City Council

CONSENT CALENDAR
June 25, 2013

To: Honorable Mayor and Members of the City Council

From: Councilmember Jesse Arreguín

Subject: Senate Bill 467: Email Privacy

RECOMMENDATION
Adopt a Resolution supporting Senate Bill (SB) 467, authored by Senator Mark Leno, which would require a search warrant when a governmental agency is seeking the contents of certain electronic communications, such as email. Copies of the Resolution to be sent to Governor Jerry Brown, Senate President Pro Tem Darrell Steinberg, Senators Mark Leno and Loni Hancock, Assembly Speaker John A. Perez, and Assemblymember Nancy Skinner.

BACKGROUND:
SB 467 updates California's electronic privacy law into the modern age, ensuring emails and other electronic communications content are protected from warrantless government intrusion when stored online and in the cloud.

Under SB 467, no government entity shall obtain the contents of an electronic communication without a warrant issued by an officer of the court, regardless of how long it has been in electronic storage or whether it has been opened or unopened.

Though SB 467 is applicable only within the jurisdiction of the State of California, it is another step in affirmatively establishing the reasonable expectation of privacy of emails and that the people do not relinquish their privacy simply because they entrust a third party for transmission and storage, or that the email is “opened” and 180 days have passed.

Previously, under the Electronic Communications Privacy Act (ECPA), the Federal government only needed a subpoena and prior notice (as opposed to a search warrant and probably cause) under the “Third Party Doctrine” to compel disclosure by an Internet Service Provider (ISP). The Third Party Doctrine holds that ‘that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information.” Additionally, it is held that after 180 days, emails that have been opened are analogous to an unsealed envelope –it contents are no longer reasonably private.

Fortunately, in *United States v. Warshak* (2010), the Court held that the Storage Communications Act (SCA) portion of the ECPA is unconstitutional to the extent that it allows the government to obtain emails without a warrant, establishing that there is a reasonable expectation to privacy for emails stored on third party servers and that these

Martin Luther King Jr. Civic Center Building ● 2180 Milvia Street, 5th Floor, Berkeley, CA 94704 ● Tel: (510) 981-7140
Fax: (510) 981-7144 ● TDD: (510) 981-6903 ● E-Mail: jarreguin@cityofberkeley.info ● Web: www.jessearreguin.com

emails are subject to full Fourth Amendment protections. However, the issue of privacy is still very much salient, from the IRS admitting to using administrative subpoenas to access to emails (see attached article) to recent revelations that the National Security Administration have been collecting nationwide call data without probable cause.

SB 467 is supported by the following groups:

Electronic Frontier Foundation (source)
American Civil Liberties Union
California Attorneys for Criminal Justice
California Newspaper Publishers Association
California Public Defenders Association
The First Amendment Coalition

FISCAL IMPACTS
None.

CONTACT PERSON:
Jesse Arreguin, Councilmember, District 4 981-7140

Attachments:

1. Resolution
2. Copy of SB 467
3. Slate Article, “The IRS Doesn’t Think “Reasonable Expectation of Privacy” Applies to Your Emails”

RESOLUTION NO.

SUPPORTING SENATE BILL 467, WHICH WOULD REQUIRE A SEARCH WARRANT WHEN A GOVERNMENTAL AGENCY IS SEEKING THE CONTENTS OF CERTAIN ELECTRONIC COMMUNICATIONS

WHEREAS, Californians have a reasonable expectation of privacy when they send and receive emails, and they do not relinquish that expectation of privacy simply because they entrust a third party to transmit and store those emails –emails that are only accessible through private passcodes; and

WHEREAS, certain electronic communications, such as emails, deserve full Fourth Amendment protections and that Government should have probable cause and a search warrant to obtain private emails; and

WHEREAS, Senate Bill 467, authored by Senator Mark Leno, would require a search warrant when a governmental agency is seeking the contents of certain electronic communications; and

WHEREAS, our civil liberties, especially the Right to Privacy, deserve the utmost protection and preservation in light of increasing governmental intrusions.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City of Berkeley does hereby support Senate Bill 467, introduced by Senator Mark Leno, which would require a search warrant when a governmental agency is seeking the contents of certain electronic communications.

BE IT FURTHER RESOLVED that copies of this Resolution be sent to Governor Jerry Brown, Senate President Pro Tem Darrell Steinberg, Senators Mark Leno and Loni Hancock, Assembly Speaker John A. Perez, and Assemblymember Nancy Skinner.

AMENDED IN SENATE APRIL 1, 2013

SENATE BILL **No. 467**

Introduced by Senator Leno

February 21, 2013

An act *to amend Section 1524.2 of, and to add Sections 1524.4, 1524.5, 1524.6, and 1524.7 to, the Penal Code,* relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 467, as amended, Leno. Privacy: electronic communications: warrant.

Existing law authorizes a court or magistrate to issue a warrant for the search of a place and the seizure of property or things identified in the warrant where there is probable cause to believe that specified grounds exist. Existing law also provides for a warrant procedure for the acquisition of stored communications *and other identifying information* in the possession of a *foreign corporation that is a* provider of electronic communication ~~service~~ *services* or remote computing ~~service~~ *services to the general public, and procedures for a California corporation that provides electronic communication services or remote computing services to the general public when served with a warrant issued by a court in another state.*

~~This bill would declare the intent of the Legislature to enact legislation prohibiting a government entity from obtaining the contents of a wire or electronic communication from a provider of electronic communication service or remote computing service that is stored, held, or maintained by that service without a valid search warrant.~~

This bill would delete the warrant requirement that the providers of electronic communication services or remote computing services be providing those services to the general public.

This bill would prohibit a governmental entity, as defined, from obtaining the contents of a wire or electronic communication from a provider of electronic communication services or remote computing services that is stored, held, or maintained by that service provider without a valid search warrant issued by a duly authorized magistrate, with jurisdiction over the offense under investigation, using established warrant procedures. The bill would require, within 3 days after a governmental entity receives those contents from a service provider pursuant to the warrant, the governmental entity to serve upon or deliver to the subscriber, customer, or user a copy of the warrant and a notice, as specified, including certain information. The bill would authorize a delay in serving the warrant notice, as provided.

This bill would prohibit, except as provided, a person or entity providing electronic communication services or remote computing services from knowingly divulging to any person or entity the contents of a wire or electronic communication that is stored, held, or maintained by that service provider.

Any knowing or intentional violation of these provisions, except as provided, would be subject to a civil action with appropriate relief, including, but not limited to, actual damages of not less than $1,000, possible punitive damages, attorney's fees, and court costs.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

1 *SECTION 1. Section 1524.2 of the Penal Code is amended to*
2 *read:*
3 1524.2. (a) As used in this section, the following terms have
4 the following meanings:
5 (1) The terms "electronic communication services" and "remote
6 computing services" shall be construed in accordance with the
7 Electronic Communications Privacy Act in Chapter 121
8 (commencing with Section 2701) of Part I of Title 18 of the United
9 State Code Annotated. ~~This section shall not apply to corporations~~
10 ~~that do not provide those services to the general public.~~
11 (2) An "adverse result" occurs when notification of the existence
12 of a search warrant results in:
13 (A) Danger to the life or physical safety of an individual.
14 (B) A flight from prosecution.

(C) The destruction of or tampering with evidence.

(D) The intimidation of potential witnesses.

(E) Serious jeopardy to an investigation or undue delay of a trial.

(3) "Applicant" refers to the peace officer to whom a search warrant is issued pursuant to subdivision (a) of Section 1528.

(4) "California corporation" refers to any corporation or other entity that is subject to Section 102 of the Corporations Code, excluding foreign corporations.

(5) "Foreign corporation" refers to any corporation that is qualified to do business in this state pursuant to Section 2105 of the Corporations Code.

(6) "Properly served" means that a search warrant has been delivered by hand, or in a manner reasonably allowing for proof of delivery if delivered by United States mail, overnight delivery service, or facsimile to a person or entity listed in Section 2110 of the Corporations Code.

(b) The following provisions shall apply to any search warrant issued pursuant to this chapter allowing a search for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services ~~to the general public~~, where those records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications.

(1) When properly served with a search warrant issued by the California court, a foreign corporation subject to this section shall provide to the applicant, all records sought pursuant to that warrant within five business days of receipt, including those records maintained or located outside this state.

(2) Where the applicant makes a showing and the magistrate finds that failure to produce records within less than five business days would cause an adverse result, the warrant may require production of records within less than five business days. A court may reasonably extend the time required for production of the records upon finding that the foreign corporation has shown good cause for that extension and that an extension of time would not cause an adverse result.

(3) A foreign corporation seeking to quash the warrant must seek relief from the court that issued the warrant within the time required for production of records pursuant to this section. The issuing court shall hear and decide that motion no later than five court days after the motion is filed.

(4) The foreign corporation shall verify the authenticity of records that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Those records shall be admissible in evidence as set forth in Section 1562 of the Evidence Code.

(c) A California corporation that provides electronic communication services or remote computing services ~~to the general public~~, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by a California court.

(d) No cause of action shall lie against any foreign or California corporation subject to this section, its officers, employees, agents, or other specified persons for providing records, information, facilities, or assistance in accordance with the terms of a warrant issued pursuant to this chapter.

SEC. 2. Section 1524.4 is added to the Penal Code, to read:

1524.4. (a) A governmental entity shall not obtain from a provider of electronic communication services or remote computing services the contents of a wire or electronic communication that is stored, held, or maintained by that service provider without a valid search warrant issued by a duly authorized magistrate, with jurisdiction over the offense under investigation, using procedures established pursuant to this chapter.

(b) Within three days after a governmental entity receives those contents from a service provider, the governmental entity shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant, to the subscriber, customer, or user a copy of the warrant and a notice that includes the information specified in paragraph (1) of and subparagraph

(A) of paragraph (2) of subdivision (c) of Section 1524.5, except that delayed notice may be given pursuant to Section 1524.5.

(c) For purposes of this chapter, "governmental entity" means a department or agency of the state or any political subdivision thereof, or an individual acting for or on behalf of the state or any political subdivision thereof.

SEC. 3. Section 1524.5 is added to the Penal Code, to read:

1524.5. (a) (1) A governmental entity acting under Section 1524.2 may, when a search warrant is sought, include in the application a request, supported by sworn affidavit, for an order delaying the warrant notification required under subdivision (b) of Section 1524.4.

(2) The court shall grant the request if the court determines that there is reason to believe that notification of the existence of the warrant may have an adverse result as defined in paragraph (2) of subdivision (a) of Section1524.2, but only for the period of time that the court finds there is reason to believe that the warrant notification may have that adverse result, and in no event shall the period of time for the delay exceed 90 days.

(b) The court may grant extensions of the delay of the warrant notification, provided for in subdivision (b) of Section 1524.4, of up to 90 days each on the same grounds as provided in subdivision (a).

(c) Upon expiration of the period of delay of the warrant notification under subdivision (a) or (b), the governmental entity shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant, the customer, user, or subscriber a copy of the warrant together with a notice that does both of the following:

(1) States with reasonable specificity the nature of the governmental inquiry.

(2) Informs the customer, user, or subscriber all of the following:

(A) That information maintained for the customer or subscriber by the service provider named in the process or request was supplied to, or requested by, that governmental entity and the date on which the supplying or request took place.

(B) That warrant notification to the customer or subscriber was delayed.

(C) The grounds for the court's determination to grant the delay.

(D) Which provisions of this chapter authorized the delay.

SEC. 4. Section 1524.6 is added to the Penal Code, to read:

1524.6. (a) Except as provided in subdivision (b), a person or entity providing an electronic communication service or remote computing service shall not knowingly divulge to any person or entity the contents of a wire or electronic communication that is stored, held, or maintained by that service.

(b) A service provider described in subdivision (a) may divulge the contents of a communication under any of the following circumstances:

(1) To an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

(2) As otherwise authorized in Section 1524.2.

(3) With the lawful consent of the originator, an addressee, or intended recipient of the communication, or the subscriber in the case of remote computing service.

(4) To a person employed or authorized or whose facilities are used to forward the communication to its destination.

(5) As may be necessary incident to the rendition of the service or to the protection of the rights or property of the provider of that service.

(6) To a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime.

(7) To a governmental entity, if the provider, in good faith, believes that an emergency involving the danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

SEC. 5. Section 1524.7 is added to the Penal Code, to read:

1524.7. (a) Except as provided in subdivision (d) of Section 1524.2, any provider of electronic communication service or remote computing service, subscriber, or other person aggrieved by any knowing or intentional violation of this chapter may, in a civil action, recover from the person, entity, or governmental entity that committed the violation, relief as may be appropriate.

(b) In a civil action under this section, appropriate relief includes, but is not limited to, all of the following:

(1) Preliminary and other equitable or declaratory relief.

(2) Damages under subdivision (c).

(3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(c) (1) The court may assess as damages, in a civil action, the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person be entitled to recover less than the sum of one thousand dollars ($1,000).

(2) If the violation is willful or intentional, the court may assess punitive damages.

~~SECTION 1. It is the intent of the Legislature to enact legislation prohibiting a government entity from obtaining the contents of a wire or electronic communication from a provider of electronic communication service or remote computing service that is stored, held, or maintained by that service without a valid search warrant.~~

O

The IRS Doesn't Think "Reasonable Expectation of Privacy" Applies to Your Emails

By Ryan Gallagher
Posted Wednesday, April 10, 2013, at 5:59 PM

Slate.com

The IRS Criminal Tax Division doesn't think the Fourth Amendment should apply to email Photo by Chris Hondros/Getty Images

With Tax Day less than a week away in the United States, you probably don't need another reason to dislike the IRS. But here's one anyway: Newly released documents show that in recent years, the agency has claimed American Internet users "do not have a reasonable expectation of privacy" when it comes to their emails being snooped on.

The documents, obtained by the ACLU under the Freedom of Information Act and published today, reveal that in 2009, the Criminal Tax Division at the IRS claimed in an internal handbook that in general "the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server." This claim may have been rooted in a reading of a controversial loophole contained in the Electronic Communications Privacy Act, which enables agencies to obtain email older than 180 days without a search warrant.

In 2010, a significant appeals court judgment held in United States v. Warshak that email was protected by the Fourth Amendment, and that government agents should obtain a probable cause warrant from a court before compelling email providers to hand over users' messages—regardless of whether they had been stored on a server for more than 180 days. This is the highest legal standard, requiring authorities to show there is "reasonable basis" for believing the search will yield evidence of a crime.

But despite that ruling, ECPA's requirements have been "inconsistent, confusing, and uncertain," as Richard Salgado, Google's legal director of law enforcement and information security, has put it. IRS emails obtained by the ACLU demonstrate this, as they suggest that that the IRS avoided having to always obtain a warrant by continuing to exploit the ECPA loophole. The loophole enables authorities to get their hands on emails older than 180 days with an administrative subpoena—which requires merely showing that the information sought is "relevant" to an ongoing investigation. A special counsel for the IRS in one email exchange seems dismissive of the Warshak ruling, stating that "I have not heard anything related to this opinion. We have always taken the position that a warrant is necessary when retrieving e-mails that are less than 180 days old"—implying that emails more than 180 days old can still be obtained by other, easier means. (It's possible that other agencies have adopted a similar position, given the confusion over ECPA. The ACLU says it has lodged FOIA requests with the FBI and other components of the Justice Department to find out.)

Last month, lawmakers proposed new legislation that aims to update ECPA by scrapping the contentious 180-days clause. Even the Justice Department—which rarely takes the same side as civil liberties advocates—is backing the change: In March, a DOJ representative admitted to the House judiciary committee that there is

"no principled basis to treat email less than 180 days old differently than email more than 180 days old." This marked a stark reversal for the DOJ, which had previously been aggressively opposed to privacy-enhancing reforms of ECPA.

The ACLU is criticizing the IRS for its lack of clarity on the issue and demanding that the agency "let the American public know whether it obtains warrants across the board when accessing people's email." The rights group is also calling on the IRS to "formally amend its policies to require its agents to obtain warrants when seeking the contents of emails, without regard to their age."

It's worth noting, though, that not all providers will play along if the IRS is still attempting to obtain emails without a warrant. Earlier this year, in a move lauded by privacy groups, Google said that it is effectively ignoring the 180-days ECPA loophole by always requiring a search warrant from authorities seeking to obtain user content stored using its Gmail, Google Drive, or other services. It is unclear whether other providers—such as Microsoft and Yahoo—have similar policies.

The IRS did not immediately respond to a request for comment. I'll update this post as and when I receive anything.

Update, April 11, 6:11 p.m.: The IRS has issued the below statement:

> Respecting taxpayer rights and taxpayer privacy are cornerstone principles for the IRS. Our job is to administer the nation's tax laws, and we do so in a way that follows the law and treats taxpayers with respect.
>
> Contrary to some suggestions, the IRS does not use emails to target taxpayers. Any suggestion to the contrary is wrong.