F I S C A L I M P A C T R E P O R T

SPONSOR Wirth **ORIGINAL DATE** 1/17/19 **LAST UPDATED** **HB**

SHORT TITLE Electronic Communications Privacy Act **SB** 199

ANALYST Jorgensen

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY19	FY20	FY21	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		See Fiscal Implications	See Fiscal Implications	See Fiscal Implications	Recurring	General Fund/ Other State Funds

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION

LFC Files

Responses Received From
Administrative Office of the District Attorneys (AODA)
Attorney General's Office (AGO)
Department of Information Technology (DoIT)
Department of Public Safety (DPS)

SUMMARY

Synopsis of Bill

Senate Bill 199, titled the Electronic Communications Privacy Act, would require law enforcement and other government entities to seek court approval in order to acquire, retain, and use electronic information found on mobile phones, found on tablets or similar devices, and/or obtained from mobile telephone and internet service providers, with some exceptions.

FISCAL IMPLICATIONS

The Attorney General's Office (AGO) and Department of Public Safety (DPS) face the largest potential costs of implementation of this legislation. While both agencies anticipate additional costs, neither estimated the impact.

Under the provisions of SB199, the AGO is required to publish summary reports of law enforcement entities' use of electronic surveillance on the AG's website. The reporting requirements will require the construction and/or maintenance of additional web pages on the AG's website as well as additional staff and attorney time related to redaction of certain materials as well as organizing and summarizing reports submitted by law enforcement.

DPS notes the requirement to report to the Attorney General on each instance of obtaining data will require significant additional staff hours. Additionally, DPS states that the requirement to provide notice to the data owner and the requirement that exculpatory evidence be kept and other evidence be destroyed within thirty days will create a significant impact on resources. The Department concludes that "it is certain that resources would need to be dedicated to meet these requirements."

SIGNIFICANT ISSUES

The Administrative Office of the Courts in response to a request for comment on an identical bill introduced in a previous session pointed out that SB199 requires the destruction of electronic information, electronic device information or electronic communication information; however, there is no guidance about how to undertake the destruction of such information. It is unclear whether government entities required to destroy such information will be aware of the procedures and have the technical knowledge necessary for complete destruction of data and metadata. It also states that the court has to "promptly rule" but the bill does not provide for a timeframe for the court to rule.

AOC states that the federal Electronic Communications Privacy Act was enacted in 1986 and is considered to be outdated. In 2015, California enacted its own ECPA, which is similar in many ways to SB199. Utah, Maine and Texas have also enacted laws protecting electronic communications. In addition to New Mexico, 15 other states and the District of Columbia introduced ECPA legislation in 2016. See, https://www.aclu-nm.org/en/news/aclu-nm-worksbipartisan-team-legislators-introduce-electronic-communications-privacy-act

The AGO states that this bill forbids a governmental actor from compelling or incentivizing the production of electronic device information from a person or service provider other than the device's "authorized possessor." Further, the government is not allowed to access the electronic device information by means of a "physical interaction or electronic communications with the electronic device." An "authorized possessor" is defined as a "natural person who owns and possesses the electronic device or a natural person who, with the owner's consent, possesses the electronic device." This dynamic raises an issue for electronic device owned by one party but allows a third party to possess the device. For instance, a parent who buys a phone for their child cannot give permission to a governmental actor to access the phone. Also, this owner/authorized possessor dynamic comes into play when an employer provides an electronic device to their employee, the employer has no authority to access or release electronic device information for a device they own.

In light of recent New Mexico Supreme Court decisions, the act is designed to increase each individual's expectation of privacy in our electronic device information. See State v. Tufts, 2016-NMSC-020; see also State v. Angelo M., 2014 WL 1315005, State v. Rigoberto Rodriguez, 2016 WL 4579254. The Act is balanced with allowances for civil subpoena, search warrants and emergent circumstances.

DPS believes that the definition of electronic devices is overly broad and scope for a warrant is overly narrow.

The Department of Information Technology (DoIT) notes that many of the definitions are broad

in scope and limitations on access are restrictive overall.

ADMINISTRATIVE IMPLICATIONS

DPS reports that it does not know how frequently it obtains data from electronic devices each year, as this is not currently tracked. However, it is estimated that the frequency is significant, as DPS participates in up to 20,000 investigations per year including specialized investigations relating to narcotics, online predators, murder, white collar crime, etc.

The bill impacts the AGO's administrative functions because the governmental actor who executes the warrant or obtains electronic information in an emergency must submit a report within 3 days to the AGO. Then within 90 days of receipt of each report, the AGO must publish the report on his website. The AGO is responsible for redacting names and all other PII from the reports. Beginning in 2020, the Act requires the AGO to tabulate the individual reports from each governmental actor and publish a summary of the individual reports.

CONFLICT

The AGO notes the following possible conflicts:

SB199 may conflict with federal law requiring disclosure of customer communications to governmental entities. For example, Section 2703 does not require notice to a subscriber or customer that a governmental entity is requesting their information if the entity obtains a warrant.
SB199 requires notice be made to the identified target(s) even if the entity first acquires a warrant, though SB199 allows such notice to be delayed for up to ninety days per Section 4(B).

SB199 may conflict with portions of the Missing Persons Information and Reporting Act, specifically requirements that missing persons reports contain, to the extent available, "information on the missing person's electronic communications devices."

TECHNICAL ISSUES

The AOC cites, Riley v. California, 573 U.S. ___ (June 25, 2014), in which the US Supreme Court ruled unanimously that a warrant was needed to search information on a mobile phone taken from an arrestee. The Court did not require states to adopt systems for addressing searches and seizures of all variety of electronic information. However, without a process committed to legislation, courts would have to devise a process through ad hoc litigation of specific issues. This bill would establish just such an omnibus procedure for use of information on mobile phones and other electronic devices.

AOC further points out that one issue that does remain is verification of destruction of information. Throughout the bill, government entities are required in a variety of circumstances to destroy the information they obtain. Often, destruction of electronic information can be incomplete, and its presence can persist even if reasonable attempts are made to destroy the information. This leaves open the questions of how much effort should be expended to destroy information, and what should happen if the information is found to continue to exist even after destruction is reported to be complete.

The AODA reports that of particular concern to the district attorneys are crimes that are committed through electronic means, such as some frauds and embezzlements, and crimes involving the electronic communication of prohibited images, such as some forms of child pornography. Other crimes may not be committed directly through electronic means, but obtaining electronic information may be vital to the investigation and prosecution of the crimes. SB199 sets out a detailed process for obtaining and retaining such information, that includes extensive notice and reporting requirements.

OTHER SUBSTANTIVE ISSUES

DPS notes the following:

> "Under any circumstances, the requirements related to destruction of unrelated, and exculpatory evidence would need to allow for retention of the searched records until a case has been adjudicated. Provisions should be added to prevent the release of these records to any person, other than through a court.
>
> The bill should also include an exception to retain the information as long as reasonably needed for an investigation, such as a six-month narcotics operation. The information obtained may incriminate others, which would likely take additional time to develop probable cause to arrest and charge that individual.
>
> The bill also provides that a court may appoint a special master charged with ensuring that only the information necessary to achieve the objective of the warrant or order is produced or accessed. A special master reviewing evidence such as narcotics transactions on a cell phone with law enforcement could add an additional risk of compromising an investigation, as some of this information obtained is highly sensitive and confidential, and there are already protections in place which prohibit from using anything unrelated."

CJ/sb