WHAT YOU NEED TO KNOW ABOUT UTAH'S PRIVACY BILL

Eliza Davis

Aviva Surugeon

Over the past few years, many states have struggled to move a comprehensive consumer privacy bill forward. Last week, it came with some surprise that it only took Utah five working days to unanimously approve the Utah Consumer Privacy Act (UCPA). The UCPA is modeled on and shares many similarities with the Virginia Consumer Data Protection ACT (VCDPA). While the bill still requires concurrence with the Senate before heading to Governor Spencer Cox's desk, here are some important points to know about the pending legislation.

To Whom Does It Apply?

The UCPA would apply to businesses with annual revenue of $25,000,000 or more that conduct business in Utah or produce products or services that target Utah residents and that:

- Control or processes personal data of 100,000 or more consumers; or
- Derive over 50% of gross revenue from the sale of personal data of more than 25,000 consumers.

Notably, the UCPA does not apply to, among others:

- Government entities;
- Higher Education institutions;
- Non-profits;
- Businesses that are covered entities pursuant to HIPPA; and
- Information subject to HIPAA, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, or the Drivers Privacy Protection Act.

Scope

The UCPA defines personal data as "information that is linked or reasonably linked to an identified individual or an identifiable individual." The UCPA specifies that deidentified data, aggregated data, or publicly available information does not constitute personal data. Under the UCPA, publicly available information is "information that a person (a) lawfully obtains from a record of a governmental entity, (b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public, or (c) if the consumer has not restricted the information to a specific audience, obtains from a person to

whom the consumer disclosed the information." In addition, the UCPA, like the VCDPA, defines sale as the "exchange of personal data for monetary consideration by a controller or a third party."

Consumer Rights

Similar to the VCDPA, the UCPA provides consumers with several rights, including:

- Right to confirm whether a controller is processing the consumer's personal data;
- Right to obtain a copy of consumer's personal data that the consumer previously provided to the controller;
- Opt-out of the processing of personal data for purposes of targeted advertising or the sale of personal data; and
- Data deletion.

Exercising Consumer Rights

A consumer may exercise a right by submitting a request to a controller, specifying which right the consumer intends to protect. Once a consumer submits a request, the controller has 45 days to:

- Take action on the consumer's request and inform the consumer of any action taken; or
- Inform the consumer of any reasons the controller is not taking action in response to the consumer's request; or
- Extend the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity or volume of the consumer's request and inform the consumer of the reason and length of the extension.

A controller may not charge the consumer a fee in response to the request, unless it is the consumer's second request in a 12-month period. A controller may, however, charge a "reasonable fee to cover the administrative costs of complying with the request."

Data Controller Obligations

Similar to the European General Data Protection Regulation, the UCPA establishes "controller" and "processor" roles, which differentiate how entities handle personal data. Controllers are those who determine the purposes and means of processing personal data, while processors are entities that process personal data on behalf of a controller and at the controller's direction. The law assigns different obligations based on an entity's status as a controller or processor. The UCPA imposes several obligations on controllers, including:

- Providing consumers with privacy notices;
- Establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices to protect confidentiality, integrity, and accessibility of personal data; and
- Outlining contractual requirements in engaging data processors.

Sensitive Data

Under the UCPA, controllers are prohibited from processing "sensitive data" without first giving the consumer explicit notice and providing an opportunity to opt-out of processing. Sensitive data includes:

- Racial or ethnic origins;
- Religious beliefs;
- Sexual orientation;
- Citizenship/immigration status;
- Biometric information; and
- Health information

Enforcement

Similar to the VCDPA, the UCPA does not provide for a private right of action. However, unlike VCDPA, which grants enforcement authority solely to the Attorney General, the UCPA provides for a bifurcated enforcement scheme. First, the Utah Department of Commerce Division will investigate companies based on consumer complaints, and it then sends cases it deems legitimate to the Attorney General's office. Before initiating an enforcement action, the Attorney General must first provide the business with (1) written notice 30 days before and (2) an opportunity to cure within 30 days from receipt of the notice.

Next Steps

The UCPA was first introduced and passed in the Senate and then passed in the House with amendments. It must now be sent back to the Senate for concurrence. If the Senate accepts the amendments, the bill will be sent to the Governor for action. The Governor has 20 days to sign or not sign, after which time the bill becomes law. Or the Governor may veto the bill. In a matter of days, Utah has taken a significant step towards becoming the next state to pass a comprehensive privacy law. Redgrave LLP will continue to monitor and report on any new developments.

For additional information on this topic, please contact the authors **Eliza Davis** and **Aviva Surugeon.** For further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*