaintiffs' bar a private right of action, affirms the exclusive enforcement role of the FTC and state attorneys general, and

---

[29] *Id*. at § 25(a) (emphasis added).
[30] *Id*. at § 25(d). *See also* Peter Hegel, *et al*., "The California Privacy Rights Act (CPRA) Has Been Enacted into Law," *PH Privacy* ((November 6, 2020), available at https://www.paulhastings.com/publications-items/blog/ph-privacy/ph-privacy/2020/11/06/the-california-privacy-rights-act-(cpra)-has-been-enacted-into-law#page=1 ("Unlike the CCPA, the CPRA cannot be repealed by the California legislature.").
[31] Issie Lapowsky, "California privacy ballot measure Prop 24 passes," *Protocol* (November 4, 2020), available at https://www.protocol.com/bulletins/election-california-privacy-ballot-measure-prop-24-passes.

safeguards the substantial and beneficial role that ad-supported goods and services play in Americans' lives.

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

Further Readings

Andrew Long, "Proposed Revisions to California's Privacy Law Create Additional Unwanted Uncertainty, Underline Need for Federal Legislation," *FSF Blog* (October 23, 2020).

Andrew Long, "California Privacy Regulation Must Account for the COVID-19 Crisis," *Perspectives from FSF Scholars*, Vol. 15, No. 26 (May 27, 2020).

Andrew Long, "State Online Advertising Laws: Wrong Policies, Wrong Time," *Perspectives from FSF Scholars*, Vol. 15, No. 22 (April 30, 2020).

Andrew Long, "Maine's ISP-Only Privacy Law Will Not Protect Consumers," *Perspectives from FSF Scholars*, Vol. 15, No. 17 (April 9, 2020).

Andrew Long, "A Privacy Private Right of Action Is Inferior to FTC Enforcement," *Perspectives from FSF Scholars*, Vol. 15, No. 4 (January 21, 2020).

Andrew Long, "Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," *Perspectives from FSF Scholars*, Vol. 14, No. 42 (December 4, 2019).

Andrew Long, "California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019).

Theodore R. Bolema, "Protecting Privacy on the Internet: Key Principles for Any Reform," *Perspectives from FSF Scholars*, Vol. 14, No. 9 (April 4, 2019).

Comments of the Free State Foundation, *Developing the Administration's Approach to Consumer Privacy*, NTIA Docket No. 180821780-8780-01 (November 9, 2018).

Randolph J. May, "The Net Neutrality CRA Would Remove FTC Privacy Protections," *Perspectives from FSF Scholars*, Vol. 13, No. 18 (May 9, 2018).

Daniel A. Lyons, "The Right Way to Protect Privacy Throughout the Internet Ecosystem," *Perspectives from FSF Scholars*, Vol. 12, No. 10 (March 24, 2017).