Snell & Wilmer
S&W Cybersecurity and Data Privacy Law Blog

What Does the New Utah Electronic Data Privacy Law Do?

POSTED ON: MAY 1, 2019 BY: ANNE BOLAMPERTI AND PATRICK X. FOWLER

Utah recently became the first state to enact a law specifically designed to protect private electronic information stored with third parties from collection by law enforcement without a valid warrant. Utah Governor Gary Herbert signed the ground-breaking legislation on March 27, 2019, and it is expected to take effect in May 2019. The aim of the new law is to protect Utahns from unreasonable searches and seizures. However, it is not without controversy. While previous iterations of the bill were initially criticized, the Utah Attorney General's Office later supported the final version of the bill.

Broad Definitions

HB57, or the "Electronic Information or Data Privacy Act," (the "Law") broadly defines an electronic device as one that "enables access to or use of an electronic communication service, remote computing service, or location information service." Electronic information or data is considered to include "intelligence of any nature" that is "transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Importantly, this information also includes location information, stored data, or the transmitted data of electronic devices.

This electronic information or data includes what may be stored in social media platforms such as Facebook, Instagram, Twitter, and Snapchat, as well as search engines like Google, Yahoo, and Bing. Email platforms like Gmail and Microsoft Outlook, and electronic communication service providers like Verizon, AT&T, and T-Mobile are also included. However, oral communications are not considered as part of the definition.

Provisions

- ***Warrant Required for Law Enforcement Access to Data on Electronic Devices***

The Law covers several provisions which address the privacy of electronic information or data. The first provision lays out when a warrant issued by a court upon probable cause is required, and what specifically cannot be obtained without a warrant. Aside from strict exceptions for stolen devices, a search warrant will be required in order for Law enforcement to obtain location information, stored data, or transmitted data from an electronic device for a criminal investigation or prosecution, as well as electronic information or data sent by the owner of that data to a remote computing service provider.

- ***Law Enforcement Allowed Only a Short Window to Delay Notification of Electronic Data Collected Through a Warrant***

The next provision details how long a Law enforcement agency may collect electronic information or data if they do obtain a warrant, as well as the specifics of a notification the agency must send after collecting the electronic device. Within fourteen days of obtaining the information or data as a result of a warrant (with thirty-day delays available from the court), the agency must notify the data owner about the the alleged offense and identify the Law enforcement agency and the judge who authorized the warrant. The notification must also state that a warrant was applied for and granted, the nature of the warrant that issued, and how long the agency may collect data. The window of time in which to send the notification is triggered when the Law enforcement agency finds the owner of the data, or when the owner could have reasonably been identified by the agency.

- ***Third-party Electronic Information or Data***

The third provision outlines the information contained in a "subscriber record," which is personal information stored in an electronic communication service provider or remote computing service. The new law precludes Law enforcement agencies from using subscriber records without a warrant. For example, cellular service providers each have vast subscriber records containing personal and financial information regarding a user's name, address, phone records, types of service used, and credit card numbers, among other details. None of this information is accessible without a warrant under Utah's new Law.

- ***Exclusion of Illegally-Collected Data***

The final provision of the Law notes that any electronic information or data, as well as subscriber records taken by Law enforcement in violation of the Law will be subject to rules governing exclusion of evidence when it is taken is in violation of the Fourth Amendment's protections against unreasonable search and seizure.

Who Will the Law Impact?

Utah's Law currently stands as the strongest law of its type in the U.S., and will likely encourage other states to follow suit with similar bills. California and Vermont in particular are likely to follow closely behind Utah due to each state's past as proponents of increased privacy protections. The California Consumer Privacy Act ("CCPA"), which will take effect on January 1, 2020, focuses on how businesses collect and use Californians' data. The CCPA only covers electronic data privacy from a consumer perspective, not from that of preventing disclosures to Law enforcement agencies. Vermont's HB764, which took effect on January 1, 2019, is also a consumer-focused Law, which focuses on protecting consumers from "data brokers," who aggregate and sell data about consumers to businesses who do not have a direct relationship to the consumer.

California and Vermont's new consumer protection privacy laws are helpful, but Utah's new Law takes privacy protection a step further towards protecting an individual's private electronic information or data that is stored with third parties. Information and data stored online is increasingly regarded as just as important—if not more so—as physical documents and other tangibles, and Utah is moving in this direction. While differences between the physical and electronic worlds exist, individual privacy is essentially viewed as the same with this new law. Stay tuned!