April 27, 2022

Utah Consumer Privacy Act

Utah Is the Fourth State in the U.S. to Enact Comprehensive Privacy Legislation

SUMMARY

On March 24, 2022, Utah enacted the Utah Consumer Privacy Act (the "UCPA"), which will go into effect on December 31, 2023.

The UCPA imposes a number of obligations on businesses that control or process the personal data of Utah consumers, and grants these consumers a range of new rights over the personal data that they previously provided to a business. Under the UCPA, Utah consumers have the right to: (1) know or confirm processing activity; (2) access personal data; (3) obtain a copy of personal data in a portable and readily usable format; (4) delete personal data; (6) opt out of targeted advertising and sales of personal information; and (7) avoid discrimination as a result of exercising their consumer rights under the UCPA. Importantly, the UCPA does not create a private right of action for consumers and is only enforceable by the Utah Attorney General.

The UCPA applies to any entity that (1) conducts business in Utah, or produces products or services that are targeted to Utah residents; (2) has annual revenue of $25 million or more; and (3) annually controls or processes the personal data of at least 100,000 Utah residents, or controls or processes the personal data of at least 25,000 Utah residents and derives over 50% of its gross revenue from the sale of personal data.[1]

The UCPA is similar to other state legislation addressing privacy, especially the Virginia Consumer Data Protection Act (the "VCDPA") and the Colorado Privacy Act (the "CPA"). But, unlike the VCDPA and the CPA, the UCPA applies only to companies with annual revenue of at least $25 million and mandates less stringent requirements, such as the lack of a requirement to conduct data protection assessments for certain types of processing activities. The UCPA also provides for some consumer rights similar to those provided by the California Consumer Privacy Act of 2018 (the "CCPA") and the recently enacted California

Privacy Rights Act of 2020 (the "CPRA") and borrows various concepts from the European Union's General Data Privacy Regulation (the "GDPR").

BACKGROUND

The UCPA passed with overwhelming support in the Utah State Legislature, receiving unanimous votes in both chambers.[2] Governor Spencer Cox signed the legislation into law on March 24, 2022, making Utah the fourth state (after California, Virginia, and Colorado) to enact a comprehensive data privacy framework.[3]

A. KEY PROVISIONS

1. Categories of Rights

The UCPA grants Utah residents acting in an individual or household context ("consumers") six categories of rights:

- The Right to Know: Consumers have the right "to confirm whether a controller is processing the consumer's personal data";[4]
- The Right to Access: Consumers have the right to access their personal data;[5]
- The Right to Deletion: Consumers have the right to "delete the consumer's personal data" that they provided to a controller;[6]
- The Right to a Copy: Consumers have the right to "obtain a copy of the consumer's personal data that the consumer previously provided to the controller" in a portable and readily usable (if technically feasible) format;[7]
- The Right to Opt Out: Consumers have the right to "opt out of the processing of personal data" for the purposes of targeted advertising and the sale of their personal data;[8] and
- The Right to Avoid Discrimination: Controllers "may not discriminate against a consumer for exercising a right" provided by the UCPA.[9]

Controllers (described in more detail below) must provide consumers with a "reasonably accessible and clear privacy notice," which includes the categories of personal data processed, the purposes of such processing, and whether third parties have access to that data.[10]

If personal data have been sold to third parties or processed for the purpose of targeted advertising, the controller must "clearly and conspicuously disclose" that activity to the consumer.[11]

If a consumer contacts the controller to exercise any of its above-described rights under the UCPA, the controller must respond within 45 days of receipt of the communication.[12]

2. Controller vs. Processor Distinction

The UCPA, like the VCDPA and the CPA, draws a distinction between controllers and processors of consumer data. A "controller" is a person or entity that "determines the purposes for which and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others."[13] A "processor" is a person or entity that "processes personal data on behalf of a controller."[14]

Processors are required to aid controllers in complying with the UCPA, including by assisting controllers in fulfilling their obligations to respond to consumer requests, helping controllers meet their obligations to process personal data securely, and providing information to aid controllers in the notification of a breach of system security.[15] The determination as to whether an entity is acting as a controller or processor is a fact-based, contextual determination.[16]

Contracts between controllers and processors must include certain elements, including that: (i) the controller clearly instructs the processor in its processing of personal data, the nature and purpose of processing, the type of personal data processed, the duration of the processing and the parties' rights and obligations; (ii) the processor is subject to a duty of confidentiality; and (iii) the processor may engage a subcontractor only if such subcontractor is also contractually required to meet the processor's obligations under the UCPA.[17]

3. Personal Data and Sensitive Data

"Personal data" is defined in the UCPA as "information that is linked or reasonably linkable to an identified individual or an identifiable individual," excluding de-identified data, aggregated data or publicly available information.[18] The UCPA also requires that a controller may not process "sensitive data" without providing a consumer "with clear notice and an opportunity to opt out" of such processing.[19] "Sensitive data" means personal data that reveal an individual's race, ethnicity, religious beliefs, sexual orientation, citizenship or immigration status, medical history, mental or physical health condition, medical treatment or diagnosis, genetic or biometric data if the purpose is to identify a specific individual, or specific geolocation data. Sensitive data do not include data processed by a video communication service that reveals an individual's race or ethnicity.[20]

4. De-identified Data

Controllers in possession of de-identified data must comply with any contractual obligations regarding that data and promptly address any breach of those obligations.[21] The UCPA defines de-identified data as data that cannot be reasonably linked to an individual and are possessed by a controller that (i) takes reasonable measures to ensure that a person cannot associate the data with an individual, (ii) publicly commits to maintaining and using such data without attempting to re-identify it, and (iii) contractually requires any recipients of de-identified data to comply with these requirements.[22] Controllers are not required to comply with consumer requests under the UCPA if the data are de-identified, and (i) the controller is not reasonably capable of associating a request with the related personal data or if it would be unreasonably burdensome to associate the request with the personal data, (ii) the controller does not use the personal data received in the request to recognize or respond to the consumer who is the subject of the personal data or associate the personal data with other personal data about the consumer, or (iii) the controller does not sell or otherwise disclose the personal data to any third party other than a processor as permitted under the UCPA.[23]

5. Public Enforcement / No Private Right of Action

The UCPA does not provide a private right of action.[24] The Utah Attorney General has exclusive authority to enforce the UCPA.[25] If a controller or processor violates the UCPA and does not cure such violation within 30 days of notice by the Utah Attorney General, the Utah Attorney General may seek actual damages for the consumer and civil penalties of up to $7,500 per violation.[26] The UCPA gives controllers and processors a 30-day cure period for all violations.[27]

The UCPA creates a consumer protection division to receive and investigate consumer complaints.[28] When the division has "reasonable cause to believe that substantial evidence exists" of a UCPA violation, the division will refer the complaint to the Utah Attorney General and provide the Utah Attorney General "consultation and assistance" upon request.[29]

The UCPA also creates a special fund called the Consumer Privacy Restricted Account, which will be funded by money received from civil enforcement actions under the UCPA.[30] Amounts paid into the Consumer Privacy Restricted Account will be used to support the AG's enforcement of the UCPA.[31]

B. EXCEPTIONS AND EXEMPTIONS

The UCPA exempts certain categories of entities from its purview, including (i) political bodies and agencies of the state, (ii) financial institutions subject to the Gramm-Leach-Bliley Act, (iii) covered entities and business associates as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, (iv) air carriers, (v) institutions of higher education, and (vi) nonprofits.[32]

The data collection limitations imposed by the UCPA do not apply if the collection of such data is required to (i) comply with federal, state or local law, (ii) comply with legal process, (iii) defend legal claims, (iv) act at a consumer's request, (v) protect the life or physical safety of an individual, (vi) conduct internal analytics or research to improve security, products and services, or (vii) perform internal operations that can be reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller.[33]

The UCPA also does not apply to certain categories of data, including information protected by HIPAA, patient-identifying information, information relating to human research subjects, information used by a consumer reporting agency, personal data covered by particular federal laws, and data that are processed and maintained about a controller's job applicants, employees, agents or independent contractors that are used in relation to such individuals' respective roles.[34] The UCPA thus follows the VCDPA and the CPA in excluding employee-related data and business contact information from its coverage. This is different than the CCPA and the CPRA, which require covered businesses to provide notice to applicants and employees of their data processing practices and will soon require businesses to respond to consumer rights requests from their applicants and employees.

Finally, the UCPA limits secondary liability. If a controller or processor discloses personal data to a third-party controller or processor in a manner compliant with the UCPA, it will not be found to have violated the law if the third-party recipient violates the law, provided the disclosing party did not have actual knowledge that the recipient intended to commit a violation.[35]

C. IMPLICATIONS

The enactment of the UCPA provides additional evidence of the increased willingness among U.S. states to mandate consumer privacy protections. Utah has joined Virginia, Colorado and California in enacting a comprehensive privacy law. The ease with which goods and services flow across state boundaries, thereby triggering obligations to comply with state privacy laws, requires businesses to be aware of and comply with the requirements of multiple state privacy laws and regulations.

The risk that a business could be liable for violating a state privacy law is likely to increase given the proliferation of privacy bills currently under consideration by state legislatures. As of the date of publication of this Memorandum, the U.S. State Privacy Legislation Tracker, which is maintained by the International Association of Privacy Professionals, lists 12 states with active privacy legislation: Alaska, Connecticut, Louisiana, Massachusetts, Michigan, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island and Vermont.[36]

The enactment of the UCPA indicates that U.S. states have not settled on a unified approach to privacy legislation. For instance, though the UCPA is similar to the VCDPA and the CPA, its scope is narrower and many of its protections for consumers and requirements of businesses are less stringent. Unlike the VCDPA and the CPA, the UCPA applies only to businesses with annual revenue of $25 million or greater,[37] applies certain requirements only to personal data that consumers provided to those businesses, instead of all the information that those businesses obtain,[38] does not provide a right for consumers to opt out of profiling,[39] and does not require businesses to affirmatively assess data processing with "a heightened risk of harm," such as the use of sensitive data and profiling.[40]

Businesses should first assess whether they are subject to the UCPA, based on the revenues and data processing activities of Utah residents. A business that is subject to the UCPA should evaluate, and, where appropriate, update, its data collection and privacy policies and practices to (i) develop a comprehensive understanding of the personal data and the sensitive data subject to the UCPA that the business collects and discloses, (ii) review its privacy notices to ensure they contain the content required by the UCPA, (iii) review its policies, procedures and systems designed to respond to consumer rights requests under the UCPA, (iv) review and revise, as appropriate, its contracts with service providers to include the provisions required by the UCPA, and (v) develop any necessary opt-out mechanisms applicable to the business's processing of sensitive data, the use of personal data for targeted advertising or the sale of personal data.

* * *

ENDNOTES

[1] UCPA § 13-61-102(1).

[2] *See Status*, *S.B. 227 Consumer Privacy Act*, UTAH STATE LEG., *available at* https://le.utah.gov/~2022/bills/static/SB0227.html.

[3] *Id.*

[4] UCPA § 13-61-201(1)(a).

[5] *Id.* § 13-61-201(1)(b).

[6] *Id.* § 13-61-201(2).

[7] *Id.* § 13-61-201(3).

[8] *Id.* § 13-61-201(4).

[9] *Id.* § 13-61-302(4).

[10] *Id.* § 13-61-302(1)(a).

[11] *Id.* § 13-61-302(1)(b).

[12] *Id.* § 13-61-203(2)–(3).

[13] *Id.* § 13-61-101(12).

[14] *Id.* § 13-61-101(26).

[15] *Id.* § 13-61-301(1)–(2).

[16] *Id.* § 13-61-301(3).

[17] *Id.* § 13-61-301(2).

[18] *Id.* § 13-61-101(24).

[19] *Id.* § 13-61-302(3).

[20] *Id.* § 13-61-101(32)(b)(i).

[21] *Id.* § 13-61-303(3).

[22] *Id.* § 13-61-101(14).

[23] *Id.* § 13-61-303(1)(c).

[24] *Id.* § 13-61-305.

[25] *Id.* § 13-61-402(1).

[26] *Id.* § 13-61-402(3).

[27] *Id.* § 13-61-402(3)(b).

[28] *Id.* § 13-61-401(1)–(2)(a).

[29] *Id.* § 13-61-401(2)(b)–(c).

[30] *Id.* § 13-61-403(1)–(2).

[31] *Id.* § 13-61-403(3).

[32] *Id.* § 13-61-102(2).

[33] *Id.* § 13-61-304(1).

[34] *Id.* § 13-61-102(2)–(4).

ENDNOTES (CONTINUED)

35 *Id.* § 13-61-304(3).

36 U.S. State Privacy Legislation Tracker, International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last accessed April 27, 2022).

37 *Compare* UCPA § 13-61-102(1)(b) *with* VCDPA § 59.1-572(A) *and* CPA § 6-1-1304(1). The $25 million revenue threshold is also contained in the CCPA. CCPA § 1798.140(c).

38 *Compare* UCPA § 13-61-201(2) *with* VCDPA § 59.1-573(A)(3) *and* CPA § 6-1-1306(1).

39 *Compare* UCPA § 13-61-201(4) *with* VCDPA § 59.1-573(A)(5)(iii) *and* CPA § 6-1-1306(1)(a)(I)(C).

40 *See* VCDPA § 59.1-576(A)(5) and CPA § 6-1-1309(1)–(2).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.