WILMERHALE

FEBRUARY 20, 2019

Privacy and Data Security Alert

States Consider Privacy Legislation in the Wake of California's Consumer Privacy Act

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

The enactment in June 2018 of California's sweeping new privacy law**,** the California Consumer Privacy Act (CCPA), has both increased momentum for enactment of a general federal privacy law and spurred state legislatures to consider privacy bills of their own. A series of widely publicized incidents involving major technology companies' data handling practices and the coming into force of the European Union's General Data Protection Regulation (GDPR) have increased the urgency of both efforts. This report reviews proposals at the state level for privacy legislation. A prior report reviewed proposals at the federal level.

The CCPA

On June 28, 2018, California's then-Governor Jerry Brown signed into law Assembly Bill 375, a sweeping privacy law that provides Californians with broad notice, access, and deletion rights concerning many types of personal information and that permits consumers to opt-out of the sale of their personal information. The law was introduced and passed within a week to head off a similar ballot initiative. Realizing that the CCPA was flawed and required amendments, the California Legislature adopted, and Governor Brown signed, Senate Bill 1121, also titled "the California Consumer Privacy Act of 2018," on September 23, 2018. The CCPA as amended takes effect on January 1, 2020, but the California Attorney General may not bring an enforcement action under it until six months after the publication of the final regulations described below or July 1, 2020, whichever is sooner.

Our alert on the CCPA is here, and a short summary follows.

The CCPA is the first comprehensive state privacy law, and it borrows heavily from concepts in the GDPR. It speaks broadly in defining California consumers' rights, covered businesses' obligations, and the definitions of terms such as "consumer," "personal information," "sell," and "household."

Under the CCPA, covered businesses must, upon a verified consumer's request, make disclosures regarding both the categories and specific pieces of personal information regarding the consumer, as well as the sources, uses, and sharing of the consumer's personal information. Covered businesses must also, in response to verified requests, make specific disclosures regarding the sale or disclosure of consumers' personal information "for valuable consideration." Covered businesses also may not sell consumers' personal information without giving notice and a chance for affected consumers to opt out. The CCPA's requirements do not apply to consumer information that is deidentified or in the aggregate.

Covered businesses must also place a link on their website "homepage" (defined to include all web pages where personal information is collected), titled "Do Not Sell My Personal Information," that redirects to a webpage that enables a consumer to opt out of the sale of the consumer's personal information.

In addition, covered businesses must, in response to a verified request, delete personal information of the requester and make sure service providers do as well, with certain exceptions.

The CCPA further requires that covered businesses' website privacy policies be updated to include California consumers' rights under the CCPA, and to update the privacy policy annually.

The CCPA significantly broadens the definition of personal information from existing California law to mean "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The definition includes, among other things: names and other identifiers such as IP addresses; account names; driver's license and passport numbers; commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; biometric information; internet browser and search history, interaction with a website, application, or advertisement; location information; professional or employment-related information; educational information; and inferences drawn from any of the above information to create a profile about a consumer.

The CCPA affords the California Attorney General a cause of action for violations of the CCPA, with penalties of up to $2,500 per violation and up to $7,500 for intentional violations. The CCPA also provides a private right of action for certain data breaches where the covered business did not have reasonable security procedures appropriate to the nature of the information, with liquidated damages of up to $750 per consumer per incident or actual damages, whichever is greater. There is, however, a limited 30-day right to cure provided to covered businesses to avoid such penalties.

The California Attorney General is required to promulgate regulations pursuant to the CCPA that would, among other things: (1) update the definition of "personal information" in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns; (2) update as needed the definition of "unique identifiers" to address changes in technology, data collection, obstacles to implementation, and privacy concerns; (3) define additional categories to the designated methods for submitting requests to facilitate a consumer's ability to obtain information from a covered business; and (4) establish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.

The California Attorney General's Office has held five public forums so far on the CCPA to receive input from interested stakeholders before issuing proposed rules for comment, and it plans a sixth and final public forum on March 5. The first set of written comments are due by March 8, 2019. While the CCPA requires the Attorney General to promulgate rules by July 1, 2019, the Attorney General's office has said that it will not issue proposed regulations until "the fall" of 2019. The Attorney General's Office's Power Point Slides displayed at the public forums note that the Attorney General's Office is seeking comment specifically on the following topics:

- categories of personal information;
- definition of unique identifiers;
- CCPA exemptions;
- submitting and complying with consumer requests;

- uniform opt-out logo/button;
- notices and information to consumers, including financial incentive offerings; and
- certification of consumers' requests.

Following the publication of proposed rules, the Attorney General's Office will solicit a second round of comments, which the Attorney General must consider prior to promulgating final regulations. That process is likely to come to a close after the law's effective date of January 1, 2020. If so, the Attorney General would not be able to enforce the CCPA or its regulations until July 1, 2020. If the Attorney General's final regulations are released close to July 1, 2020, industry is sure to urge an amendment to law delaying the enforcement date to give companies sufficient time to come into compliance.

Proposed State Bills

The privacy bills recently introduced in state legislatures may be grouped in two categories: those that draw on the CCPA as a model and those that do not.

- **Bills Modeled on the CCPA**

1. Hawaii – S.B. 418

Current status: The bill was introduced in January 2019 and referred to the Commerce, Consumer Protection, and Health Committee.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "identifying information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The definition of "consumer" is broader than in the CCPA; it includes any individual "who interacts with a business" in Hawaii (instead of residents of the state).
- Covered businesses would not be limited by any revenue or affected consumer thresholds.
- The CCPA's exemptions for data covered by various federal laws are omitted.
- No data breach provisions are included.

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

Current status: The Senate version was introduced in February 2019 and referred to the Finance Committee. The committee is scheduled to hold a hearing on March 8. The House version was introduced in February 2019 and referred to the Economic Matters Committee. The committee is scheduled to hold a hearing on March 6.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from third-party disclosures.
- In the definition of covered businesses, the affected consumer threshold is 100,000 users (rather than the 50,000 in the CCPA).
- In definition of "personal information," the CCPA's list of examples has been omitted, though the definition remains similar in scope. Unlike in the CCPA, personal information must relate to an individual or their device, not a household.
- The bill changes the CCPA's restrictions on "sales" to apply to "third-party disclosures."

3. Massachusetts – S.D. 341

Current status: The bill was docketed by four senators in January 2019 but has not yet been formally introduced.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The bill includes an exemption for collection and disclosure of employee personal data within the scope of its role as employer that does not appear in the CCPA.
- The annual gross revenue threshold for covered businesses is $10 million (rather than $25 million in the CCPA) and the provision including companies with more than 50,000 users is omitted.
- The bill would create a private right of action for any violation, with damages of $750 per person per incident, or actual damages.
- The Massachusetts Attorney General could seek penalties of up to $2,500 per violation and $7,500 per intentional violation.

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

Current status: The bill was introduced in January 2019 and referred to the Corporations & Transportation Committee.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The definition of "personal information" is limited to information from federal, state, or local government records.
- The bill would not apply to information collected or used pursuant to other state or federal laws if the application is in conflict with that law, as clarified in regulations issued by the Attorney General.

5. Rhode Island – Consumer Privacy Protection Act (S.B. 234)

Current status: The bill was introduced in January 2019 and referred to the Judiciary Committee.

Key provisions:

- Modeled closely on the CCPA, the bill would give consumers rights to notice of "personal information" collected and parties with whom such information is shared; deletion; and opt-out from sale.
- The annual gross revenue threshold for covered businesses is $5 million.
- The bill contains no exemptions for personal information collected or used pursuant to other laws.
- The bill contains no provisions granting rulemaking and enforcement authority to the Attorney General.

➢ **Bills Not Modeled on the CCPA**

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

Current status: The Senate version was introduced in February 2019 and referred to the Assignments Committee. The House version was introduced in February 2019 and referred to the Rules Committee.

Key provisions:

- Operators of commercial websites or online services that collect personal information about Illinois customers must, in their terms of service or privacy policy, "identify all categories of personal information the operator collects," "identify all categories of third party persons or entities with whom the operator may disclose" that information, and "provide a description of the customer's rights" to access their information.
- If a business discloses personal information to a third party, it must make available on request, free of charge, "the categories or personal information that were disclosed" and "the name or names of all third parties" that received personal information. The business can make this specific to the individual consumer's information or provide all categories and third parties for any consumer's personal information.
- The House version of the bill requires businesses to "develop a safety plan for the protection of customer data."
- The Attorney General would be empowered to enforce the law. The House version creates a private right of action, but the Senate version does not.

7. New Jersey – A.B. 4640/S.B. 3153

Current status: The Assembly version was introduced in January 2019 and referred to the Homeland Security and State Preparedness Committee. The Senate version was introduced in October 2018 and referred to the Commerce Committee.

Key provisions:

- "Operators," defined as those that own an Internet website or online service that collects and maintains personally identifiable information from a customer and that is operated for commercial purposes," would be required:
    - to provide customers, at or before the point of collection, with "(1) a complete description of the personally identifiable information that the business collects about a data subject and the means by which a business collects the personally identifiable information; (2) the purpose and legal basis for the processing of the personally identifiable information; (3) all third parties with which the business may disclose a data subject's personally identifiable information; (4) the purpose of the disclosure of personally identifiable information, including whether the business profits from the disclosure; and (5) the contact information of the person employed at the business responsible for personally identifiable information data protection;
    - to provide customers, at the time the personally identifiable information is obtained, (1) the period for which the personally identifiable information will be stored or the criteria used to determine that period; and (2) the right of the data subject to request from the business access to their personally identifiable information;
    - to provide customers, upon request, (1) confirmation that the data subject's personally identifiable information is, or has been, processed; and (2) a copy of the data subject's personally identifiable information that has been processed that the data subject can access in a structured and commonly-used machine-readable format; and

- to "opt out, in a reasonable form and manner as determined by the business, at any time during processing of the data subject's personally identifiable information," unless certain conditions are present.

- Businesses would be required to maintain an information security program meeting any applicable federal requirements or "industry standards."
- The bill would create a private right of action for consumers, with penalties of $100-$750 per person per incident or actual damages, whichever is greater, for violations leading to. "unauthorized access and exfiltration, theft, or disclosure of a data subject's personally identifiable information."

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

Current status: The Senate version was introduced in January 2019 and referred to the Consumer Affairs and Protection Committee. The Assembly version was introduced in January 2019 and referred to the Consumer Affairs and Protection Committee.

Key provisions:

- The bill would apply to "publishers," defined as "any company, individual or other group that has a website, webpage or other internet page," and "advertising networks," defined as "any company, individual or other group that is collecting online consumer activity for the purposes of ad delivery"; "online preference marketing" is defined as "a type of advertisement delivery and reporting whereby data is collected to determine or predict consumer characteristics or preferences for use in advertisement delivery on the internet."
- Publishers of a webpage or advertising networks contracted with a publisher would:

    - be prohibited from collecting personally identifiable information purposes of "online preference marketing" without the affected individual's consent;
    - be required to give affected individuals an opportunity to opt out of the collection of any other information for purposes of "online preference marketing";
    - be required to post a privacy policy conspicuously; and
    - be required to provide reasonable security for the advertising data they collect or log.

- The New York Attorney General would be empowered to seek penalties up to $250 per violation, and $750 if the company is found to have engaged in a pattern or practice of violating the law.

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

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

Key provisions:

- Owners of an Internet website, online service, online application, or mobile application "directed primarily to minors" or "that has actual knowledge that a minor is using" its facility would be required:

    - to permit minors who are users of such websites or applications to remove or request the operator of the website to remove any content that they have created or posted to the website;

- to permit users older than 21 to remove or request the operator of the website to remove any content created or posted when the user was under 21 as long as the content was created or posted no more than 20 years before the request was made; and
- to provide notice to all minors who are registered users of their removal rights and instructions on how to exercise them.

- For these purposes, removal means rendering the content no longer visible to other users of the service and the public even if the content or information remains on the operator's servers in some form.

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

Current status: The Senate version was introduced in January 2019 and referred to the Committee on Consumer Protection. The Assembly version was introduced in January 2019. It was referred to the Consumer Affairs and Protection Committee.

Key provisions:

- Businesses that retain a customer's personal information would be required "to make available to the customer free of charge access to, or copies of, all of the customer's personal information retained by the business."
- Businesses that disclose a customer's personal information to a third party would be required "to make the following information available to the customer free of charge: (1) [a]ll categories of the customer's personal information that were disclosed, . . . (2) [t]he names and contact information of all of the third parties that received the customer's personal information from the business . . . .
- The bill authorizes a private right of action as well as Attorney General enforcement.

11. Oregon – H.B. 2866

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

Key provisions:

- Organizations—whether for-profit businesses or non-profits—would not be permitted to "collect, use or store," "analyze or derive inferences from," or "sell, lease or otherwise transfer" geolocation information or audiovisual data about an Oregon resident without:

  - "obtaining express written consent" from the consumer on a dedicated form;
  - "identifying the specific items of geolocation information or audiovisual data";
  - "describing how often and the method by which" the information will be collected, used, stored, etc.; and
  - "specifying the purposes for which" the information will be collected, used, stored, etc.

- Organizations that collect, use, store, analyze, derive inferences from, sell, lease, or transfer personal information, geolocation information, or audiovisual data about an Oregon resident would be required to disclose on request, free of charge:

  - "all items" of the resident's information that have been collected, used, stored, etc.;

- "the categories into which the person has divided or organized" the information;
- the names, addresses, and contact information of any sources of the information, and of any third parties to whom the information was transferred;
- the organization's policies and procedures related to such information; and
- "the purposes for which" the information was collected, used, stored, etc.

- A violation would be classified as an unlawful business practice under Oregon law, which includes a private right of action.

12. Virginia – H.B. 2535: Digital Protections for Virginia's Minors

Current status: The bill was introduced in January 2019 and referred to the Committee on Science and Technology.

Key provisions:

- An operator of a digital service—defined as a website, online service, online application, or mobile application—directed to minors or an operator of a digital service that has actual knowledge that a minor is using its digital service would be required:
  - to permit minors who are users of the service to remove or request the operator to remove any content that they have created or posted; and
  - to provide notice to all minors who are registered users of their removal rights and instructions on how to exercise them.

- For these purposes, removal means rendering the content no longer visible to other users of the service and the public even if the content or information remains on the operator's servers in some form.
- An operator of a digital service directed to minors would be prohibited from advertising certain products on its service, including alcohol beverages; rifles, shotguns, and certain other weapons; tobacco products; and controlled substances; and would be prohibited from "knowingly us[ing], disclos[ing], compil[ing], or allow[ing] a third party to use, disclose, or compile, the personal information of a minor with actual knowledge that the use, disclosure, or compilation is for the purpose of marketing or advertising products or services to that minor for a restricted product or service.

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

Current status: The Senate version was introduced in January 2019 and referred to the Committee on Environment, Energy and Technology, which held a hearing on January 22. A substitute Senate version was introduced in February 2019 and referred to the Ways and Means Committee. The House version was introduced in February 2019 and referred to the Technology and Economic Development Committee, which held a hearing on February 12.

Key provisions:

- The bill would apply only to "legal entities" that either control or process data of at least 100,000 Washington consumers or that derive more than 50% of their gross revenue from the sale of personal information and process or control at least 25,000 Washington consumers.
- Like the CCPA, there are exemptions in the bill for data covered by other federal or state privacy laws, such as HIPAA and GLBA.

- Like the GDPR, the bill distinguishes between "controllers," which "determine[] the purposes and means of the processing of personal data," and "processors," which "process[] data on behalf of the controller." Controllers are "responsible for meeting the obligations under this act"; processors "are responsible . . . for adhering to the instructions of the controller and assisting the controller to meet its obligations."
- On request, controllers would be required:
    - to "confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data";
    - to "provide a copy of the personal data undergoing processing";
    - to "correct inaccurate personal data concerning the consumer" without undue delay;
    - to "delete the consumer's personal data without undue delay" in a number of circumstances and "take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data";
    - to "restrict processing" of the consumer's personal data in various circumstances; and
    - to "provide the consumer any personal data concerning such consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format" if certain conditions apply.
    - In the Senate bill, these requirements only apply to personal data "that the controller maintains in identifiable form." The requirement to notify other controllers is also limited to controllers "of which [the business] is aware."

- The Senate version of the bill would require controllers to respond to consumer requests within 30 days of receipt, which could be extended by 60 additional days where reasonably necessary.
- The bill would prohibit subjecting consumers to "a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer" unless the consumer consents or the decision-making is legally required.
    - Legal or similarly significant effects "include, but are be limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services."

- The bill would establish a group of restrictions on the use of facial recognition technology:
    - Controllers "must obtain consent from consumers prior to deploying facial recognition services";
    - "Providers of commercial facial recognition services that make their technology available as an online service for developers and customers to use in their own scenarios must make available" an API or other technical capability chosen by the provider, to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of those facial recognition services for accuracy and unfair bias";

    - Controllers "using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects concerning consumers or similarly significant effects concerning consumers";
    - Processors "that provide facial recognition services must prohibit, in the contract required by section of this act, the use6 of such facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers"; and
    - State and local government agencies would be prohibited from using "facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces, unless such use is in support of law enforcement activities and either (a) a court order has been obtained to permit the use of facial recognition services for that ongoing surveillance; or (b) where there is an emergency involving imminent danger or risk of death or serious physical injury to a person."

- Controllers must publish privacy notices that are "reasonably accessible to consumers" in a "clear, meaningful" form that "includes: (a) The categories of personal data collected by the controller; (b) The purposes for which the categories of personal data is used and disclosed to third parties, if any; (c) The rights that consumers may exercise pursuant to section 6 of this act, if any; (d) The categories of personal data that the controller shares with third parties, if any; and (e) The categories of third parties, if any, with whom the controller shares personal data."

    - Controllers that sell personal data to data brokers or use personal data for direct marketing must disclose such processing and provide an opportunity for consumers to object.
    - In the House version of the bill, controllers that engage in profiling "must disclose such profiling to the consumer at or before the time personal data is obtained, including meaningful information about the logic involved and the significance and envisaged consequences of the profiling."

- Controllers "must conduct and document risk assessments covering the processing of personal data prior to the processing of such personal data whenever there is a change in processing that materially impacts the risk to individuals," and they must make risk assessments available to the Attorney General upon request. The House version of the bill would require risk assessments to be completed at least annually.
- "A controller or processor that uses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments."
- The Attorney General would be authorized to enforce the law, and violations would be defined as unfair trade practices.
- The bill would establish an "office of privacy and data protection" in the office of the state chief information officer "to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection."

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

Current status: The bill was introduced in February 2019 and referred to the Innovation, Technology and Economic Development Committee. The committee held a hearing on February 20.

Key provisions:

- The bill would apply to "the processing of personal data in the context of the activities of an establishment of a processor in Washington state, regardless of whether the processing takes place in Washington state" or to "the processing of personal data of data subjects who reside in Washington state by a processor not established in Washington state," if the latter relates to the "offering of goods or services" or "monitoring of data subject's behavior" within the state.
- The bill's requirements refer to "processors," but would apply to both processors and controllers in most circumstances.
- Processors would be required to provide "timely and conspicuous notice, in clear and concise language, about the processor's privacy and security practices."
    - The notice would be required to be provided in three languages, and would need to include what data is collected, the sources and purposes of collection, categories of parties with which the data is shared, retention policies, and security measures.
    - Consumers would have to be given "a meaningful opportunity to access their personal data and grant, refuse, or revoke consent for the processing of personal data."
- Companies that sell or monetize data would be required to "inform data subjects in a timely and conspicuous manner of each agreement or transaction" and "provide data subjects convenient and reasonable access to a record of all agreements and transactions."
    - Upon request, they would need to disclose the specific categories of data sold or monetized and the persons receiving it.
- The Attorney General would be empowered to enforce the law, with restitution of at least $1,000 per consumer and civil penalties of up to $10,000 per violation ($15,000 for violations related to sale or monetization of data).

➢ **More Limited or Undeveloped Privacy Bills**

15. Other Bills

- In **Arizona**, H.B. 2259 was introduced in January 2019. It would require any commercial website that collects information from any person with more than 500 users to create a portal through which users could gain access to and correct their personal information.
- In **California**, A.B. 288 was introduced in January 2019. It would require social media sites to give users who close their accounts the option to permanently delete their data and exclude it from sale.
- In **Connecticut**, H.B. 6601 was introduced in February 2019 and referred to the Joint Committee on Children. There is not yet a full text available. The bill would require social media platforms to enable minors to request removal of content they created.
- In **Montana**, H.B. 457 was introduced in February 2019 and referred to the Judiciary Committee. It would require "affirmative express opt-in consent" for an Internet service provider to "use, disclose, sell, or permit access to a customer's personal information."
- In **New Jersey**, S.B. 2634/A.B. 3923 was introduced in January 2019. It would require owners of commercial websites that collect and maintain personally identifiable information from consumers to post a privacy policy conspicuously.

The Senate version was referred to the Commerce Committee, and the Assembly version was referred to the Science, Innovation and Technology Committee.

- In **New York**, S.B. 518/A.B. 2420 was introduced in January 2019 and referred to the Consumer Protection Committee. It would prohibit Internet service providers (ISP) from knowingly disclosing personally identifiable information resulting from the consumer's use of the telecommunications service or ISP without express written approval from the consumer.
- In **New York**, S.B. 1180 was introduced in January 2019 and referred to the Consumer Protection Committee. It would require ISPs operating in New York to honor a consumer's request that the ISP refrain from sharing, selling, providing or in any way disclosing to a third party any of his or her personally identifiable information.
- In **North Dakota**, H.B. 1485 was introduced in January 2019 and reported out of the Joint Industry, Business, and Labor Committee. It was originally drafted as a comprehensive privacy law, but was amended simply to require "legislative management" to undertake a study of "protections, enforcement, and remedies regarding the disclosure of consumers' personal data."

Conclusion

WilmerHale's Cybersecurity and Privacy Practice will continue to track and provide periodic reports on the development of state privacy legislation over the course of 2019.