UTAH BECOMES FOURTH STATE TO PASS CONSUMER PRIVACY ACT, FIRST WITH REPUBLICAN-CONTROLLED HOUSE AND SENATE

On March 24, 2022, Utah Governor Spencer Cox signed the Utah Consumer Privacy Act (UCPA) into law, making Utah the fourth state to pass a comprehensive consumer privacy law, and the first in a state with a Republican-controlled legislature. Though the law shares many similarities with those passed in Colorado, Virginia, and California, its narrow scope and lack of a private right of action make it potentially less onerous for businesses. The Act goes into effect on December 31, 2023.

Key issues

- Utah became the fourth state to enact a comprehensive consumer privacy law.
- The statute overlaps in certain respects with other recent state consumer privacy protection legislation but is narrower in scope, and potentially more business friendly.
- The Utah Division of Consumer Protection can investigate claims and refer legitimate claims for further investigation by the state Attorney General's office. Businesses have 30 days in which to rectify alleged violations before the attorney general can bring an action against them.
- The law does not provide for a private right of action.

OVERVIEW OF THE ACT

Scope: Which Companies Must Comply

The act applies to companies that conduct business in the state of Utah and which:

- Have an annual revenue of $25 million or more AND
    - Control or process personal data of 100,000 or more Utah consumers; OR
    - Derive over 50% of their gross revenue from the sale of personal data, and control or process data of 25,000 or more Utah consumers.

The UCPA applies more narrowly than similar acts in other states by limiting its application to companies that meet a minimum threshold of both their annual revenue and the number of Utah residents whose personal data they process. This means the law will only apply to relatively large companies. As a point of comparison, the California Privacy Rights Act applies to business that meet either a revenue or resident threshold. The difference is magnified given California's resident population is over ten times that of Utah.

Like the privacy laws passed in other states, the USCPA does not define what it means to "conduct business" in Utah, creating some uncertainly for companies

considering whether they fall within the scope of this law, though the data processing volume thresholds specific to the USCPA provide some additional clarity and will likely capture fewer business entities than laws in other states.

Exemptions: What Data is Not Covered

There are numerous exemptions to the types of data covered by the UCPA. For example, the UCPA:

- does not apply to personal data already protected by other laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) (including data collected by health institutions) and the Gramm-Leach-Bliley Act (including data collected by financial institutions).;
- provides carve-outs for certain types of data used by credit and consumer reporting agencies;
- does not apply to personal data processed in the context of employment or business-to-business transactions; and
- does not apply to several broad categories of entities, including tribes, intuitions of higher learning, nonprofits, and government entities(or third parties contracting with governmental entities and acting on the governmental entity's behalf).

Notably, while most of these exemptions are present in similar form in the privacy laws of California, Colorado, and Virginia, the UCPA's exemption for tribes and government contractors are new.

In addition to these exemptions, the UCPA also explicitly protects controllers, processors, third parties and consumers from being compelled to disclose trade secrets.

Consumer Rights

The UCPA establishes four main consumer personal data rights:

- The right to confirm whether a company is processing their personal data and to **access** that data;
- The right to **request deletion** of their personal data that the consumer provided;
- The right to **opt-out** of the processing of their personal data for targeted advertising or sale;
- The right to **obtain a copy of** their data in a form portable and readily usable, to the extent technically feasible and practicable.

The UCPA does not include a consumer "right to correction," which other recent state laws provide, which would allow consumers to correct inaccuracies in their personal data.

Duties of Controllers: Procedural Safeguards

The UCPA requires "controllers" to implement a number of procedural safeguards to protect the consumer rights created by the law. A controller is defined in the law as the entity that determines the purposes and means of data processing.

The procedural safeguards include the requirement to provide a "reasonably accessible and clear" privacy notice indicating the types of data collected by a controller and how that data will be used. Further, controllers are required to "conspicuously disclose" how a consumer can opt-out of the sale of data or processing for the purpose of targeted advertising, if the controller sells personal data to one or more third parties or engages in targeted advertising.

The UCPA defines sale similarly to Virginia, meaning the "exchange of personal data for monetary consideration by a controller to a third party," a definition which is narrower than those used in the California and Colorado legislation. Importantly, the UCPA does not consider a sale to include instances in which a controller discloses data to a third party if the purpose of the disclosure is consistent with a consumer's reasonable expectations at the time the consumer initially provided the data to the controller.

In addition to the consumer-directed notice requirements addressed above, **controllers** must engage in reasonable efforts to protect the confidentiality and integrity of any personal data collected and proactively reduce foreseeable risks of harm to consumers as a result of data processing. Data security practices should be in-line with the size, scope, and type of the business collecting the data.

Unlike similar laws in other states, the UCPA does not require covered entities to conduct data processing assessments in which the risks of processing data are weighed against the benefits of processing it.

Duties of Controllers: Sensitive Data

Controllers may not process sensitive data collected from consumers without first presenting the consumer with clear notice and opportunity to opt-out of the processing or, in the case of sensitive data involving a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act. This is different from the Virginia and Colorado state consumer privacy protection acts which require affirmative consumer consent before processing sensitive data.

The Act defines **sensitive data** as personal data that reveals:

- An individual's race or ethnic origin (not including data processed through a video communication service);
- Religious beliefs;
- Sexual orientation;
- Citizenship or immigration status; or
- Information regarding medical history, mental or physical health conditions, or medical treatment or diagnosis by a health care professional (not including data processed by persons licensed to provide health care under Title 26 or Title 28).

Duties of Controllers: Responding to Rights Requests

Controllers must comply with a consumer's request to exercise a right conferred by the act within **45 days**. They must then take action and inform the consumer of any actions taken. If a request is particularly complex or burdensome, the controller may extend the response period to a total of 90 days. The UCPA does not require a controller to engage in an appeals process if it denies a consumer's request related to personal data, as is required by Virginia's law.

Under certain circumstances, a controller may charge a **fee** in response to a consumer's request, including if the consumer makes two or more requests during the same 12-month period, or to cover the administrative costs of complying with a request of the request is excessive, repetitive, technically infeasible, or unfounded. Unlike other state laws, Utah permits businesses to charge a fee if the business reasonably believes the primary purpose for submitting the request was something other than the exercise of right, like harassment or disruption.

Further, controllers must not discriminate against consumers for exercising rights, such as denying a good or service to the consumer or charging a different price or rate for a service. However, if a consumer has opted out of targeted advertising or an offer is related to voluntary participation in a loyalty or other discount program, the controller may offer a different price or rate. Controllers are not required to provide a good or service if a consumer's personal data (or processing that data) is necessary for the controller to provide the good or service and the consumer has not provided the data or does not consent to it being processed.

Duties of Processors

Processors are required to adhere to controller's instructions and assist the controller in meeting the controller's obligations, including those related to the security of processing personal data and notifications of security breaches. The UCPA defines "processor" as any entity who processes personal data on behalf of a controller.

Before processing any data, processors must enter a contract that:

- Clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of processing, and the rights and obligations of parties;
- Requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the data; and
- Requires the processor to engage any subcontractor pursuant to a written contract outlining the same obligations.

While the requirements imposed on processors are in many ways similar to the privacy protection acts in other states, they are less onerous, for example by imposing no duty to participate in controller-led audits as called for in the Virginia and Colorado laws.

Penalties and Enforcement

The UCPA employs a bifurcated structure to enforce the rights it creates. First, the **Division of Consumer Protection** within the Utah Department of Commerce will investigate consumer complaints to determine whether a controller or processor violated the act. Claims that the director of the division deems legitimate may then

be referred to the state **attorney general**, who has the exclusive authority to enforce the act. The act does not create a **private right of action**.

Controllers or processors suspected of violating the UCPA will have an opportunity to cure their noncompliance. At least 30 days before commencing an enforcement action, the attorney general must provide written notice to the controller or processor suspected of violating the act. That entity will have 30 days after the day on which the entity receives written notice from the attorney general in which to cure or rectify the alleged violation. Penalties include actual damages to the consumer and up to $7,500 in fines for each violation. If one or more controller or processor is involved in the same processing violation, the penalty will be shared equally among the parties in line with comparative fault.

By mediating the claims process through two different state agencies, businesses will have ample opportunity to explain alleged violations or to cure processing deficiencies identified by the Division of Consumer Protection and/or by the attorney general before they will face any fines or penalties. At the same time, by conferring the Division of Consumer Protection the ability to investigate and refer alleged violations to the attorney general, Utah's legislature has effectively expanded the capacity of the attorney general's office to investigate violations and turn its attention to the most noteworthy.

CONCLUSION

Utah's Consumer Privacy Act is the fourth such bill nationwide but is unlikely to be the last, particularly as businesses reengage in the aftermath of the pandemic and regulatory authorities turn their attention toward Big Tech. Concerns over new Web 3.0 technologies and massive sectoral developments in corporate structure (e.g., Facebook rebranding as Meta) will lead to heightened scrutiny as regulators and consumers alike seek to assign liability for breaches and perceived shortcomings.

Utah's law is narrower in scope than other recent legislation, conferring relatively fewer rights and more procedural protections for businesses. As other states join the movement toward greater personal data protection, multistate businesses must engage in comprehensive compliance programs to navigate the challenges resulting from varying state standards, particularly in the absence of federal minimums.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Thomas Chapman
Associate

T +1 202 912 5921
E thomas.chapman@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA