SENATE COMMITTEE ON PUBLIC SAFETY

Senator Steven Bradford, Chair
2021 - 2022 Regular

Bill No:	SB 1000	**Hearing Date:**	April 19, 2022
Author:	Becker		
Version:	March 16, 2022		
Urgency:	No	**Fiscal:**	Yes
Consultant:	AB		

Subject: ***Law enforcement agencies: radio communications***

HISTORY

Source: California News Publisher's Association

Prior Legislation: AB 1555 (Gloria, 2019), died in Assembly Governmental Organization

Support: CalAware, California Broadcasters Association; California Public Defenders Association; City of Palo Alto; First Amendment Coalition; National Association of Black Journalists of Los Angeles; National Press Photographers Association; National Writers Union; Oakland Privacy; Online News Association Local Los Angeles; Orange County Press Club; Radio Television Digital News Association; San Diego Pro Chapter of the Society of Professional Journalists

Opposition: California State Sheriff's Association

PURPOSE

The purpose of this bill is to ensure public access to law enforcement radio communications and require law enforcement agencies to prevent or substantially minimize criminal justice information or personally identifiable information from being broadcast in a manner that is accessible to the public.

Existing law, the California Constitution, declares the people's right to transparency in government. ("The people have the right of access to information concerning the conduct of the people's business, and therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny....") (Cal. Const., art. I, Sec. 3.)

Existing law, the California Public Records Act, generally provides that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. (Gov, Code § 6250 et. seq.)

Existing law provides that public records are open to inspection at all times during the office hours of the state or local agency and every person has a right to inspect any public record, except as provided. (Gov. Code § 6253)

Existing law exempts from the California Public Records Act the disclosure of investigations conducted by the office of the Attorney General and the Department of Justice, the Office of

Emergency Services and any state or local police agency, or any investigatory or security files compiled by any other state or local police agency, or any investigatory or security files compiled by any other state or local agency for correctional, law enforcement, or licensing purposes. (Gov. Code § 6254(f).)

Existing law provides that the Commission on Peace Officer Standards and Training (POST) shall conspicuously post on their internet websites all current standards, policies, practices, operating procedures, and education and training materials that would otherwise be available to the public if a request was made pursuant to the California Public Records Act. (Penal Code §13650).

Existing law establishes the Legislature's intent to provide an efficient law enforcement communications network available to all public agencies of law enforcement, and that such a network be established and maintained in a condition adequate to the needs of law enforcement. (Gov. Code §15151).

Existing law requires the Department of Justice (DOJ) to maintain a statewide telecommunications system of communication for the use of law enforcement agencies (CLETS), and provides that CLETS shall be under the direction of the Attorney General, and shall be used exclusively for the official business of the state and any city, county, city and county, or other public agency. (Gov. Code §§15152, 15153).

Existing law requires the Attorney General to appoint an advisory committee on CLETS, and establishes various requirements and responsibilities related thereto. (Gov. Code §§15154 – 15159)

Existing law requires the Attorney General to adopt and publish the operating policies, practices and procedures, and conditions of qualification and membership, of CLETS. (Gov. Code §15160).

Existing law requires the DOJ to provide a basic telecommunications network consisting of no more than two relay or switching centers in the state and circuitry and terminal equipment in one location only in each county in the state. (Gov. Code §15161).

Existing law requires that CLETS provide service to any law enforcement agency qualified by the CLETS advisory committee which, at the agency's own expense, desires connection through the county terminal. (Gov. Code §15163).

Existing law prohibits any person not authorized by the sender, who intercepts any public safety radio service communication, by use of a scanner or any other means, from using that communication to assist in the commission of a criminal offense or to avoid or escape arrest, trial, conviction, or punishment or who divulges to any person he or she knows to be a suspect in the commission of any criminal offense, the contents of that communication concerning the offense with the intent that that individual may avoid arrest, trial, conviction or punishment. (Penal Code §636.5)

This bill requires each law enforcement agency, as defined, to ensure that all radio communications, as defined, are accessible to the public by January 1, 2023.

This bill defines "law enforcement agency" as 'a department or agency of the state, or any political subdivision thereof, that employs any peace officer and that has the primary function of providing uniformed patrol and general law enforcement services to the public,' and specifies the types of agencies included in that definition.

This bill defines "radio communications" as 'verbal communications that are broadcast over a radio frequency either from a dispatch center to field personnel, from field personnel to a dispatch center, or between field personnel, and are accessible to all personnel monitoring that frequency.' However, "radio communications" does not include private communications between two devices, such as a cellular telephone, or the transmittal of data to or from a mobile data terminal, tablet, text messaging device or similar device.

This bill specifies that a law enforcement agency may comply with the public access requirement in any manner that provides reasonable public access to radio communications including, without limitation, any of the following means:

- Use of unencrypted radio communications on a radio frequency that is able to be monitored by commonly available radio scanning equipment.
- Online streaming of radio communications accessible through the agency's internet website.
- Upon request and for a reasonable fee, providing access to encrypted communications to any interested person.

This bill specifies that the public access requirement does not apply to any encrypted radio channel that is used exclusively for the exchange or dissemination of confidential information or to any encrypted radio channel that is used for tactical operations, undercover operations, or other communications that would unreasonably jeopardize public safety or the safety of officers if made public.

This bill requires each law enforcement agency to enact policies that prevent or substantially minimize criminal justice information or personally identifiable information directly obtained through CLETS from being broadcast in a manner that is accessible to the public.

This bill specifies that a law enforcement agency may comply with this confidentiality requirement in any manner that safeguards confidential CLETS information, including, without limitation, any of the following means:

- The use of an encrypted channel for the exchange or dissemination of confidential information
- Transmission of confidential information to a mobile data terminal, tablet, or other text display device.
- Communication of confidential information via telephone or other private device-to-device communication

This bill specifies that the confidentiality requirement does not apply to confidential information that has previously been made public through a bulletin, alert or other means or to the broadcast of confidential information that is immediately necessary for the safety of the public or the safety of officers under circumstances where compliance would otherwise be unreasonable.

This bill requires each law enforcement agency to adopt a written policy implementing its provisions no later than January 1, 2023.

This bill specifies that it does not limit the responsibility of any entity not covered by its provisions to comply with any law or regulation regarding the usage of CLETS.

COMMENTS

1. Need for This Bill

According to the author:

> "For 80 years, news outlets, journalists and the public have had access to police radio communications. This access is important for police transparency, accountability, and reporting activity to the public. However, in October 2020, the California Department of Justice's California Law Enforcement Telecommunications System (CLETS) issued a memo regarding the requirement for police agencies to protect identifying information via encryption. As a result, dozens of California police departments, including much of the Bay Area and San Francisco, have made the poor decision to fully encrypt their communications, barring the press and the public from access without legislative or public comment. There are 13 Santa Clara County law enforcement agencies and almost all have encrypted radio in the name of protecting sensitive information. This problem is likely to become statewide if corrective action is not taken. Now is not the time to reduce public access to police activity. Access to information regarding police activity is not an "operational change" that should be taken without input from the public, the media, or city, county and state elected officials".

2. Public Interest in and Access to Police Records

The right to transparency in government is a cornerstone of California's democracy, enshrined in its constitution and implemented by various statutes and regulations.[1] One of these statutes, the California Public Records Act (CPRA), enacted in 1968, recognizes that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[2] The California Supreme Court has reinforced that this right is especially important in the context of law enforcement officers and agencies:

> "The public's interest in the qualifications and conduct of peace officers is substantial […] Peace officers hold one of the most powerful positions in our society; our dependence on them is high and the potential for abuse of power is far from insignificant. A police officer possesses both the authority and the ability to exercise force. Misuse of his authority can result in significant deprivation of constitutional rights and personal freedoms, not to mention bodily injury and financial loss. The public has a legitimate interest not only in the conduct of individual officers, but also in how […] local law enforcement agencies conduct the public's business."[3]

---

[1] California Constitution, Article 1, §3

[2] Government Code §6250

[3] *Commission on Peace Officer Standards & Training v. Superior Court*, 42 Cal. 4th 278 (2007), at 299-300.

Recent years have seen an increase in legislation requiring law enforcement agencies to collect and report specific data and disclose various records and policies to the public. In 2015, AB 953 (Weber, Ch. 466, Stats. of 2015) and AB 71 (Rodriguez, Ch. 462, Stats. of 2015) generally required law enforcement to report data on police stops and use of force incidents, respectively. In 2018, the Legislature adopted SB 1421 (Skinner, Ch. 988, Stats. of 2018), required that certain records relating to police misconduct and serious uses of force be made publicly available under the CPRA. SB 1421 was co-sponsored by the California News Publisher's Association (CNPA), who wrote in support of the bill that it would finally allow the press to "fully investigate the activity of powerful public institutions," and that "recent events, like the death of Stephon Clark […] underscore the immense public concern related to police and community interactions."[4] The CNPA is also the sponsor of this bill, and argues that media access to police radio communications is essential to reporting critical information to the public:

> "To fulfil this duty to the public to provide accurate and timely information, journalists across California – and throughout the United States – monitor police and first responder agency scanners. The public has turned to their local publications for the latest updates on raging wildfires, mass shootings, and other major news events, a public service that is made possible by monitoring radio transmissions. In a recent survey of our members, CNPA found that 78 percent of our members find monitoring police radio transmissions is very valuable in reporting on breaking news or developing situations."

3. Police Radio Communications

The Federal Communications Commission (FCC) is responsible for assigning licenses to individual law enforcement agencies for the operation of their radio systems on the "public safety spectrum," which serves the telecommunications needs of most public safety agencies across the country.[5] Until very recently, most police radio communications in California have been unencrypted, which means that the public can access police radio transmissions using a radio scanning device. With the development of online radio streaming, many unencrypted police radio channels have become accessible via internet websites that provide a livestream.[6]

The advent of digital radio "trunking" has spawned broader debates about whether police radio communications should remain largely unencrypted. "Trunked" radio systems centrally manage a pool of channels or frequencies and automatically switch users to whatever channel is open at a given time, allowing those channels to be shared by a large number of users without their conversations interfering with each other.[7] As trunking has facilitated the public's access to unencrypted police radio channels, some have argued that more encryption is necessary to prevent criminals from exploiting that access and threatening officer and public safety. Conversely, proponents of increased access argue that more encryption would reduce officer accountability and infringe upon the public's right to government records.

---

[4] "Brown Signs Bill to Shine Light on California Police Conduct." *Courthouse News.* 1 October 2018. https://www.courthousenews.com/brown-signs-bill-to-shine-light-on-california-police-conduct/

[5] "Public Safety Spectrum." *Federal Communications Commission*. https://www.fcc.gov/public-safety/public-safety-and-homeland-security/policy-and-licensing-division/public-safety-spectrum

[6] For instance, Sacramento County Sheriff and City Police radio can be streamed at https://www.broadcastify.com/listen/feed/5688.

[7] "Trunked Radio System." *ScienceDirect.* https://www.sciencedirect.com/topics/computer-science/trunked-radio-system

4. October 2020 CLETS Memo and Response

Implemented in the 1970's, the California Law Enforcement Telecommunications System (CLETS) is a data interchange network administered by the California Department of Justice (DOJ). CLETS provides law enforcement and criminal justice agencies access to databases maintained by state and federal agencies, and allows for the exchange of administrative messages to agencies within California, other states, and Canada. Its primary function is to provide law enforcement with individuals' criminal and driving records, often in real time as officers conduct investigations and respond to calls in the field. In October 2020, the DOJ division charged with administering CLETS issued a memo directing law enforcement agencies to take steps to restrict access to Criminal Justice Information (CJI) and Personally Identifiable Information (PII).[8] According to the memo, agencies were permitted to comply with its directives via the following methods:

- "Encryption of radio traffic pursuant to FBI Criminal Justice Information Service Security Policy. This will provide the ability to securely broadcast all CJI (both restricted and unrestricted information) and all combinations of PII." [Encryption approach]

- "Establish policy to restrict dissemination of specific information that would provide for the protection of restricted CJI database information and combinations of name and other data elements that meet the definition of PII. This will provide for the protection of CJI and PII while allowing for radio traffic with the information necessary to provide public safety."[9] [Hybrid approach]

In response to the DOJ's memo, several law enforcement agencies began to adopt the department's first suggested approach and fully encrypt their radio communications. Most notably, law enforcement agencies in San Jose, San Francisco, Palo Alto, San Diego, Mountain View and Tracy have opted for full encryption over adopting a policy that restricts the dissemination of CJI and PII while allowing some public access to radio channels.[10] Many of these agencies faced criticism from the journalists, the public, and local leaders advocating for greater transparency. In Palo Alto, for instance, the police department issued a memo asserting that because of the dangerous nature of police work, officers' ability to obtain critical information, including PII and CJI, is most safely done via radio communication. The memo went on to conclude that "other means of receiving this information can put the officer and the public at risk," and thus, "there are no other feasible options at this time to implement

---

[8] Generally, PII is information that can be used to distinguish or trace an individual's identity, such as an individual's first name, or first initial, and last name in combination with any one or more specific data elements, including SSN, passport number, driver's license number, or other unique ID numbers issued on a government document.

[9] "Information Bulletin: Confidentiality of Information from the California Law Enforcement Telecommunications System." No. 20-09-CJIS. Issued by California Department of Justice California Justice Information Services Division. 12 October 2020. https://oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/20-09-cjis.pdf

[10] The only agency in San Diego that opted for a hybrid approach was the San Diego Police Department; all other agencies opted for full encryption. "Sheriff's Department encrypts radio communications; critics say the move will reduce transparency." *San Diego Union Tribune.* 16 January 2022. https://www.sandiegouniontribune.com/news/public-safety/story/2022-01-16/sheriffs-department-encrypts-radio-communications

'unencrypted' radio transmissions."[11] As of April 4, 2022, radio communications for roughly 120 law enforcement agencies across California are fully encrypted, allowing no public access.[12]

5. Effect of this Bill

a. Access Requirement

Existing law does not guarantee public access to police radio communications, nor does it prohibit public access to unencrypted police radio channels. Existing law does, however, make it a crime to use any intercepted public safety radio communication to assist in the commission of a crime or evade capture by law enforcement.[13] This bill would require each law enforcement agency in California, by January 1, 2023, to ensure that all radio communications are accessible to the public, with the exception of encrypted radio channels used exclusively for the dissemination of confidential information or for communications that would jeopardize public safety or officer safety if made public (such as tactical or undercover operations). This bill allows agencies to comply with this requirement in any manner that provides reasonable public access, including, but not limited to, the use of unencrypted radio channels, online streaming through the agency's website, or providing access to encrypted communications upon request for a reasonable fee.

b. Confidentiality Requirement

Notwithstanding the access requirement outlined above, this bill requires each California law enforcement agency to prevent or substantially minimize CJI or PII obtained via CLETS from being broadcast in a manner that is accessible to the public. Confidential information that has already been made public or that must be broadcast immediately to ensure officer or public safety is exempt from this requirement. This bill allows agencies to comply with this requirement in any manner that safeguards confidential CLETS information, including, but not limited to, the use of an encrypted channel used exclusively for the transmission of confidential information or the communication of confidential information via data terminal, tablet, phone or other similar device.

6. Definitions Related to Confidential Information

Existing law, across numerous California codes, contains several definitions of and provisions related to "personally identifiable information." Additionally, although the term "criminal justice information" is well-defined in the lexicon of public safety and law enforcement agencies, a statutory definition of this term has not been codified in California law. This bill uses several unique terms to describe the type of information intended to be kept confidential, including "confidential information," "confidential CLETS information," "personally identifiable information," and "criminal justice information." It can be inferred from the plain language of the bill that CJI and PII are both intended to be included in the meaning of "confidential information" and "confidential CLETS information," though it is unclear whether there is other

[11] "Report on Radio Encryption." Issued by the Palo Alto Police Department on March 24, 2021. https://www.paloaltoonline.com/news/reports/1648222031.pdf

[12] "Encrypted Agencies." *The Radio Reference Wiki.* Updated 4 April 2022. https://wiki.radioreference.com/index.php/Encrypted_Agencies#California

[13] Penal Code §636.5

information that can or should be covered by these terms. The Author may wish to amend the bill to establish definitions of "criminal justice information" and "personally identifiable information," possibly using definitions established by the FBI's Criminal Justice Information Security Policy, which dictates many of the federal requirements related to CLETS.[14] The Author may also wish to define the terms "confidential information" and "confidential CLETS information" in reference to CJI and PII.

7. Arguments in Support

According to the California Public Defender's Association:

> "We have proudly supported recent efforts by members of the California Legislature to put police policies and procedures online (SB 978 (Bradford), increase transparency of some police disciplinary records (SB 1421 (Skinner) and SB 16 (Skinner)) and to create a commission to investigate and decertify police officers (SB 2 (Bradford). Yet despite these efforts to move toward more openness, some police agencies have continued to try to shield information from the public eye. For 80 years, news outlets, journalists and the public have had access to police radio communications. This access is critically important for police transparency, accountability, and reporting activity to the public. However, in October 2020, the California Department of Justice's California Law Enforcement Telecommunications System (CLETS) issued a memo regarding the requirement for police agencies to protect identifying information via encryption." […]
>
> "We agree that now is not the time to reduce public access to police activity. Access to critical information regarding police activity is not an "operational change" that should be taken without input from the public, the media, or city, county and state elected officials. Nuanced approaches like the one CHP has chosen to take strike a better balance between openness and protecting private information and should be adopted by other police agencies rather than wholesale encryption. SB 1000 is a much-needed correction to the actions of certain local law enforcement agencies seeking to completely shield important information from the public view. It is also a preventative measure to keep this problem from becoming a statewide issue."

According to the City of Palo Alto:

> "The Palo Alto City Council recently had an extensive discussion about radio encryption and favored the sorts of options in SB 1000 which increase visibility for the public and the media into police calls for service. On an interim basis, Palo Alto has created an interactive map (https://opengis.cityofpaloalto.org/betaPoliceCFSmap/index.html) to display calls for service and the City Council recently directed work to enhance its functionality. While this approach provides some benefit to the press and public, it is only an effort to mitigate the loss of transparency resulting from complying with the DOJ directive. Your bill would significantly advance these efforts."

[14] "Criminal Justice Information (CJIS) Security Policy." Version 5.9, 1 June 2020. Prepared by CJIS Information Security Officer and approved by CJIS Advisory Policy Board. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

8. Argument in Opposition

According to the California State Sheriff's Association:

> "To comply with state and federal requirements, some law enforcement agencies have encrypted their radio communications. SB 1000's general default to unencrypted radio communications would represent a significant burden to agencies that went to tremendous expense to obtain new technology or have previously encrypted their communications. Additionally, to switch back to mainly unencrypted radio communications will require costly and time-consuming training in order to protect CJI and PII.
>
> Also, the bill's contemplation of using alternate, non-broadcasting radio technology to protect information may not be easy or achievable in some geographic locations due to unavailable cell service or computers that cannot connect. Switching to encrypted or alternate media in tactical or undercover situations will likely complicate already complex scenarios."

-- END –