March 28, 2022

Utah becomes the Fourth Comprehensive State Privacy Law and a National Pattern Emerges

by John M. Brigagliano , Jon Neiditz

State legislative activity kicked off with a frenetic pace in 2022 and it seemed that there would be a number of new comprehensive privacy laws this year. Surprisingly to some, many of those efforts in other states fizzled while Utah's law was proposed and passed with blazing speed. Utah became the fourth state to enact a comprehensive, general consumer privacy law when Governor Spencer Cox signed the Utah Consumer Privacy Act ("**UCPA**") into law on March 24, 2022.

The law takes effect on December 31, 2023, making 2023 the apparent year of privacy compliance deadlines—new privacy laws take effect in January (Virginia and California), July (Colorado), and December (Utah).

As the UCPA does not become effective until the end of 2023, here is what you should do now to be well-positioned for compliance in 2023:

- **Figure out your organization's annual revenue and how many Utah consumers' personal data your organization processes to determine whether the UCPA applies to your organization.** As discussed below, the UCPA applies only to certain for-profit entities based on revenue and control or processing thresholds.
- **Create a plan to comply with the various state and global privacy laws that apply to your organization.** Required compliance measures will vary greatly for each organization depending on an organization's business model (e.g., whether the entity is a provider or customer of technology services) and whether the organization has complied with the California Consumer Privacy Act ("CCPA") and/or the European Union's General Data Protection Regulation ("GDPR"). Companies that have gone through such compliance may find little to do to become compliant with the UCPA, especially considering that the UCPA is not enforceable through a private right of action. Despite that broad interoperability with certain other privacy laws, however, the UCPA has certain unique compliance requirements for which covered organizations should account.
- **Check the scope of your compliance documents.** Your organization may have prepared internal documents (e.g., data subject access request policies, etc.) and executed agreements (e.g., privacy notices and data protection addenda) to comply with the CCPA and GDPR. Review whether those documents apply only to residents of California and/or the European Union and amend those documents accordingly for Utah, Virginia and Colorado.

Limited Scope with Annual Revenue Minimum

The UCPA applies to for-profit entities that have annual revenues of $25 million or more and do business in Utah or produce products or services that are targeted to Utah residents, so long as an entity meets one of two processing thresholds:

- Controls or processes the personal data of 100,000 or more Utah consumers annually; or
- Controls or processes the personal data of 25,000 or more Utah consumers and derives more than 50% of its gross revenue from selling personal data (i.e., data brokers).

The UCPA excludes entities regulated by the Gramm-Leach-Bliley Act ("GLBA") as well as covered entities and business associates as defined under the Health Insurance Portability and Accountability Act ("HIPAA"). That coverage represents a departure from the California privacy laws, which exclude federally regulated data rather than regulated organizations. Furthermore, the UCPA does not apply to an activity by a consumer reporting agency that is subject to regulation by the Fair Credit Reporting Act ("FCRA") and involves the collection, maintenance, disclosure, sale, communication or use of a consumer's personal data bearing on credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living. The relative narrowness of the UCPA's scope thereby provides a compliance reprieve for the federally regulated entities that had to comply with the CCPA and will have to comply with the CPRA in addition to those federal regimes.

Exclusions for B2B and Employee Personal Data

Unlike the California privacy laws and similar to Colorado's and Virginia's law, the UCPA defines consumers (the group of data subjects that the statute protects) as Utah residents acting in an individual or household capacity. That definition expressly excludes persons acting in a "commercial or employment context." Furthermore, the UCPA contains an additional exclusion to the law's scope for the personal data of emergency contacts if used for emergency contact purposes.

Data Protection Agreements (DPAs)

The UCPA requires controllers and processors (the entity that processes personal data on behalf of a controller) to enter into a DPA, the content requirements for which somewhat mirror those arising under the GDPR (e.g., the DPA must establish the nature and scope of the processing as well as the processor's obligations to assist the controller). Under the UCPA, processors must agree in the DPA that they have contractually obligated each person processing personal data to protect the confidentiality of the personal data provided by the controller and flow down obligations to protect such data to its subcontractors.

Consumer Rights

Generally speaking, the consumer privacy rights that the UCPA creates are similar to those in Virginia's Consumer Data Protection Act ("**CDPA**"):

- To confirm whether a controller processes the consumer's personal data;
- To access the consumer's personal data;
- To receive a copy of the consumer's personal data provided to the controller in a portable format;
- To delete personal data provided by the consumer to the controller (not all personal data about such consumer in the controller's possession); and
- To opt-out of targeted advertising and personal data sales.

Unlike the comprehensive privacy laws in California, Colorado and Virginia, the UCPA does not provide consumers with a correction right.

The requirement to provide an opt-out of information sales is much narrower than the somewhat equivalent right arising under California law, as the UCPA narrowly defines sales as the "exchange" of personal data for monetary consideration by the controller to a third party. The definition expressly excludes, among other exceptions, sharing directed by the consumer, sharing with a third party to provide a product or service requested by the consumer, affiliate sharing, disclosures to a processor and disclosures that are consistent with the consumer's reasonable expectations given the context in which the consumer provided the personal data originally.

The UCPA defining sales as an exchange of personal data, and not merely making personal data "available" to a third party (as is the case under California privacy law), reduces the scope of potential sales under the UCPA. In an online context, a website publisher allowing third parties to collect information (that the publisher may never receive) on a website is more clearly "making information available" (and thereby a potential sale under California privacy law) than an "exchange" of information (and therefore not likely a sale under the UCPA). That said, the right to opt out of targeted advertising will likely provide consumers with the option to opt out of much online tracking.

Under the UCPA, controllers are also prohibited from discriminating against a consumer for exercising one of their rights under this law by denying a good or service to such consumer, charging a different rate or price or providing a different level of quality of good or service. Note, however, that controllers may offer a different price, rate, level, quality or selection of good or service (including offering a good or service for free at a discount) if the consumer has opted out of targeted advertising or the offer is related to a loyalty program.

Consumers have the Right to Opt-Out of Processing Sensitive Personal Data

Prior to processing sensitive personal data, the controller must provide the consumer with clear notice and an opportunity to opt of the processing. When processing the personal data of a known child, a controller must process such data in accordance with the Children's Online Privacy Protection Act. The UCPA therefore aligns with the CPRA (California) by regulating sensitive personal information, unlike the CDPA (Virginia) or CPA (Colorado), which require opt-in consent before a controller may process sensitive personal information. Controllers may try to resolve that discrepancy by, where feasible, providing consumers with persistently available consent controls (which are defaulted to "off" for at least those located in Colorado or Virginia).

The UCPA defines "sensitive personal data" to include racial or ethnic origin, citizenship or immigration status, specific geolocation information, genetic personal data or biometric information if processed for the purpose of

identifying a specific individual, sexual orientation, religious beliefs, medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.

That requirement seemingly creates operational burdens for controllers, especially those without privity to consumers through which the controller may present the notice. Such controllers, however, could approach that requirement by requiring contractual counterparties with privity to the consumer to present the notice on the controller's behalf.

Enforcement

Enforcement (which is the Attorney General's responsibility) for the Utah law also remains uncertain. As mentioned above, there is no private right of action. The UCPA has a bifurcated process of enforcement that requires a consumer to first initiate a complaint with the Division of Consumer Protection. The director of the Division will refer such complaint to the Attorney General ("AG") if the "director has reasonable cause to believe that substantial evidence exists" that an entity subject to the law has violated the UCPA. If the AG decides to take action, the controller or processor will have a 30 day period from the AG's notice to cure the violation and provide a written statement that the violation has been cured and no future violation of the cured violation will occur. For uncured violations or upon a reoccurrence of a past violation, the AG can initiate an action to recover actual damages suffered by the consumer and fines of up to $7,500 per violation.

Furthermore, a currently effective Utah consumer privacy law (the Notice of Intent to Sell Nonpublic Personal Information Act) requires notice for and somewhat restricts the sale of personal information. That law has not, to our knowledge, been enforced to date. Whether the Utah AG will take a more active enforcement approach with respect to the UCPA (given the law's comprehensiveness), therefore, remains an open question.

Why More State Laws Are Looking Better to Business Than Preemptive Federal Law

In a bygone era, say 2021, the business community was still pressuring Congress to enact a preemptive national privacy law to avoid a patchwork of laws as aggressive as California's that (unlike the state breach laws) cut so deep into operations that compliance with all of them would be very expensive and close to impossible. The UCPA confirms a different strategy now, continuing the trend of state laws less restrictive than business-friendly Virginia's law (*pace* a few Colorado innovations). Likewise, some in the privacy community who hoped that the Utah Governor would veto the UCPA, as it undermines their hopes of a federal law and a stronger law in Utah. Reading the tea leaves, we would predict that we will continue to see state laws on this "Virginia-Minus" model proposed and passed. As we've mentioned previously, California's privacy law remains the high bar, the rest of the country will look like Greater Virginia and a comprehensive federal privacy law remains unlikely. Keep an eye out, however, for some state that does not want to be a suburb of Virginia, changing the game again and turning K Street into a bunch of privacy advocates again.