LFC Requester:	

AGENCY BILL ANALYSIS
2015 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:

Original X **Amendment** ____
Correction ___ **Substitute** ____

Date 1-26-16
Bill No: SB154

Sponsor: Peter Wirth and Jim Dines
Short Title: Electronic Communications Privacy Act

Agency Code: 264
Person Writing Gail MacQuesten
Phone: 466-0532 **Emai** gailmacquesten@q.com

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY16	**FY17**		
0	0	n/a	n/a

(Parenthesis ( ) Indicate Expenditure Decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY16	**FY17**	**FY18**		
0	**0**	**0**	n/a	n/a

(Parenthesis ( ) Indicate Expenditure Decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY16	FY17	FY18	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:

SB154 creates the "Electronic Communications Privacy Act."

Section 2 of SB154 defines 12 terms used in the act: "adverse result;" "authorized possessor;" "electronic communication;" "electronic communication information;" "electronic communication service;" "electronic device;" "electronic device information;" electronic information;" "government entity;" "service provider;" "specific consent;" and "subscriber information."

Section 3 sets out in detail how a government entity may access certain electronic information, and how long the government entity may retain such information:

- A government entity may compel production of or access to electronic communication information from a service provider or a person other than the authorized possessor of the device only under a warrant that complies with the act or under a wiretap order;
- A government entity may access electronic device information through physical interaction or electronic communication with the device only under a warrant that complies with the act; a wiretap order; with the specific consent of the device's authorized possessor; with the specific consent of the device's owner if the device has been reported as lost or stolen; for the purpose of attempting to identify, verify or contact the device's authorized possessor if the entity believes in good faith that the device is lost, stolen or abandoned; or because the entity believes in good faith that an emergency involving danger of death or serious physical injury to a natural person requires access to the electronic device information;
- A warrant for the search and seizure of electronic information must describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the natural persons or accounts targeted, the applications or services covered, and the types of information sought, and require that any information obtained that is unrelated to the objective of the warrant be destroyed within 30 days (except for information exculpatory with respect to the natural person targeted), and otherwise comply with state and federal laws;
- A court may appoint a special master to ensure that only information necessary to achieve the objective of the warrant or order is produced or accessed;
- A service provider may voluntarily disclose information if the law otherwise permits the disclosure;

- A government entity receiving voluntarily disclosed information under this section shall destroy that information within 90 days unless the entity obtains the specific consent of the sender or recipient, or obtains a court order;
- A court may order retention of information only upon a finding that the conditions justifying the initial voluntary disclosure persist and such order shall last only for the time those conditions persist or there is probable cause to believe that the information constitutes criminal evidence;
- Information retained under this section shall be shared only with a person who agrees to limit use of the information to the purposes identified in the order and is legally obligated to destroy the information or voluntarily agrees to destroy the information when the court order expires or is rescinded;
- If the government entity obtains information due to an emergency the entity shall, within three days, file with the appropriate court an application for a warrant or order, or a motion seeking approval of the emergency disclosures;
- A court receiving such an application or motion shall rule promptly, and if the court does not find that an emergency exists or otherwise rejects the application, it shall order immediate destruction of all information obtained and immediate notification as provided in the act;
- A government entity may use an administrative, grand jury, trial or civil discovery subpoena to require: an originator, addressee or intended recipient of an electronic communication to disclose information associated with that communication; or a person who provides electronic communications services to its officers, directors, employees or agents to disclose information associated with those communications; and a service provider to provide subscriber information;
- The intended recipient of an electronic communication may voluntarily disclose electronic communication information concerning that communication to a government entity.

Section 4 requires a government entity that obtains information under the act through a warrant or under the emergency provisions of the act must give notice to the identified targets, stating that information has been compelled or requested and stating with reasonable specificity the nature of the government investigation under which the information is sought. Notice is to be given contemporaneously with the execution of a warrant or in the case of an emergency, within 3 days after obtaining the information, and must include a copy of the warrant or a statement setting forth the facts giving rise to the emergency. The government entity may request a court order delaying notification, if there is reason to believe that notification may have an adverse result (defined as danger to life or physical safety, flight from prosecution, destruction or tampering with evidence, witness intimidation or serious jeopardy to the investigation). The court may delay notification for 90 days, and may extend the delay for additional 90 day periods upon a proper showing. Once the period of delay expires, the government entity must serve upon or deliver to the targets of the warrant, a document that includes the notice information described above, and a copy of all information obtained or a summary of that information, including, at a minimum, the number and types of records, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the targeted person. If there is no identified target, the information is to be submitted to the attorney general, and the reports shall be published on the attorney general website with names and other personal identifying information from the reports.

Section 5 allows a person in a trial, hearing or proceeding to move to suppress any information

obtained or retained in violation of the act (or the state or federal constitutions). The attorney general may also commence a civil action to compel compliance with the act. A person, service provider or other recipient of a warrant, order or other process obtained in violation of the act (or the state or federal constitutions) may petition to void or modify the order, or for an order requiring the destruction of information obtained in violation of law.

Section 6 requires a government entity obtaining information under the act to report to the attorney general every year. The report shall include the number of times electronic information was sought or obtained under the act, the number of times specific types of information were sought, and for each type of information:

- the number of times that type of information was sought or obtained under a wiretap order, a search warrant or 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 on service providers, the number of demands complied with fully, partially or refused;
- the number of times notice was delayed and the average length of the delay;
- the number of times records were shared and the entity, department or agency 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 led to a conviction and the number of instances in which information was sought or obtained that was relevant to the criminal proceedings leading to those convictions.

Every year the office of the attorney general shall publish on its website the individual reports and a summary aggregating each of the items required in the reports. A service provider may also produce an annual report summarizing demands or requests under the act.

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.

Complying with the act will have a significant fiscal impact on law enforcement, and particularly on the district attorneys. SB154 sets out detailed requirements for obtaining information, providing notice, retaining information, destroying information and providing an extensive annual report. No appropriation appears in SB154 to cover these additional costs.

SIGNIFICANT ISSUES

As more transactions and communications take place electronically, the more important electronic information becomes to state agencies charged with enforcing civil and criminal statutes. 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. SB154 sets out a detailed process for obtaining and retaining such information, that includes extensive notice and reporting requirements.

The requirements set out in SB154 are extremely detailed, and will require considerable work for prosecuting agencies, with additional showing, hearings, motion, reports and administrative procedures to ensure compliance. Many of the protections appear to be for the protection of service providers, rather than for the target of the criminal investigation. That is clear from the fact that the act provides that the service provider can forgo all the protections set out in the act and voluntarily disclose electronic communication information or subscriber information if the law otherwise permits that disclosure. See Section 3F.

PERFORMANCE IMPLICATIONS

Prosecutors (and other state entities that need electronic information to carry out their responsibilities) will have additional hearings and showings. Not only must they obtain a warrant, wiretap order or emergency order, they will need to provide notice (or have hearings to delay notice), evaluate evidence and destroy it within a certain time period (or obtain a court order delaying destruction), and file detailed annual reports.

ADMINISTRATIVE IMPLICATIONS

See performance implications, above.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

None noted.

TECHNICAL ISSUES

Section 3 L (2) is difficult to understand: "This section does not limit the authority of a government entity …to require…when a person that provides electronic communications services to its officers, directors, employees or agents for those officer, directors, employees or agents to carry out their duties, the person to disclose the electronic communication information associated with an electronic communication to or from the officer, director employee or agent."

OTHER SUBSTANTIVE ISSUES

None.

ALTERNATIVES

None.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Production of electronic information will be governed by existing statutory and constitutional provisions.

AMENDMENTS

None proposed.