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

SPONSOR Wirth/Dines **ORIGINAL DATE** 1/26/17 **LAST UPDATED** 02/16/17 **HB**

SHORT TITLE Electronic Communication Privacy Act **SB** 61/aSJC

ANALYST Sánchez

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY17	FY18	FY19	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total		Indeterminate increase	Indeterminate Increase	Indeterminate Increase	Recurring	General Fund/Other State Funds

(Parenthesis ( ) Indicate Expenditure Decreases)

Relates to HB15

SOURCES OF INFORMATION
LFC Files

Responses Received From
Administrative Office of the Courts (AOC)
Administrative Office of the District Attorneys (AODA)
Attorney General's Office (AGO)
Department of Public Safety (DPS)
Commission on Public Records (CPR)
Department of Information Technology (DoIT)
Public School Insurance Authority (PSIA)
New Mexico Corrections Department (NMCD)

SUMMARY

Synopsis of SJC Amendment

Senate Judiciary Amendment to Senate Bill 61 inserts "as necessary and" to Section 3, Subsection C, Paragraph 5 limiting access to a device by a government entity if the government entity believes in good faith the device is lost, stolen or abandoned. The paragraph now reads as follows

> because the government entity believes in good faith that the device is lost, stolen or abandoned, in which case, the government entity may access that information only **as necessary and** for the purpose of attempting to identify, verify or contact the device's authorized possessor.

Synopsis of Bill

Senate Bill 61 seeks to address the issue of law enforcement's acquisition of information found in mobile phones, tablets and other electronic devices. The bill does so by creating a system by which law enforcement must seek court approval to retain and use this information, with notable exceptions.

FISCAL IMPLICATIONS

The Department of Public Safety (DPS) believes that reporting, notice requirements and destruction of exculpatory evidence will impact negatively its staff and financial resources. It also states that the bill will extend the level of effort required to complete each investigation.

Other agencies report minimal or no fiscal impact from this bill.

SIGNIFICANT ISSUES

AOC point out that SB61 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 SB61. 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-works-bipartisan-team-legislators-introduce-electronic-communications-privacy-act

The AGO opines 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) believes the bill will cause it and (state) agency IT departments significant confusion and potential civil liability because the definitions are so expansive that they touch every inch of the business of IT, and would limit DoIT's ability to provide services. Additionally, DoIT falls under the definitions of "government entity" and "service provider" as it is both and this bill could potentially hamper access its own or another agencies data located on state employee's cell phone or computer, or any state IT resources without a warrant or court order in the regular course of business. Moreover, DoIT provides public safety communications which could be hindered by this bill.

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 2019, the Act requires the AGO to tabulate the individual reports from each governmental actor and publish a summary of the individual reports.

The Commission on Public Records (CPR) states that the rule on retaining investigative records will have to amend or a new classification for retention of electronic communication information will have to be created.

AODA opines that the requirements set out in SB61 are extremely detailed, and will require considerable work for prosecuting agencies, with additional showing, hearings, motion, reports and administrative procedures to ensure compliance.

RELATIONSHIP

SB 61 relates to HB15, Data Breach Notification Act

TECHNICAL ISSUES

AOC states that while the term "natural person" is not defined in SB61, the term is usually interpreted to mean a human being, as opposed to the term "person" which, in contrast, is defined as used in the statutes and rules of New Mexico to mean "an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture or any legal or commercial entity." Section 12-2A-3(E) NMSA 1978

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. SB61 sets out a detailed process for obtaining and retaining such information, that includes extensive notice and reporting requirements. 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.

OTHER SUBSTANTIVE ISSUES

SB61 protects against unauthorized collection or access of electronic devices or information by government entities yet allows government entities a means by which to obtain electronic devices or information to accomplish its responsibilities. The bill seeks to protect against bulk data collection such as that done by the National Security Agency.

The AGO believes SB 61 may conflict with the federal Electronic Communications Privacy Act. 18 U.S.C. 2703; rules for grand jury investigations and other laws such as the child solicitation by electronic communication device statute, NMSA 1978, § 30-37-3.2.

The New Mexico Corrections Department (NMCD) states that it does not seem to prevent it from accessing an employee's cell phone during administrative investigations.

ALTERNATIVES

DPS suggests amending the paragraph on exculpatory evidence to allow for the securing of the records, regardless until the case has been adjudicated. Provisions could be added to prevent the release of these records to any person, other than through the court. It recommends including an exception to retain the information as long as reasonably needed for the investigation, such as a six month narcotics operation, where information is located in one suspect's phone that incriminates another. It may take a couple months to develop probable cause to arrest the other suspect, but evidence would still need to be retained from months prior. As currently written, the only paragraph in the bill tending to address this need to retain the evidence for a longer period

in the investigation requires that there be a finding by the court that the conditions justifying the initial voluntary disclosure persist and probable cause to believe the information constitutes criminal evidence. Finally, it would like more time to file an emergency order that would take into consideration holidays and weekend.

DoIT suggests looking to the laws in Minnesota and Ohio which have Electronic Communication Privacy laws that follow a similar pattern and have similar language. The language similarities stem from federal law 18 U.S. Code Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications. For example, Minnesota, Ohio and the U.S. code define "investigative or law-enforcement officer;" this bill offers no definition for that word.

ABS/jle/al