Updates
January 27, 2021

Washington, New York, and Minnesota Introduce New Privacy Laws to Begin the New Year

It's a new year and it looks like 2021 is going to be another eventful one for privacy. In the past few weeks, we've seen several states introduce new privacy legislation, starting with Washington. On January 5, the Washington Privacy Act of 2021 (SB 5062) was introduced in the Washington State Senate and subsequently referred to the Environment, Energy & Technology Committee. SB 5062 incorporates key concepts from California's Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR), and empowers Washingtonians to control their personal data by granting new privacy rights and imposing corresponding obligations on businesses who collect and process this data. If passed, SB 5062 would take effect on July 31, 2022, with a four-year delayed effective date for higher education institutions and nonprofits.

On the other side of the country, New York introduced six privacy-related bills this month. We discuss the two most notable bills, SB S567, which amends and adds to New York's privacy laws, and the Biometric Privacy Act (AB 27), in more detail below.

Finally, Minnesota introduced a bill (HF 36) that would grant consumers new privacy rights, impose corresponding obligations on businesses, and create a private right of action and civil enforcement regime.

This update provides an overview of these bills. We expect more privacy bills will be introduced in other states this year—and possibly also at the federal level—and we will be tracking these developments closely. If you are interested in purchasing access to our Privacy Legislative Tracker, please contact us.

The Washington Privacy Act of 2021

The Washington Privacy Act of 2021 (SB 5062), modeled more closely to the GDPR than the CCPA, provides robust consumer rights and imposes affirmative obligations on companies that collect and process personal data. Further, it prohibits businesses from processing personal data in ways that would unlawfully discriminate against consumers and calls for data protection impact assessments where processing involves sensitive personal data. The proposed law also includes a new provision that regulates the processing of public health data for contact tracing during the COVID-19 pandemic.

Scope of the 2021 Bill

SB 5062 confers rights on "consumers," defined as natural persons who are Washington residents. The statutory obligations imposed apply to legal entities that conduct business in Washington or target Washington residents with their products and services provided one of the following additional thresholds apply to the business:

- Controls or processes personal data of 100,000 consumers or more
- Derives over 25% of gross revenue from the sale of personal data **and** processes or controls personal data of 25,000 consumers or more
- Excludes government entities, municipal corporations, and data collected in the employment context

Key Definitions

Like the GDPR, SB 5062 defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person." Sec. 101(23). Note, "de-identified data" and "publicly available information" are excluded from the scope of this definition.

- "De-identified data" is "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller ... (a) [t]akes reasonable measures to ensure that the data cannot be associated with a natural person; (b) publicly commits to maintain and use the data only in a de-identified fashion and not attempt to reidentify the data; and (c) contractually obligates any recipients of the information to comply." Sec. 101(12)
- "Publicly available information" is information that is lawfully made available from federal, state or local government records

Also like the GDPR, SB 5062 uses the terms "controller" and "processor." "Controller" is defined as the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data." Sec. 101(8). A "processor is a natural or legal person who processes personal data on behalf of a controller." Sec. 101(25).

Consumer Rights

SB 5062 gives Washington residents eight distinct privacy rights that can be exercised twice annually.

1. *The Right to Access* the categories of personal data processed
2. *The Right to Correct* inaccurate personal data
3. *The Right to Delete* personal data
4. *The Right to Appeal* a refusal to take action on a consumer request
5. *The Right to Portability* (i.e., to obtain personal data in a portable and readily usable format)
6. *The Right to Not to Be Discriminated Against* for exercising their rights under the law and/or in the processing of their personal data
7. *The Right to Opt In* to the processing of sensitive data (including data of children under 13 or biometric data) and data processed for unnecessary or incompatible secondary uses
8. *The Right to Opt Out* of the processing of personal data for the purposes of (a) targeted advertising; (b) sale; and (c) profiling in furtherance of decisions that produce legal (or similarly significant) effects concerning a consumer.

To exercise these rights, consumers must send to the controller a request specifying which rights they wish to exercise. A parent or legal guardian can submit such a request on behalf of a child.

Business Obligations

To support Washington consumers' new rights, SB 5062 imposes corresponding obligations on businesses. Both controllers and processors have obligations under the law. Thus, a contract that determines their respective rights and obligations is required before any processing begins. These respective rights and obligations are laid out below.

First, controllers must give consumers a privacy notice that includes (1) the categories of personal data processed, (2) the purposes for processing such data, (3) how and where consumers may exercise their rights, (4) the categories of personal data shared with third parties, (5) the categories of third parties with whom personal

data is shared, and (6) whether personal data is sold to third parties or used for targeted advertising. Sec. 107(1).

Second, controllers must comply with an opt out request within 15 days of receipt and respond to the other consumer rights within 45 days of receipt (unless it involves pseudonymized data and information necessary to identify the consumer is separate and technical and organizational controls prevent access). To do so effectively, the controller must provide one or more means for consumers to submit requests and then deliver the information requested free of charge twice a year.

Third, controllers must establish an internal process and email address or other online mechanism whereby consumers can appeal a denial of a request. Controllers can refuse to act on a request if it is manifestly unfounded or excessive, in particular due its repetitive nature. If a consumer appeals the decision, the controller must respond to the appeal within 30 days of its receipt. This period may be extended by 60 days where necessary, provided the consumer is informed before the deadline. In responding to an appeal, the controller must give the consumer information on how to file a complaint with the consumer protection division of the attorney general's office. Also, the controller must maintain records of all appeals (including how it responded to them) for at least 24 months and provide a copy of such records to the attorney general when requested.

Fourth, controllers must obtain opt-in consent to process sensitive data and data processed for unnecessary or incompatible secondary uses. Sensitive data includes, but is not limited to race, ethnic origin, religious beliefs, sexual orientation, specific geolocation data, children's data, citizenship, and genetic or biometric data.

In addition to obtaining consent, controllers must conduct data protection assessments when processing involves sensitive data. These assessments must take into account the type of personal data, including its sensitivity and the context in which it will be processed. Next, it must weigh the benefits that may flow from such processing against the potential risks to consumer rights and identify safeguards that can be employed to reduce the risks—e.g., use of de-identified data.

Fifth, controllers must not discriminate against consumers who exercise their rights and/or process personal data in ways that would unlawfully discriminate against consumers. Specifically, SB 5062 prohibits controllers from processing personal data on the basis of a consumer's actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability, in a manner that unlawfully discriminates against the consumer or class of consumers with respect to (a) housing, (b) employment, (c) credit, (d) education, or (e) goods, services, facilities, privileges, advantages, or public accommodations.

Further, controllers must not discriminate against consumers who exercise their privacy rights. Examples of discrimination include denying goods or services to the consumer, charging different prices or rates for goods or services, or providing a different level or quality of goods or services to the consumer.

Sixth, controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. These data security practices must be appropriate to the volume and nature of the personal data.

Seventh, the obligations imposed on processors are similar to those laid out in GDPR Article 28. For instance, processors must adhere to the controller's instructions, help the controller meet its security obligations and respond to consumer requests, contribute to audits and inspections, ensure employees are subject to a duty of confidentiality, give the controller an opportunity to object to subcontractors, and provide all the information necessary to demonstrate compliance with its obligations under the bill.

New COVID-19 Emergency Provisions

SB 5062 contains new provisions that regulate the processing of public health data during the COVID-19 emergency for the purposes of contact tracing. Specifically, contract tracing is the process of "detecting symptoms of an infectious disease, enabling the tracking of a consumer's contacts with other consumers, or with specific locations to identify in an automated fashion whom consumers have come into contact with, or digitally notifying, in an automated manner, a consumer who may have become exposed to an infectious disease, or other similar purposes directly related to a state of emergency." Sec. 201(9). To process such data, controllers and processors must give consumers a privacy notice and obtain consent. SB 5062 also prohibits the disclosure of such data to federal, state and local law enforcement or for sales purposes and unauthorized sharing.

Enforcement

The proposed law does not include a private right of action; rather, it would be enforced exclusively by the Washington attorney general. Violators could be liable for statutory damages of up to $7,500 for each violation. Notably, businesses are given a 30-day right to cure.

New York's Proposal S567

The CCPA appears to have been a very significant influence on New York's S567 proposal. The proposed bill would grant consumers CCPA-like privacy rights (such as access and nondiscrimination rights, in addition to the right to opt out of sales of personal information) and would impose corresponding obligations on companies that collect and process their personal information. In addition, many of the pertinent definitions in the bill—like "personal information" and "sale"—mirror the terminology in the CCPA. If S567 is enacted, companies that have developed CCPA-compliant privacy programs will likely be able to leverage much of that work for compliance in New York.

Definition of Personal Information

S567 would grant consumers new rights regarding their "personal information," which is defined as "information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including, but not limited to ... any information that identifies, relates to, describes, or is capable of being associated with, a particular individual." Enumerated data elements are "name, alias, signature, social security number, physical characteristics or description, address, electronic mail address, internet protocol address, unique identifier, account name, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

Along with the enumerated types of data elements, personal information includes a number of broader categories, which closely track the CCPA's definition of personal information. These broader categories include: "characteristics of protected classifications under state or federal law," "commercial information," "biometric data," "internet or other electronic network activity information," "geolocation data," "audio, electronic, visual, thermal, olfactory, or similar information," "psychometric information," "professional or employment-related information," "inferences drawn from any of the information identified above," and any of the foregoing as they "pertain to the minor children of the consumer." The definition of personal information expressly excludes publicly available information.

Consumer Rights and Business Obligations

Under S567, consumers would have the right to request information from businesses about the categories of personal information that the business collected, as well as the identities of any third parties to whom such personal information was sold or shared. Additionally, consumers would have the right to opt out of having their personal information sold. Businesses would be prohibited from discriminating against consumers who exercise these rights, meaning that they could not subsequently deny consumers goods or services, charge different prices or rates for goods or services, or provide a different level or quality of goods or services.

Like the CCPA, businesses would be required to provide consumers with at least two methods for exercising their rights "including, at a minimum, a toll-free telephone number, and if the business maintains a website, a website address." Businesses would also be required to respond to rights requests within 45 days.

Notably, the law also would provide consumers with the ability to opt out of "sales" of their personal information. The bill defines "sale" as "(A) selling, 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 valuable consideration; or (B) sharing orally, in writing, or by electronic or other means, a consumer's personal information with a third party, whether for valuable consideration or for no consideration, for the third party's commercial purposes." This definition largely tracks the CCPA's definition of "sale." Like the CCPA, S567 also would exclude certain instances from the definition of "sale," namely when a consumer uses the business to intentionally disclose personal information, or to intentionally interact with a third party. Also excluded would be when the business uses an identifier for a consumer who has opted out of the sale of personal information for the purpose of alerting third parties that the consumer has opted out of sales. Unlike the CCPA, the New York proposal would not expressly exclude from the definition of "sale" the transfer of personal information to a third party pursuant to a bankruptcy or other liquidation proceeding.

Private Right of Action

The law would provide a broad private right of action for violations. The proposal specifies that a violation of the law constitutes "an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this section."

Statutory damages would be $1,000 or actual damages, whichever is greater. In the case of knowing or willful violations the statutory amount would be not less than $1,000 and not more than $3,000, or actual damages, whichever is greater. When awarding damages, a fact finder could consider: the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Civil Enforcement Actions

Violations of S567 could also lead to civil enforcement actions and penalties by the state attorney general, and the proposal sets out a fairly complex civil enforcement structure. The bill would establish a "Consumer Privacy Fund," which "shall consist of all penalties received by the department of state pursuant to" any civil enforcement actions brought under the Act.

New York Biometric Privacy Act

New York's proposed Biometric Privacy Act is similar in scope to Illinois' Biometric Information Privacy Act (740 ILCS 14 *et seq.*), which has spawned over 800 putative class action lawsuits in recent years against companies across the country.

Biometric Data Covered by Proposal

New York's proposed Biometric Privacy Act (AB 27) covers "biometric identifiers"—defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"—and "biometric information"—defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."

Business Obligations

Under the proposal, "private entities" that possess biometric identifiers or information would be required to establish retention schedules for permanently destroying that information either "when the initial purpose for collecting or obtaining" that information "has been satisfied or within three years of the individual's last interaction with the private entity."

In addition, private entities may not "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" absent informed consent from the individual in writing. Private entities would also be prohibited from disclosing biometric identifiers or biometric information unless: the individual consents to the disclosure; such disclosure completes a requested financial transaction; or, the disclosure is required by legal process or applicable law. Private entities would be further prohibited from selling, leasing, trading, or otherwise profiting from a person's or customer's biometric identifier or biometric information. Finally, private entities would also be required to "store, transmit, and protect from disclosure" biometric identifiers and biometric information "using the reasonable standard of care within the private entity's industry."

Private Right of Action

The proposal would make New York the second state (after Illinois) to afford individuals a private right of action for violations involving their biometric information. The proposal includes statutory damages: negligent violations would incur $1,000 or actual damages, whichever is greater; intentional or reckless violations of the act would incur $5,000 or actual damages, whichever is greater.

Minnesota Privacy Bill

Scope of the Minnesota Bill

HF 36 is very similar to the CCPA. HF 36, for example, would impose obligations on legal entities that meet at least one of the following thresholds:

- Annual gross revenues in excess of $25,000,000
- Annually buys or sells the personal information of 50,000 or more consumers, households, or devices
- Derives 50% or more of the business's annual revenues from selling consumers' personal information

Also like the CCPA, businesses would also be subject to the provisions of the bill if they "share common branding" with a separate business, which means "a share name, service mark, or trade mark."

Definition of Personal Information

Minnesota's privacy bill, also similar to the CCPA, would define "[p]ersonal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer." The proposal expressly enumerates the following data elements as "personal information": identifiers such as a "real name, alias, postal address, telephone number, unique personal identifier, online identifier, Internet Protocol address, e-mail address, account name, Social Security number, driver's license or state identification card number, passport number, signature, or other similar identifiers."

Additional categories of personal information enumerated in the proposal include: financial information, "such as a bank account number, loan or mortgage information, income, an insurance policy, credit card number, or debit card number"; physical characteristics or descriptions; education, professional, or employment-related information; sleep, health, exercise, fitness, medical, or health insurance information; protected classifications under federal or state law; commercial information; biometric information; internet or other electronic network activity information; and, inferences drawn from any of the above information "reflecting the consumer's preferences, characteristics, traits, predispositions, behavior, attitudes, abilities, and aptitudes."

Notably, publicly available information is not mentioned in the Minnesota proposal, and so unlike other proposals the definition of personal information does not expressly exclude information that is publicly available.

Consumer Rights and Business Obligations

Under the Minnesota bill, as with the CCPA, businesses would be obligated to notify consumers "at or before the point of collection" of the categories of personal information the business collects, as well as the identities of any third parties to whom such personal information would be sold or shared.

Consumers would be given the right to access their personal information from businesses, and the right to opt out of the sale of their personal information. The proposal would provide consumers with the right to request that their personal information be deleted, although the business would not need to delete personal information "if it is necessary for the business ... to maintain the consumer's personal information in order to" complete a business transaction, detect security incidents, debug to identify and repair errors, exercise free speech, engage in public or peer-reviewed research, comply with legal obligation, or "to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."

In order to comply with these obligations, businesses would need to make available to consumers at least two methods for exercising their rights including, a toll-free telephone number and, if the business maintained a website, a website address. Businesses would need to respond to consumer rights requests within 45 days and businesses would be prohibited from discriminating against consumers who choose to exercise their rights, meaning that businesses could not deny consumers goods or services, charge different prices or rates for goods or services, or provide a different level or quality of goods or services.

The law defines the term "sell" to mean "selling, renting, releasing, 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 a commercial purpose or for any monetary or other valuable consideration." Notably, the law expressly states that "sell does not include disclose," which would vary from the CCPA in that the latter expressly defines "sell" to include "disclose." Also this bill would, like the CCPA, expressly exclude from the definition of "sale" instances where a consumer uses the business to intentionally disclose personal information, or to intentionally interact with a third party, or when he business uses an identifier for a consumer who has opted out of the sale of the consumer's personal information for the

purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information. Disclosure to a service provider is not a sale provided that certain requirements are met, and transferring personal information to a third party pursuant to a bankruptcy or other liquidation proceeding also does not constitute a sale.

Enforcement

Violations of this proposal would be enforceable by the Minnesota attorney general and would be subject to civil penalties. The law would also include a private right of action for violations of its provisions. The law would also provide for damages between $100 and $750 per violation, or actual damages, whichever amount was greater. For "malicious or willful violations," "exemplary damages in an amount not exceeding three times other damages" could be awarded.

In determining a damages award, the law enumerates certain factors that a court should consider, such as the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Authors

Miriam Farhi

Partner
MFarhi@perkinscoie.com 206.359.8195

Calvin Cohen

Counsel
CCohen@perkinscoie.com 312.263.3018

James G. Snell

Partner
JSnell@perkinscoie.com 650.838.4367

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Ryan Spear

Partner
RSpear@perkinscoie.com 206.359.3039

Explore more in

Privacy & Security Technology Transactions & Privacy Law Retail & Consumer Products

Related insights

Update

FERC Meeting Agenda Summaries for October 2024

Update

New White House Requirements for Government Procurement of AI Technologies: Key Considerations for Contractors