ASSEMBLY THIRD READING
AB 904 (Chau)
As Amended January 16, 2020
Majority vote

SUMMARY:

Clarifies that if a law enforcement agency utilizes software to track a person's movements, whether in conjunction with a third party or by interacting with a person's electronic device, the provisions for obtaining a tracking device search warrant apply.

Major Provisions
Specify that the reference to "software" is not intended to expand the authority of a government entity to use software for surveillance purposes under any law.

COMMENTS:

Constitutional Protections Against Unreasonable Searches and Seizures: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." (United Constitution, 4th Amendment)

As technology advances, the courts and lawmakers should be careful not to "embarrass the future" by making decisions that are in discord with the "progress of science." This sentiment is at the core of the holdings in three recent United States Supreme Court cases, Jones, Riley and Carpenter which establish warrant requirements for use of and access to electronic communications and devices to surveil a person.

In tandem with the evolving Supreme Court case law, California passed the CalECPA with SB 178 (Leno), Chapter 651, Statutes of 2015. SB 178 established in statute that law enforcement officials are required to obtain a warrant before "searching" a third party's electronic records for law enforcement purposes, either by actually searching a person's cellphone or electronic device, or by requesting that information from a third party which holds it.

According to the Author:
According to the author, "The rights of individuals against unlawful search and seizure are enshrined in both the Constitutions of the United States (through the Fourth Amendment) and the State of California. Having stood for over 200 years, this basic human right has consistently been reinterpreted to account for changes in government, technology, and society. Judicial understanding of this right has morphed from an explicit right of privacy within the home and personal documents, to an expansive protection against the collection of information by the government in a great many applications. Most recently, the United States Supreme Court recognized in Carpenter v. United States that the use of cell phone location information by law enforcement is an invasion of personal privacy, which requires the granting of a search warrant.

"This decision certainly represents a landmark case in the jurisprudence of the Supreme Court, but had limited applicability to the residents of California because this specific requirement has been applied to law enforcement agencies in California since 2012. With the rest of the country following suit, it is important that California continues to look ahead at the changing landscape of technology and maintains the lead in protecting our residents against unlawful search and seizure.

"Penal Code Section 1534 currently requires search warrants prior to an officer 'installing a tracking device or serving a warrant on a third-party possessor of the tracking data.' It is, however, no longer necessary for an officer to make physical contact with a device, person, or vehicle to 'install' a 'device' in order to track an individual. On the contrary, a government official need only have wireless access to download tracking software that will provide investigators with far more information than just a person's or a vehicle's location.

"AB 904 would make clear that a tracking device includes any software that permits the tracking of the movement of a person or object for purposes of the statute."

Arguments in Support:
According to the California Attorneys for Criminal Justice, "This bill closes a loophole in the law that could allow for the software-based tracking of individuals by law enforcement without a warrant. Search warrants protect the public from unreasonable searches and seizures, a constitutional right that CACJ supports and believes should be expanded in the face of new technology."

Arguments in Opposition:
According to the Electronic Frontier Foundation¸ "A.B. 904 would amend the California Electronic Communications Privacy Act (CalECPA), a watershed statute that established bright-line rules for California government entities seeking to obtain, retain, and use digital information. CalECPA was drafted with the specific intention of reinforcing the privacy rights set forth at Article 1, Section 1, of the California Constitution—a response to the 'modern threat to personal privacy' posed by increased surveillance and then-emerging data collection technology. White v. Davis, 13 Cal.3d 757, 774 (1975).

"We are extremely concerned that A.B. 904 would create and authorize, for any California government entity, an entirely new 'procedure for accessing or installing software into an electronic device.' CalECPA already allows access to information stored on a device. A.B. 904's new procedure would seem to expressly authorize the government to 'access' applications like cameras, microphones, or electronic mail on a person's smartphone, tablet, or computer. At the very least, this could allow the government to use a person's device as a hidden camera or microphone, or as a launching pad to covertly access email or other documents or communications that are not stored on the device."

FISCAL COMMENTS:

Unknown. This bill is keyed non-fiscal by the Legislative Counsel.

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0
YES: Chau, Kiley, Bauer-Kahan, Berman, Calderon, Kalra, Gallagher, Irwin, Obernolte, Smith, Wicks

ASM PUBLIC SAFETY: 8-0-0
YES: Jones-Sawyer, Lackey, Bauer-Kahan, Diep, Kamlager, Quirk, Santiago, Wicks

UPDATED:

VERSION: January 16, 2020

CONSULTANT: Nikki Moore / PUB. S. / (916) 319-3744 FN: 0002614