

APRIL 30, 2019

Privacy and Data Security Alert

Privacy Legislation Continues To Move Forward in Many States

By [Jonathan G. Cedarbaum](#), [D. Reed Freeman, Jr.](#) and [Lydia Lichlyter](#)

Since our [February 20, 2019 report](#) on privacy bills moving through state legislatures around the country, four new bills modeled on the California Consumer Privacy Act (CCPA) have been introduced, and many of the previously described bills have moved further along in the legislative process. Washington's Privacy Act, which previously seemed likely to be the first state enactment to follow in the CCPA's wake, failed to make it out of the state house before the end of the legislative session. In [Section A](#) below, we provide brief updates on the CCPA-like bills described in our previous report. In [Section B](#) below, we then describe the four newer bills resembling the CCPA, introduced in Connecticut, New York, Pennsylvania, and Texas. Last week, the Connecticut bill modeled on the CCPA was substituted with one instead establishing a consumer privacy task force. The senate passed the substitute task force bill unanimously.

Sections C and D review substantial privacy bills not modeled on the CCPA. [Section C](#) provides status updates on the bills of this sort reviewed in our prior report. [Section D](#) describes three newly introduced bills—one in Illinois addressing the handling of geolocation information in particular; one in Louisiana that would prohibit online service providers from disclosing consumers' personal information without their express consent; and one in Nevada that would require online service providers to give consumers the opportunity to opt out of the sale of their personal information.

Sections E and F address more targeted privacy bills. [Section E](#) describes the status of the bills of this sort that we summarized in our prior report. One of those, North Dakota's H.B. 1485, has been signed into law, requiring "legislative management" to undertake a study of "protections, enforcement, and remedies regarding the disclosure of consumers' personal data." [Section F](#) describes eight more limited privacy bills introduced since our last report. Many of these would restrict the ability of Internet service providers to disclose or sell consumers' personal information without consumers consent. One would prohibit targeted advertising aimed at children.

Finally, [Section G](#) reviews the bills seeking to amend the CCPA that the California legislature has under consideration.

On April 23, the California Assembly Privacy and Consumer Protection Committee approved eight bills: A.B. 25, A.B. 846, A.B. 873, A.B. 874, A.B. 981, A.B. 1146, A.B. 1355 and A.B. 1564. The most significant are A.B. 25, which would clarify that the CCPA does not apply to information

collected from job applicants, employees, contractors, and agents in the context of those roles; A.B. 846, which would amend the non-discrimination section of the CCPA to make clear that covered businesses may offer loyalty and rewards programs; A.B. 873, which would narrow the definition of “personal information” slightly and harmonize the definition of “deidentified” data with Federal Trade Commission (FTC) guidance; A.B. 873, which would modify the definition of “publicly available” information to remove the requirement that businesses consider the context in which information in government records was collected; A.B. 874, which would modify the definition of “publicly available” information to remove the requirement that businesses consider the context in which information in government records was collected; A.B. 981, which would exempt from the CCPA individuals and entities subject to the Insurance Information and Privacy Protection Act; and A.B. 1146, which would exempt vehicle information shared in connection with repairs, warranties, and recalls. Two bills (A.B. 288 and A.B. 1760) were withdrawn before the hearing.

S.B. 561, which would make the entire CCPA subject to a private right of action, was scheduled to be considered by the Senate Appropriations Committee on April 29 (having previously been approved by the Senate Judiciary Committee), but it was instead moved to the suspense file for an assessment of its fiscal impact.

Section A. Status of Bills Similar to the CCPA Described in Our Prior Report

1. **Washington – Washington Privacy Act (S.B. 5376/H.B. 1854)**

Current status: The bill passed the senate, but the house failed to pass it before the close of the legislative session.

2. **Hawaii – S.B. 418**

Current status: The bill remains in committee.

3. **Maryland – Online Consumer Protection Act (S.B. 613/H.B. 901)**

Current status: The legislature adjourned without passing the bill.

4. **Massachusetts – S.B. 120**

Current status: Introduced in January 2019, the bill was referred to the Joint Committee on Consumer Protection and Professional Licensure. No action has yet followed.

5. **New Mexico – Consumer Information Privacy Act (S.B. 176)**

Current status: The legislature adjourned without passing the bill.

6. **Rhode Island – Consumer Privacy Protection Act (S.B. 234/H.B. 5930)**

Current status: Both versions of the bill remain in committee. The Senate version is scheduled for a hearing on April 30. The House version was withdrawn from a scheduled hearing on April 2.

Section B. Newly Introduced Bills Similar to the CCPA

7. **Connecticut – S.B. 1108**

Current status: Introduced in March 2019, the bill was referred to the Joint Committee on Government Administration and Elections. It was voted out of committee in early April 2019,

referred to Legislative Commissioner's Office for research and fiscal analysis, which reported it out with a favorable report. On April 25, the senate adopted an amendment substituting the bill for one establishing a consumer privacy task force and passed the substitute bill.

Key provisions of the earlier bill version:

- Modeled closely on the CCPA, the bill would have given consumers rights to notice of "personal information" collected and parties to whom such information is sold or disclosed for a business purpose; to request deletion; and to optout from sale.
- As under the CCPA, consumers would have had a private right of action for data breaches caused by a business's failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Under S.B. 1108, unlike under the CCPA, they would have been required to give the Attorney General notice and an opportunity to intervene in any case filed.
- Rulemaking under the bill would have been conducted by the Commissioner of Consumer Protection, in consultation with the state's Chief Information Officer, instead of by the Attorney General.
- The law would have taken effect January 1, 2020, notwithstanding that the Commissioner of Consumer Protection would not have been required to promulgate regulations until the same date (and not until January 1, 2021, for some categories of regulations).

8. New York – [S.B. 4411/A.B. 6351](#)

Current status: Both versions (which are identical) were introduced in March 2019 and referred to their respective chambers' Consumer Affairs and Protection committees.

Key provisions:

- Modeled on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties to whom such information is sold or disclosed for a business purpose; to request deletion; and to optout from sale.
- The bill does not contain the CCPA's right to have personal information deleted.
- In the definition of covered businesses, the revenue threshold is \$50 million (rather than the \$25 million in the CCPA); the affected consumer threshold is 100,000 users (rather than the 50,000 in the CCPA).
- The bill does not contain the CCPA's requirement that a business disclose the "specific pieces" of personal information that it has collected.
- The bill authorizes private rights of action for violations of any of the rights established, not just for data breaches.
 - Any violation of the act is deemed an "injury in fact," and a plaintiff "need not suffer a loss of money or property as a result of the violation in order to bring an action."

- Damages are \$1000 per violation, or actual damages, whichever is greater; for “knowing and willful violations,” a consumer can receive up to \$3000 per violation, or actual damages, whichever is greater.
- If “any person becomes aware, based on non-public information, that a person or business has violated” the law, they would be able to file a request with the attorney general to bring a suit.
 - If the Attorney General elects to pursue the case, the whistleblower would receive 15% of any civil penalties collected.
 - If the Attorney General elects not to pursue the case, the whistleblower could pursue it themselves and receive 25-50% of the proceeds of the action.
- The bill does not contain the CCPA’s exceptions for information collected as part of a clinical trial, and for information subject to the Gramm-Leach-Bliley Act.
- The bill states that a business that suffers “a breach of the security of the system involving consumers’ personal information” is liable for violating the law “if the business has failed to implement reasonable security procedures and practice, appropriate to the nature of the information.” No personal information need be lost or any harm suffered as a result of the breach.
- The bill applies to “the collection and sale of all personal information collected by a business from consumers,” not only information collected “electronically or over the Internet.”

9. **Pennsylvania – H.B. 1049**

Current status: The bill was introduced in April 2019 and referred to the Consumer Affairs Committee.

Key provisions:

- Modeled on the CCPA, the bill would give consumers rights to notice of “personal information” collected and parties to whom such information is sold or disclosed for a business purpose; to request deletion; and to optout from sale.
- In the definition of covered businesses, the revenue threshold is \$10 million (rather than the \$25 million in the CCPA).

10. **Texas – Texas Consumer Privacy Act (H.B. 4518)**

Current status: The bill was introduced in March 2019 and referred to the Business & Industry Committee. The committee held a hearing to consider the bill in April 2019.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of “personal information” collected and parties to whom such information is sold or disclosed for a business purpose; to request deletion; and to optout from sale.

- The bill would require businesses to disclose categories of personal information collected and “items within each category” (instead of “specific pieces” of information, as in the CCPA).
- The bill omits a private right of action, along with the associated requirement that businesses provide “reasonable security.”
- The law would take effect on September 1, 2020; no deadline is given for the promulgation of regulations by the attorney general

Section C. Status of Bills Not Modeled on the CCPA Summarized in Our Prior Report

11. Illinois – The Right to Know Act (S.B. 2149/H.B. 2736)

Current status: Both versions of the bill remain in committee.

12. New Jersey – A.B. 4640/S.B. 3153

Current status: Both versions of the bill remain in committee.

13. New York – Online Consumer Protection Act (S.B. 2323/A.B. 3818)

Current status: Both versions of the bill remain in committee.

14. New York – S.B. 1177: Removal of Online Content Posted by Minors

Current status: The bill remains in committee.

15. New York – Right to Know Act of 2019 (S.B. 224/A.B. 3739)

Current status: Both versions of the bill remain in committee.

16. Oregon – H.B. 2866

Current status: The Judiciary Committee held hearings on March 12 and 13. No action has yet followed.

17. Virginia – H.B. 2535: Digital Protections for Virginia’s Minors

Current status: The legislature adjourned without passing the bill.

18. Washington – Consumer Data Transparency Act (H.B. 2046)

Current status: The bill remains in committee.

Section D. Newly Introduced Bills Not Modeled on the CCPA

19. Illinois – Geolocation Privacy Protection Act (H.B. 2785)

Current status: The bill was introduced in February 2019 and referred to the Rules Committee.

Key provisions:

- The bill would prevent companies that operate apps from collecting, using, storing, or disclosing geolocation information from an app without affirmative express consent.
- The bill contains exceptions for emergency situations.

- The bill would not apply to location information stored locally on a device.
- The bill would apply only to apps created or modified after the effective date.

20. **Louisiana – [Internet and Social Media Privacy and Protection Act \(H.B. 465\)](#)**

Current status: The bill was introduced in March 2019 and referred to the Committee on Commerce.

Key provisions:

- The bill would apply to Internet service providers (ISPs), social media companies, any company that operates a website or online service for commercial purposes, and anyone who uses marketing on social media.
- Covered entities would not be permitted to disclose consumer personal information without “express consent.”
- ISPs and social media companies would be required to post a privacy notice.
- The bill contains a private right of action (without statutory damages) for consumers whose personal information is unlawfully disclosed.

21. **Nevada – [S.B. 220](#)**

Current status: The bill was introduced in February 2019 and passed the senate in April 2019. It is currently pending in the assembly’s Committee on Commerce and Labor.

Key provisions:

- The bill would create a right for consumers to opt out of the sale by operators of websites or online services of their “covered information,” including names, addresses, emails, Social Security numbers, unique identifiers, and “any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable.”
- Operators would be required to provide a “designated request address” — an email address, toll-free telephone number, or website—consumers could use to submit opt-out requests.
- Operators would be required to respond verified requests within 60 days, or within 90 days if the extension is reasonably necessary.

Section E. Status of Limited Privacy Bills Summarized in Our Prior Report

22. In **Connecticut**, the Joint Committee on Children held a hearing on [H.B. 6601](#) in February 2019. There still is no full text readily available.

23. In **Montana**, the [Internet Access Service Customer Privacy Act \(H.B. 457\)](#) was passed by the House and tabled in the Senate Judiciary Committee.

24. In **New Jersey**, [S.B. 2634](#) remains in committee. The Assembly version, A.B. 3923, was reported out of the Science, Innovation and Technology Committee.
25. In **New York**, [S.B. 518](#), [A.B. 2420](#), and [S.B. 1180](#) remain in committee.
26. In **North Dakota**, [H.B. 1485](#) was signed into law. It requires “legislative management” to undertake a study of “protections, enforcement, and remedies regarding the disclosure of consumers’ personal data.”

Section F. Recently Introduced Limited Privacy Bills

27. In **Illinois**, the [App Privacy Protection Act](#) (H.B. 3051) was introduced in February 2019 and referred to the Rules Committee. It would require an operator of a “web site, online service, or software application” to disclose in its terms of service the names of third parties that collect electronic information through its service, along with the categories of information they collect.
28. In **Vermont**, [S.B. 110](#) was introduced in February 2019, passed the Senate in March 2019, and was referred to the House Committee on Commerce and Economic Development. It would prohibit targeted advertising, building of profiles, and selling of data on sites, services, or applications used for school purposes through grade 12.
29. In **Maine**, [S.B. 946](#) was introduced in February 2019 and referred to the Joint Energy, Utilities and Technology Committee. It would require Internet service providers to obtain “express, affirmative consent” before using, disclosing, selling, or permitting access to a customer’s personal information, and to take reasonable measures to protect the security of customer personal information.
30. In **Pennsylvania**, the [Internet Privacy and Consumer Protection Act](#) (H.B. 246) was introduced in January 2019 and referred to the Commerce Committee. It would require Internet service providers to obtain written or electronic authorization before disclosing a customer’s personally identifiable information. The bill also contains provisions regarding disclosure of electronic communication records to governmental entities and commercial email solicitation.
31. In **Minnesota**, [S.F. 1553](#) was introduced in February 2019 and referred to the Energy and Utilities Finance and Policy Committee. It would require Internet service providers to obtain written or electronic authorization before disclosing a customer’s personally identifiable information, and to take reasonable steps to protect the security of customer personal information.
32. In **Minnesota**, [H.B. 1030](#) was introduced in February 2019 and referred to the Commerce Committee. It would prohibit Internet service providers with contracts with the state from collecting personal information from customers without “express written approval.”
33. In **New York**, [A.B. 3612](#) was introduced in January 2019 and referred to the Consumer Affairs and Protection Committee. It would prohibit Internet service providers from sharing, using, selling, or providing a customer’s sensitive personal information to a third party without the customer’s “written and explicit permission.”

34. In **South Carolina**, the [South Carolina Cellular Data Privacy Protection Act](#) (H.B. 3701) was introduced in January 2019 and referred to the Committee on Labor, Commerce and Industry. It would prohibit a cellular telecommunications provider from selling a consumer's data to a third party.

Section G. Bills Amending the CCPA

35. [S.B. 561](#)

Current status: The bill was introduced in February 2019 and referred to the Senate Judiciary Committee. It passed that committee in April 2019 and was referred to the Senate Appropriations Committee. It has been moved to the suspense file for an assessment of its fiscal impact.

Key provisions: The bill would make the entire CCPA subject to a private right of action. It would remove businesses' ability to seek guidance from the attorney general and the 30-day right to cure violations.

36. [S.B. 753](#)

Current status: The substance of the bill was introduced in April 2019 and referred to the Senate Judiciary Committee. It was withdrawn from a scheduled hearing on April 23.

Key provisions: The bill would amend the definition of "sale" to allow businesses to disclose unique identifiers for the purpose of serving or auditing advertisements.

37. [A.B. 25](#)

Current status: The substance of the bill was introduced in March 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would clarify that the CCPA does not apply to information collected from job applicants, employees, contractors, and agents in the context of those roles. The bill may (depending on the outcome of negotiations) make further changes regarding business-to-business interactions, specific pieces of information, and/or household and device information.

38. [A.B. 288](#)

Current status: The bill was introduced in January 2019 and referred to the Assembly Committee on Privacy and Consumer Protection. It was withdrawn from a scheduled hearing on April 23.

Key provisions: Though not technically an amendment to the CCPA, the bill would add additional requirements for "social networking services" to delete consumer information upon request. It would create a private right of action for violations of these requirements.

39. [A.B. 846](#)

Current status: The substance of the bill was introduced in March 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: This bill would amend the non-discrimination section of the CCPA to make clear that covered businesses may offer loyalty and rewards programs.

40. [A.B. 873](#)

Current status: The substance of the bill was introduced in March 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would narrow the definition of “personal information” slightly and harmonize the definition of “deidentified” data with FTC guidance.

41. [A.B. 874](#)

Current status: The substance of the bill was introduced in March 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would modify the definition of “publicly available” information to remove the requirement that businesses consider the context in which information in government records was collected.

42. [A.B. 981](#)

Current status: The substance of the bill was introduced in April 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would exempt from the CCPA individuals and entities subject to the Insurance Information and Privacy Protection Act.

43. [A.B. 1146](#)

Current status: The bill was introduced in February 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would exempt vehicle information shared in connection with repairs, warranties, and recalls.

44. [A.B. 1355](#)

Current status: The bill was introduced in February 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would make non-substantive and typographical changes to the CCPA, including to ensure that deidentified and aggregate information are excluded from the definition of “personal information.”

45. [A.B. 1416](#)

Current status: The bill was introduced in February 2019 and referred to the Assembly Committee on Privacy and Consumer Protection. It is set for a hearing on April 30.

Key provisions: The bill would add exceptions to the CCPA to allow businesses to protect against fraud, security incidents, and other “malicious, deceptive, or illegal activity.”

46. [A.B. 1564](#)

Current status: The bill was introduced in February 2019 and voted out of the Assembly Committee on Privacy and Consumer Protection on April 23.

Key provisions: The bill would allow a business to maintain an email address for consumers to submit requests for personal information, instead of requiring them to have a toll-free telephone number.

47. **A.B. 1760**

Current status: The substance of the bill was introduced in April 2019 and referred to the Assembly Committee on Privacy and Consumer Protection. It was withdrawn from a scheduled hearing on April 23, and it is not expected to pass this year.

Key provisions: The bill would make massive changes to the CCPA, including subjecting the entire law to a private right of action, authorizing enforcement by city attorneys, requiring companies to name specific third parties with which they share data, and changing the CCPA's limitations on "selling" data to apply to "sharing" data.

For more information on this or other privacy and data security matters, contact:

Jonathan G. Cedarbaum +1 202 663 6315 jonathan.cedarbaum@wilmerhale.com

D. Reed Freeman, Jr. +1 202 663 6267 reed.freeman@wilmerhale.com

Lydia Lichlyter +1 202 663 6460 lydia.lichlyter@wilmerhale.com

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 1875 Pennsylvania Avenue, NW, Washington, DC 20006, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. © 2018 Wilmer Cutler Pickering Hale and Dorr LLP