DAVIS GILBERT

Privacy + Data Security

Iowa Becomes the 6th State to Pass Comprehensive Consumer Privacy Legislation

The Bottom Line

- Iowa has become the sixth state to enact a comprehensive privacy law, but certainly will not be the last.
- Similar to Utah's forthcoming law, Iowa's statute has many features that are more business-friendly than the laws in California, Virginia, Colorado and Connecticut.

Not to be outdone by California, Virginia, Colorado, Utah and Connecticut, Iowa is the sixth U.S. state to enact a comprehensive consumer privacy law. Gov. Kim Reynolds signed An Act Relating to Consumer Data Protection, Providing Civil Penalties, and Including Effective Date Provisions (ICPA) into law on March 29, 2023. The new law will take effect on Jan. 1, 2025.

Threshold Requirements

The ICPA applies to any person that conducts business in the state or produces products or services targeted to state residents, and that controls or processes the personal data of at least:

- 100,000 consumers during a calendar year or
- 25,000 consumers and derives over 50% of gross revenue from the "sale" (defined below) of personal data.

Unlike the California Consumer Privacy Act (CCPA) and Utah Consumer Privacy Act (UCPA), but similar to the Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA) and Connecticut Data Privacy Act (CTDPA), there is no revenue threshold that companies must satisfy to be governed by the ICPA.

Consumer Rights

The ICPA provides consumers with rights of access, deletion, data portability and to opt out of sales of personal data. It

also implicitly includes the right to opt out of targeted advertising (although not expressly listed as a consumer right, privacy notices must "clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity").

In line with the VCDPA and UCPA, the ICPA narrowly defines the "sale" of personal data as "the exchange of personal data for monetary consideration by the controller to a third party," excluding non-monetary forms of consideration from the definition. Similar to the UCPA and in contrast to the other four state laws, the ICPA does not include a right to correction and its right to deletion is limited to personal data that the consumer provided directly to the controller. The ICPA also does not give consumers the right to opt out of profiling, which the VCDPA, CPA and CTDPA do allow. Additionally, the ICPA follows the VCDPA and UCPA in that it does not recognize opt-out preference signals (such as global privacy controls) as a method for consumers to exercise their opt-out rights.

One additional feature unique to the ICPA is that consumer privacy rights are subject to an exemption with regard to "pseudonymous data." The ICPA defines "pseudonymous data" as "personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person."

Duties for Controllers

The ICPA obligates controllers to uphold many of the same duties proscribed under the other five state privacy laws, including adopting reasonable data security practices, providing a reasonably accessible privacy notice and not discriminating against consumers for exercising their rights.

Unlike the VCDPA, CPA and CTDPA, but similar to the UCPA, the ICPA does not require that controllers conduct "data protection assessments." Moreover, while the ICPA's requirements for data protection agreements are stricter than the UCPA (which does not require the processor to delete or return all personal data to the controller, or make available to the controller all information necessary to demonstrate compliance), the ICPA is more lenient than the VCDPA, CPA and CTDPA in that it does not require processors to submit to audits or assessments by the controller.

Sensitive Data

The ICPA's definition of "sensitive data" largely mirrors the VCDPA, CPA, UCPA and CTDPA, as it includes personal data that reveals an individual's racial or ethnic origin, religious beliefs, sexual

orientation, citizenship or immigration status, and mental or physical health diagnosis. However, unlike those laws, the ICPA does not deem such data "sensitive" if used to avoid "discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law." Sensitive data also includes genetic and biometric data processed for the purpose of uniquely identifying a natural person, data collected from a known child and precise geolocation data (accurate within a radius of 1,750 feet).

Similar to the UCPA, controllers cannot process sensitive data collected from a consumer without providing a "clear notice and an opportunity to opt out of such processing." The VCDPA, CPA and CTDPA, by contrast, follow an opt-in consent standard for processing sensitive data, while the CCPA provides a more limited right to limit the use and disclosure of such information.

Enforcement

The Iowa Attorney General has exclusive authority to enforce the ICPA, and there is no private right of action. Violations of the ICPA are subject to a fine of up to $7,500 per violation. However, prior to initiating an enforcement action, the Iowa Attorney General must offer violators a 90-day notice-and-cure period. This is the longest notice-and-cure period offered by any of the state privacy laws — Virginia and Utah offer 30 days while Colorado and Connecticut offer 60 days. Moreover, echoing Virginia's and Utah's laws, there is no expiration date on the ICPA's notice-and-cure period. As such, the ICPA is among the more lenient of the state privacy laws with regard to enforcement.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com