

LFC Requester:	
-----------------------	--

**AGENCY BILL ANALYSIS
2019 REGULAR SESSION**

WITHIN 24 HOURS OF BILL POSTING, EMAIL ANALYSIS TO:

LFC@NMLEGIS.GOV

and

DFA@STATE.NM.US

{Include the bill no. in the email subject line, e.g., HB2, and only attach one bill analysis and related documentation per email message}

SECTION I: GENERAL INFORMATION

{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Check all that apply: Date Jan. 17, 2019
Original **Amendment** **Bill No:** SB199
Correction **Substitute**

Sponsor: Peter Wirth **Agency Code:** 264
Short Electronic Communications **Person Writing** Gail MacQuesten
Title: Privacy Act **Phone:** 505 466-0532 **Email** gailmacquesten@gmail.com

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY19	FY20		
0	0	n/a	n/a

(Parenthesis () Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY19	FY20	FY21		
0	0	0	n/a	n/a

(Parenthesis () Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY19	FY20	FY21	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	0	unknown	unknown	unknown	recurring	general

(Parenthesis () Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis:

SB199 creates the “Electronic Communications Privacy Act.”

The Act sets out how a government entity may compel the production of or obtain access to electronic communication information from a service provider or compel the production of or obtain access to electronic device information from a person other than the authorized possessor of the device, and how a government entity may access electronic device information by means of physical interaction or electronic communication with the device. The Act does not limit the authority of a government entity to use an administrative, grand jury, trial or civil discovery subpoena to obtain certain information. The Act also does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication.

Obtaining information or access from a service provider or a person other than the authorized possessor requires a warrant or a wiretap order. However, a service provider may voluntarily disclose electronic communication information or subscriber information if the law otherwise permits that disclosure. In that situation, the government entity must destroy that information within 90 days unless the government has obtained the specific consent of the sender or recipient of the electronic communication or obtains a court order authorizing the retention of the information.

Accessing electronic device information directly from a device requires a warrant or wiretap order, or one of the following:

- Specific consent of the device’s authorized possessor;
- Specific consent of the device’s owner if the device has been reported as lost or stolen;
- If the government entity believes in good faith that the device is lost, stolen or abandoned, it may access information solely for the purpose of attempting to identify, verify or contact the device’s authorized possessor; or
- If the government entity believes in good faith that an emergency involving danger of death or serious physical injury to a natural person requires access to the information. The government entity must then follow by applying for a warrant or order or by a motion seeking approval.

A warrant must describe with particularity the information to be seized by specifying the time periods covered and, as appropriate, the natural persons or accounts targeted, the applications or services covered and the types of information sought. Except when the information obtained is exculpatory, any information unrelated to the objective of the warrant must be destroyed within 30 days.

When a government entity obtains electronic information under a warrant or in an emergency situation, it must give notice to the identified targets that information has been compelled and state with specificity the nature of the investigation under which the information is sought, and include a copy of the warrant or a written statement setting forth the facts giving rise to the emergency. The government entity may request a court order delaying the notification. If there is not an identified target of a warrant or emergency request at the time of the warrant's or request's issuance, the government entity must notify the attorney general. The court may appoint a special master to ensure that only the information necessary to achieve the objective of the warrant or order is produced or accessed.

A person in a trial, hearing or proceeding may move to suppress electronic information obtained or retained in violation of the Act. The attorney general may commence a civil action to compel a government entity to comply with the Act. The recipient of a warrant or order issued pursuant to the Act may petition the court to void or modify it or order the destruction of any information obtained in violation of the Act.

A government entity that obtains electronic communication information under the Act must provide a detailed annual report to the attorney general including the following information: The number of times each of type of information (electronic communication content, location information, electronic device information, and other electronic communication information) was sought and, for each, the number of records obtained. In addition, for each type of information:

- the number of times that type of information was sought or obtained under: 1) a wiretap order; 2) a search warrant; and 3) an emergency request;
- the number of persons whose information was sought or obtained;
- the number of instances in which information sought or obtained did not specify a target natural person;
- for demands or requests issued upon a service provider, the number of those demands or requests that were fully complied with, partially complied with and refused;
- the number of times notice to targeted persons was delayed and the average length of the delay;
- the number of times records were shared with other government entities or any department or agency of the federal government and the government entity, department or agency names with which the records were shared;
- for location information, the average period for which location information was obtained or received; and
- the number of times electronic information obtained under the Act led to a conviction and the number of instances in which electronic information was sought or obtained that were relevant to the criminal proceedings leading to those convictions.

Every year the attorney general shall publish on its website the individual reports from each government entity and a summary aggregating each of the items listed in the reports.

FISCAL IMPLICATIONS

Note: major assumptions underlying fiscal impact should be documented.

Note: if additional operating budget impact is estimated, assumptions and calculations should be reported in this section.

SB199 is likely to have a significant fiscal impact on government entities that seek electronic information through the provisions of the Act. The Act contains additional requirements regarding the contents of a warrant, special master proceedings, emergency requests, notification, requests to delay, and evaluation, retention and destruction of information obtained. In addition, the Act contains extensive record keeping requirements.

SIGNIFICANT ISSUES

As discussed above, the Act sets out detailed procedures with deadlines and reporting requirements. Any violation of the Act can be the subject of a motion to suppress. The more cumbersome and detailed the requirements, the more likely it is that a violation will occur, and a motion to suppress will be successful.

PERFORMANCE IMPLICATIONS

See Fiscal Implications and Performance Implications, above.

ADMINISTRATIVE IMPLICATIONS

The reporting requirements are extensive, and detailed. The attorney general's office must compile and post the information. If the reporting formats are not consistent in the various governmental entities seeking information pursuant to the Act, it will be extremely difficult to compile the information in a meaningful way.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

None noted.

TECHNICAL ISSUES

None noted.

OTHER SUBSTANTIVE ISSUES

None noted.

ALTERNATIVES

None proposed.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

New Mexico will not have a statutory framework addressing government access to electronic

communications.

AMENDMENTS

None proposed.