

SB 178 (LENO and ANDERSON)

Principal Co-author: Assemblymember Gatto

Co- authors: Senators Cannella, Gaines, Hertzberg, Hill, McGuire, Nielsen and Roth
Assemblymembers Chiu, Gordon, Maienschein, Obernolte, Quirk,
Ting and Weber

THE CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT *Safeguard Californians, Spur Innovation, Support Public Safety*

SUMMARY

SB 178 safeguards the electronic information of California residents and supports innovation in the digital economy by updating state privacy law to match our expanding use of digital information.

Californians are guaranteed robust constitutional rights to privacy and free speech and the Legislature has long been a leader in protecting individual privacy; however, the emergence of new technology has left California's statutory protections behind. This bill will provide needed protection against warrantless government access to mobile devices, email, text messages, digital documents, metadata, and location information.

BACKGROUND

California residents use technology every day to connect, communicate, work and learn. Our state's leading technology companies rely on consumer confidence in these services to help power the California economy.

But consumers are increasingly concerned about warrantless government access to their digital information, and for good reason. While technology has advanced exponentially, California privacy law has remained largely unchanged. Law enforcement is increasingly taking advantage of outdated privacy laws to turn mobile phones into tracking devices and to access emails, digital documents, and text messages without proper judicial oversight.ⁱ For example:

- Google has had a **250% jump** in government demands in just the past five years.

- AT&T received over 64,000 demands for location information in 2014, nearly **70% increase** in a single year.ⁱⁱ
- Verizon received over 15,000 demands for location data in the first half of 2014, **only 1/3 with a warrant**.
- Twitter had a **52% jump** in the number of demands this year, only 20% were with a warrant, and more than **11% of the demands came from California**.ⁱⁱⁱ

As a result, public confidence in technology has been badly damaged. Polls consistently show that consumers believe that their electronic information is sensitive and that current law does not provide adequate protection from government monitoring.^{iv} Companies in turn are increasingly concerned about the loss of consumer trust and its business impact.

Courts and legislatures around the country are recognizing the need to update privacy laws for the digital age. In two recent decisions, *United States v. Jones* and *Riley v. California*, the U.S. Supreme Court upheld Fourth Amendment privacy rights against warrantless government surveillance. Justice Alito in *Jones* also prompted lawmakers to take action, noting that in circumstances involving dramatic technological change "a legislative body is well suited to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."

Sixteen state legislatures throughout the country have already heeded Justice Alito's call and enacted new legislation, with 10 states safeguarding location information^v and 6 states protecting electronic communications content.^{vi} The White House has called on lawmakers to update the law to "ensure the standard of

protection for online, digital content is consistent with that afforded in the physical world.” A federal bill on the subject garnered over 270 bipartisan co-sponsors in the United States Congress.

California has fallen behind states as diverse as Texas, Maine, and Utah that have already enacted legislation to safeguard rights, spur innovation, and support public safety.

SOLUTION

SB 178 heeds the call in *Jones* for the legislature to balance privacy and public safety, and will spur innovation by updating state privacy law to match our expanding use of digital information. The bill provides:

- Appropriate Warrant Protection for Digital Information
- Proper Transparency & Oversight
- Appropriate Exceptions for Public Safety

SB 178 will ensure that, in most cases, the police must obtain a warrant from a judge before accessing a person’s private information, including data from personal electronic devices, email, digital documents, text messages, and location information.

The bill also includes thoughtful exceptions to ensure that law enforcement can continue to effectively and efficiently protect public safety in emergency situations. Notice and enforcement provisions in the bill provide proper transparency and judicial oversight to ensure that the law is followed.

Californians should not have to choose between using new technology and keeping their personal lives private. The business impacts of eroding public confidence brought on by unwarranted government monitoring has prompted California’s leading technology companies to partner with the state’s premiere privacy advocates in supporting the enactment of SB 178, The California Electronic Communications Privacy Act (CalECPA).

SUPPORT

Adobe Inc.
Airbnb
American Civil Liberties Union of California
American Library Association
Apple Inc.
Asian Americans Advancing Justice (AAAJ)
Bay Area Council
California Chamber of Commerce (CalChamber)
California Newspaper Publishers Association
California Attorneys for Criminal Justice (CACJ)
California Public Defenders Association
Center for Democracy and Technology
Center for Media Justice
Centro Legal de la Raza
Citizens for Criminal Justice Reform
Civil Justice Association of California (CJAC)
Common Sense Media
ConnectSafely
Color of Change
Consumer Action
Consumer Federation
Council on American-Islamic Relations (CAIR)
Dropbox
Electronic Frontier Foundation
Engine
Facebook
Foursquare
Google
Internet Archive
Legal Services for Prisoners With Children
LinkedIn
Media Alliance
Microsoft
Mozilla
NameCheap
National Center for Lesbian Rights (NCLR)
New America: Open Technology Institute
Privacy Rights Clearinghouse
reddit
Restore the 4th
San Diego Police Officers Association
Small Business California
TechNet
Tech Freedom
The Internet Association
The Utility Reform Network (TURN)
Twitter

CONTACT

CONTACT : Office of Senator Mark Leno
916-651-4011
Version: September 2, 2015

ⁱ For example, Google's transparency report shows a 250% jump demands from U.S. law enforcement in just the past five years, including 32,000 requests in the first 6 months of 2014 alone.

ⁱⁱ AT&T's 2013 and 2014 transparency reports available at

http://about.att.com/content/dam/csr/transpreport/ATT_Transparency%20Report.pdf and

http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf

ⁱⁱⁱ Twitter's transparency report for July 2015 available at <https://blog.twitter.com/2015/expanding-the-scope>

^{iv} According to a recent Pew Internet & Society survey, 80% of adults feel that Americans are rightly concerned about government monitoring of internet communications, 70% of social networking site users express concern about government access, and 75% or more believe that their email messages, text messages, and location information are sensitive.

^v IN H.B. 1009 (2014); IL S.B. 2808 (2013); MD S.B. 698 (2013); ME S.P. 157 (2013); MN S.F. 2466 (2014); MT H.B. 603 (2013); TN S.B. 2087 (2013); UT H.B. 128 (2014); WI A.B. 536 (2013); VA H.B. 1408 (2015).

^{vi} HI H.B. 1641 (2013); MD S.B. 698 (2013); ME S.P. 484 (2013); TX H.B. 2268 (2013); UT H.B. 128 (2014); VA H.B. 1408 (2015).