DORSEY
DORSEY+WHITNEY LLP

Utah's New Privacy Law: Will This New Balance Become the Norm?

Related Capabilities

- Privacy & Social Media

Governor Spencer Cox of Utah has now signed into law the Utah Consumer Privacy Act ("UCPA"), which was recently passed unanimously by the Utah legislature, and which will go into effect on December 31, 2023. Utah joins California, Colorado, and Virginia as the fourth state to enact a comprehensive privacy law. Of the three aforementioned states, the UCPA most closely parallels the Virginia Consumer Data Privacy Act ("VCDPA") and the Colorado Privacy Act ("CPA"), following what appears to be the trend toward less-ambitious privacy laws as compared to the hallmark California Consumer Privacy Act ("CCPA").

What Does the UCPA Do?

Application. The UCPA applies to any controller or processor who

1. *Conducts business* in the state of Utah *or* produces products or services *targeted toward consumers* who are Utah residents;
2. Has an *annual revenue of $25 million* or more; and either
3. Processes or controls *personal data of 100,000 or more Utah citizens or* derives more than *50% of its gross revenue* from processing or controlling the *personal data* of *25,000 or more Utah consumers*.

Exemptions. The UCPA does *not* apply to government entities, tribes, higher education institutions, or nonprofit corporations; nor to information or covered entities or business associates governed by the federal Health Insurance Portability and Accountability Act ("HIPAA"), financial institutions and information under the umbrella of the Gramm-Leach-Bliley Act ("GLBA"), information subject to the Federal Credit Reporting Act ("FCRA"), and personal data regulated by the Family Educational Rights and Privacy Act ("FERPA"). The language of the UCPA further exempts entities such as consumer reporting agencies and their affiliated activities, among other delineated exemptions.

Rights of Consumers. UCPA grants consumers certain privacy rights, as follows:

- *Access* – the right to know whether a controller is processing their personal data and access their personal data;
- *Deletion* – the right to delete the personal data that the consumer provided to the controller;
- *Portability* – the right to obtain a copy of their personal data in a format that is portable, readily usable, and allows the consumer to transmit the data to another controller without impediment; and
- *Opt out* – the right to opt out of the processing of their personal data if used for targeted advertising or the sale of personal data.

Controllers shall provide a process for consumers to exercise their rights. Consumers, in their requests, must specify the right they intend to exercise, and controllers are expected to respond within forty-five days of receipt of any request. Controllers may extend the forty-five day deadline, but must communicate the justification to the consumer. There are no fees for information requested or provided in response to a request, unless the request is deemed duplicative, or harassing toward or unduly burdensome on the controller.

Obligations of Controllers. Controllers have the following obligations and responsibilities:

- *Transparency, purpose specification,* and *data minimization* – A controller shall provide consumers with a reasonably accessible and comprehensive privacy notice that includes (1) the categories of personal data processed; (2) the purposes for which the personal data is processed; (3) how and where consumers may exercise a right; (4) the categories of personal data that the controller shares with third parties; and (5) the categories of third parties with whom the controller shares personal data;
- *Consent for secondary use* – A controller may not process sensitive consumer information without first presenting the consumer with clear notice and an opportunity to opt out;
- *Security* – A controller must maintain appropriate data security practices to protect the personal data and reduce risks of harm to the consumer relating to the processing of the data;
- *Nondiscrimination* and *nonretaliation* – A controller may not discriminate against a consumer for exercising a right; and
- *Nonwaiver of consumer rights* – Any provision of a contract purporting to limit or waive a consumer's right under the UCPA is void.

Enforcement. Violations are *only* enforceable by the Utah Attorney General's office. Before the Attorney General can initiate an enforcement action, the controller is entitled to a *thirty-day cure* or safe harbor period, with written notice explaining the basis of the allegation and giving the controller the opportunity to remedy it.

As Compared to Other Existing Privacy Laws

The VCDPA, CPA, and UCPA have a significant number of elements in common, but also some important differences. The key commonalities include:

- No private right of action, (in contrast to the CCPA's private right of action for data breaches);

- Comparable definitions of “personal data”; and
- Right to cure period of thirty days (the same as Virginia; Colorado has sixty-day cure period, and California’s thirty-day cure period is slated for repeal in 2023).

Departing from the VDCPA and CPA, the UCPA and the CCPA have in common:

- No right of appeals if a controller declines a consumer request (CPA and VCDPA require a process for which consumers can appeal any refusal).

Unlike other state privacy laws, the UCPA:

- Does not require data protection assessments (“DPA”);
- Does not provide a right of correction/accuracy to consumers;
- Allows consumer opt-outs only for targeted advertising and sale of personal data; and
- Provides consumers a narrow deletion right that applies only to personal data that the consumer provided to the controller.

Interaction with Utah’s Cyber Safe Harbor

The UCPA’s obligation to maintain appropriate data security practices to protect the personal data and reduce risks of harm to the consumer offers an interesting, and important, complement to Utah’s Cybersecurity Affirmative Defense Act (referred hereafter as the “Utah Safe Harbor” or the “Safe Harbor”), signed into law last year on March 11, 2021, which provides an affirmative defense to claims arising out of a breach of security to businesses with a written cybersecurity program.

Simply summarized, Utah businesses now have an even greater incentive to take the relatively straightforward steps necessary to qualify for Safe Harbor, which include:

1. creating, maintaining, and reasonably complying with a *written cybersecurity program* meeting certain minimum requirements; and,
2. protocols to provide notice to individuals about security breaches.

In order to meet the minimum technical requirements, a written cybersecurity program must conform to certain recognized cybersecurity frameworks, such as the National Institute of Standards and Technology (“NIST”) and the International Organization for Standardization (“ISO 27000”) among others. Compliance with the privacy standards outlined in HIPAA or GLB or any other applicable federal or state regulation—including the recently enacted UCPA—can also qualify under Safe Harbor.

Best Practices Going Forward

As more states consider enacting their own privacy laws, understanding the applicability of, and complying with, the various state laws that apply to them will become increasingly challenging for companies with multi-state operations. A standing ‘change of law’ process for such companies will be an essential part of doing business. Companies that collect or process personal information of consumers in Utah should ensure that they:

1. Know what personal data is being collected and what “category” this data falls under;
2. Know how the personal data is being processed, including the purpose for which it is being processed;

3. Know with whom the personal data is being shared and what “category” potential third-parties fall under;
4. Draft the appropriate disclosures, paying close attention to the specific notice requirements that the legislations outline;
5. Develop processes and procedures for facilitating and responding to consumer requests, whether these requests are for personal information or to opt out of having personal information processed at all; and
6. Document and reassess each of these elements on an annual basis.

As you navigate the rapidly developing privacy landscape, please do not hesitate to reach out to your Dorsey privacy counsel for further guidance and information.