State Legislatures Make Privacy a Priority as 2020 Sessions Begin

FEBRUARY 3, 2019

By Jonathan G. Cedarbaum, D. Reed Freeman, Jr., Lydia Lichlyter, and Ali A. Jessani

As state legislatures begin their 2020 sessions, proposals for stronger privacy laws are at the top of the agenda across the country. Carrying forward the story we told in reports in February, April, and July of last year, this report describes more than a dozen bills that have been introduced in state legislatures in the last month or carried over from the previous legislative session.

Omnibus bills have been introduced in at least seven states, including Washington, where a similar bill narrowly failed to pass in 2019. We describe these bills in Section A.

At least eight bills with more targeted requirements have also been introduced, including bills in Florida, Hawaii, and Maryland that would provide some version of a consumer right to opt out from sale similar to the one in the California Consumer Privacy Act (CCPA). We provide overviews of these bills in Section B.

Throughout the year, WilmerHale's Privacy and Cybersecurity Group will be tracking and reporting on the progress of these and other proposals for enhanced privacy protections in state law.

Section A. Omnibus Privacy Bills

1. **Illinois – Data Privacy Act (S.B. 2263)**

   Current status: Introduced in May 2019 and referred to the Senate Assignments Committee. It did not come to a vote in 2019. It has been carried over to the 2020 session.

   Key provisions:

   - Draws its terminology primarily from the EU's General Data Protection Regulation (GDPR) and is similar to the Virginia Privacy Act described below

- Would apply to businesses that (i) control or process the personal data of 100,000 or more Illinois residents or (ii) derive over 50% of their gross revenue from the sale of personal data and process or control the personal data of 25,000 or more Illinois residents
- Contains exemptions for individuals acting in an employment or commercial context, as well as for information subject to Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), or Gramm-Leach-Bliley Act (GLBA)
- Consumers would have rights, upon request, to access (in a portable form), correct, delete, and object to processing. The right to object to processing includes a right to object to the use of personal data for targeted advertising
- Controllers would be required to disclose the categories of personal information they collect, the purposes for which personal data is used, the categories of personal data shared with third parties, and the categories of third parties with whom it is shared
- Controllers would be required to conduct risk assessments of their processing activities and provide them to the attorney general upon request
- Would not create a private right of action; the attorney general would be empowered to seek civil penalties of $2,500 per violation or $7,500 per intentional violation

2. **Nebraska – Nebraska Privacy Act (L.B. 746)**

Current status: Introduced in January 2020 and referred to the Unicameral Committee on Transportation and Telecommunications. Hearing scheduled for February 4, 2020.

Key provisions:

- Largely mirrors the CCPA
- Would apply to businesses that collect personal information from Nebraska residents, determine the purposes and means of processing that personal information and meet one of the following thresholds:
    - annual gross revenue in excess of $10 million;
    - alone, or in combination, annually buy, receive for the business's commercial purposes, sell, or share the personal information of 50,000 or more consumers; or
    - derive 50 percent or more of annual revenue from selling consumer personal information
- Like the CCPA, contains exemptions for information subject to HIPAA, FCRA, or GLBA; unlike the CCPA, also has an entity-level exemption for financial institutions or their affiliates that are regulated by the GLBA
- Consumers would have rights, upon request, to access, delete, and opt out of the sale of their personal information; businesses may not discriminate against consumers for exercising their rights

- Upon request from a consumer, businesses would be required to disclose the categories of personal information they collect, the business or commercial purposes for which the information is collected, the categories of sources from which the information is collected, the specific pieces of personal information collected, and the categories of third parties with whom it is shared
- Businesses would have to make certain disclosures in their online privacy policy
- Businesses that sell personal information would be required to place a "Do Not Sell My Personal Information" link on their homepage, in their privacy policy, and in any Nebraska-specific description of consumer rights
- No private right of action; enforceable by the attorney general, with fines up to $7,500 per violation

3. **New Hampshire – H.B. 1680-FN**

Current status: Introduced in December 2019 and referred to the House Committee on Commerce and Consumer Affairs. Hearing held on January 23, 2020.

Key provisions:

- Largely mirrors the CCPA
- Would apply to businesses that collect personal information from New Hampshire residents, determine the purposes and means of processing that personal information, and meet one of the following thresholds:
    - annual gross revenue in excess of $25 million;
    - alone, or in combination, annually buy, receive for the business's commercial purposes, sell, or share the personal information of 50,000 or more consumers; or
    - derive 50 percent or more of their annual revenue from selling consumer personal information
- Like the CCPA, contains exemptions for information subject to HIPAA, FCRA, or GLBA
- Consumers would have rights, upon request, to access, delete, and opt out of the sale of their personal information; businesses may not discriminate against consumers for exercising their rights
- Upon request from a consumer, businesses would be required to disclose the categories of personal information they collect, the business or commercial purposes for which the information is collected, the categories of sources from which the information is collected, the specific pieces of personal information collected, and the categories of third parties with whom it is shared

- Businesses that sell personal information would be required to place a "Do Not Sell My Personal Information" link on their homepage, in their privacy policy, and in any New Hampshire–specific description of consumer rights
- Businesses would have to disclose certain information in their privacy policy
- Like the CCPA, provides a private right of action for data breaches only, with fines up to $750 per violation; privacy violations enforceable only by the attorney general, with fines up to $2,500 per violation or $7,500 per intentional violation

4. **New Jersey – S.B. 269**

Current status: Introduced in January 2020 and referred to the Senate Commerce Committee.

Key provisions:

- Uses a mixture of GDPR and CCPA principles and terms
- Would apply to businesses that meet one of the following thresholds:
    - annual gross revenue in excess of $5 million;
    - alone, or in combination, annually buys, receives for the business's commercial purposes, sells, or shares the personal information of 25,000 or more data subjects; or
    - derives 50 percent or more of annual revenue from selling personal information
- No exemptions for information subject to HIPAA, FCRA or GLBA
- Would require businesses to maintain an information security program that either meets federal law requirements (if applicable) or industry standards
- Upon collecting information from a data subject, businesses would be required to provide the data subject with:
    - the purpose and legal basis for the processing of the personally identifiable information;
    - a complete description of the personally identifiable information that the business collects about the data subject and the means by which a business collects the personally identifiable information;
    - all third parties to which the business may disclose the data subject's personally identifiable information;
    - the purpose of the disclosure of personally identifiable information, including whether the business profits from the disclosure; and
    - the contact information of the person employed at the business responsible for personally identifiable information data protection, where applicable
- Would require businesses to allow data subjects to opt out of the processing of their data, subject to certain exceptions

- Would require businesses to provide data subjects with the data retention period of the data processing, as well as the right to access the data
- Like the CCPA, would create a private right of action only for data breaches, with fines as high as $750 per violation

5. **New York – New York Privacy Act (S.B. 5642)**

Current status: Originally introduced in May of 2019, it has been reintroduced and was referred to the Senate Consumer Affairs and Protection Committee in January 2020.

Key provisions:

- Partially based on the GDPR; would give consumers access, correction, deletion, and portability rights, including the right to know the third parties to whom their data is sold
- Would apply to any legal entity that conducts business in New York or targets products or services to New York residents.
- Would prohibit any use, processing, or transfer of personal data without express consent
- Definition of "personal data" similar to definition of "personal information" under the CCPA
- As does the GDPR, would prohibit making decisions about consumers based solely on "automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person," unless required by federal or state law; businesses that engage in such profiling would be required to disclose their profiling to affected consumers at or before the time personal data is obtained, including meaningful information about the logic involved and the envisaged consequences of the profiling
- **Would create a private right of action for the entire law; businesses could be enjoined from conducting unlawful practices, as well as be required to pay actual damages and reasonable attorney's fees**

6. **Virginia – Virginia Privacy Act (H.B. 473)**

Current status: Introduced in January 2020 and referred to the House Committee on Communications, Technology and Innovation. On January 27, 2020, by voice vote, the bill was carried over to the 2021 session.

Key provisions:

- Primarily draws its terminology from the GDPR; resembles the Illinois Data Privacy Act described above

- Would apply to businesses that control or process the personal data of 100,000 or more Virginia residents, or that derive over 50% of their gross revenue from the sale of personal data and process or control the personal data of 25,000 or more Virginia residents
- Contains exemptions for individuals acting in an employment or commercial context, as well as for information subject to HIPAA, FCRA, or GLBA
- Consumers would have rights, upon request, to access (in a portable form), correct, delete, and object to processing; the right to object to processing includes a right to object to the use of personal data for targeted advertising
- Controllers would be required to disclose the categories of personal information they collect, the purposes for which the information is used, the categories of information shared with third parties, and the categories of third parties with whom it is shared
- Controllers would be required to conduct risk assessments of their processing activities and provide them to the attorney general upon request
- **Enforceable under the Virginia Consumer Protection Act either by the attorney general or a private party after a 30-day right to cure**
- **Private parties can recover actual damages or $500 (whichever is greater), or treble damages or $1,000 (whichever is greater) if the violation is found to be willful**

7. **Washington – Washington Privacy Act** (**S.B. 6281**)

Current status: Introduced in January of 2020, it was approved by the Senate Committee on Environment, Energy, and Technology on January 23, 2020. Referred to the Senate Ways & Means Committee, which held a hearing on January 30. The Committee materials from that hearing can be found here.

Key provisions:

- Draws on both GDPR and CCPA principles
- Would apply to any legal entity that conducts business in Washington or targets products or services to Washington residents and meets one of the following criteria:
    - during a calendar year, controls or processes personal data of 100,000 Washington consumers or more; or
    - derives 50 percent or more of its gross revenue from the sale of personal data and processes or controls personal data of at least 25,000 Washington consumers
- Like the CCPA, does not apply to information subject to HIPAA, FCRA or GLBA
- Consumers would have the right to access, correct, delete, and opt out of the processing of their personal data, as well as the right to data portability
- Obligations of data controllers would include:

    - transparency (including through privacy policy disclosures);
    - purpose specification;
    - data minimization;
    - avoiding secondary use;
    - security;
    - nondiscrimination;
    - special standards for "sensitive" data (only process with consent); and
    - non-waiver of consumer rights.
- Controllers would have to conduct data protection assessments of certain processing activities, including the sale of personal data and the processing of personal data for targeted advertising
- Would impose special requirements on controllers and processors that use facial recognition technology
- Only the attorney general could bring enforcement actions, with fines as high as $7,500 per violation

Section B. More Limited Privacy Bills

1. **California –A.B. 950**

   Current status: Introduced in February 2019 and referred to the Assembly Consumer Affairs and Protection Committee, it was carried over to the 2020 session.

   Key provisions:

   - Would require any business subject to the CCPA to disclose the "monetary value to the business" of California residents' "consumer data" (a term that is not defined)
   - Would require businesses to include in their privacy policy the average value of consumers' data and update this disclosure at least every 90 days
   - Would require businesses to disclose the average price for which they sell consumer data, and, upon request, the actual price
   - Would supplement the CCPA and be enforceable by the California attorney general under the same authority

2. **Florida – H.B. 963 / S.B. 1670**

   Current status: Introduced in January 2020; the Senate version was referred to the Commerce and Tourism Committee, Judiciary Committee, and Rules Committee; the House version was referred to the State Affairs Committee and Oversight Committee.

Key provisions:

- Would apply to anyone who "owns or operates a website or online service for commercial purposes" and "collects and maintains covered information" from Florida residents
- Entities subject to HIPAA or GLBA would be exempt
- "Covered information" includes only seven enumerated categories:
    - first and last name;
    - street address;
    - email address;
    - telephone number;
    - Social Security number;
    - "An identifier that allows a consumer to be contacted either physically or online"; and
    - Information maintained in combination with an identifier in a form that makes it personally identifiable.
- Consumers would have a right to opt out of the sale of their covered information
- The definition of "sale" requires an exchange of money for covered information, and it includes fairly broad exceptions for disclosures to processors/service providers or affiliates, or disclosures "for purposes that are consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information to the operator"
- Operators would also be required to disclose, in a reasonably accessible manner, the categories of covered information collected and the categories of third parties with whom the operator shares covered information, as well as whether a third party "may collect covered information about a consumer's online activities over time and across different websites or online services when the consumer uses the operator's website or online service"
- Contains a 30-day right to cure and does not provide a private right of action

3. **Hawaii – S.B. 2451**

Current status: Introduced in January 2020 and referred to the Senate Commerce, Consumer Protection, and Health Committee.

Key provisions:

- Would give consumers a right to opt out of the sale of their personal information
- Unlike the CCPA, a third party would be prohibited from selling or using personal information that has been sold to it unless the consumer receives explicit notice and provides express written consent

- Does not include the CCPA's broad definition of "sale," meaning that the term would likely be interpreted to have a more typical definition that requires the exchange of monetary consideration
- Enforceable under existing Hawaii statute by the attorney general or office of consumer protection, with penalties up to $2,500 per violation; **also includes private right of action for actual damages and attorneys' fees**

4. **Illinois – App Privacy Protection Act (H.B. 3051)**

Current status: Introduced in February 2019 and referred to the House Cybersecurity, Data Analytics, & IT Committee, it was carried over to the 2020 session.

Key provisions:

- 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
- Enforceable by attorney general or state's attorneys under Illinois Consumer Fraud and Deceptive Business Practices Act, including civil penalties up to $50,000
- **If attorney general and state attorneys do not bring a case, private plaintiffs may sue for injunctive relief, compensatory damages, attorney's fees, and punitive damages**

5. **Maryland – H.B. 249**

Current status: Introduced in January 2020 and referred to the House Economic Matters Committee. Hearing scheduled for February 26.

Key provisions:

- Would give consumers a right to opt out of the disclosure of their personal information
- Would apply to businesses that have annual gross revenues above $25 million, that process the personal information of 100,000 or more Maryland residents, or that derive at least 50 percent of their annual revenue from selling the personal information of Maryland residents
- Consumers would have the right to opt out of the disclosure of their personal information, including "through a setting indicating the consumer's intent to opt out of third-party disclosure, including a browser setting, browser extension, or global device setting"
- Businesses would be prohibited from disclosing to a third party the personal information of individuals the business knows or should know are under the age of 18

- Enforceable under Consumer Protection Act, which includes civil penalties of up to $10,000 for a first violation and $25,000 for subsequent violations, **as well as a private right of action for damages and attorney's fees**

6. **Massachusetts – H.B. 243**

Current status: Introduced in January 2019 and referred to the House Joint Committee on Consumer Protection and Professional Licensure. Hearing held in October 2019. Carried over to the 2020 session.

Key provisions:

- Would strictly limit the collection and use of "account numbers," defined to include Social Security numbers, driver's license numbers, license plate numbers, bank account numbers, credit card numbers, telephone numbers, and account numbers with businesses that sell goods or services
- Use of "account numbers" without prior written permission would be limited to a set of enumerated purposes, including processing transactions, verifying identity, and complying with federal or state law
- Prior written permission for other purposes could be obtained only by a paper-and-ink document and would have to be renewed annually
- The state government would be prohibited from maintaining any electronic information containing Social Security numbers, financial information, employer identification numbers, or "other confidential information" in a form that is accessible via the Internet.
- **Would create a private right of action, including the potential for class actions, a fiduciary duty, and strict liability**

7. **New Hampshire – H.B. 1236**

Current status: Introduced in January 2020 and referred to the House Judiciary Committee. Hearing scheduled for February 12.

Key provision:

- Would establish an expectation of privacy in personal information provided to "third-party providers of information and services," including cell service providers, Internet service providers, and social media companies.

8. **New York – S.B. 3036**

Current status: Introduced in February 2019 and referred to the Senate Codes Committee, it has been carried over to the 2020 session.

Key provision:

Would make knowingly making a "false or misleading" statement in an online privacy policy a Class A misdemeanor, punishable by up to 364 days in jail and/or a $1,000 fine

For more information on this or other cybersecurity and privacy 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

Ali A. Jessani + 1 202 663 6105 ali.jessani@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. Prior results do not guarantee a similar outcome. © 2004-2020 Wilmer Cutler Pickering Hale and Dorr LLP