
SENATE COMMITTEE ON PUBLIC SAFETY

Senator Aisha Wahab, Chair

2023 - 2024 Regular

Bill No: AB 1034 **Hearing Date:** June 20, 2023
Author: Wilson
Version: May 1, 2023
Urgency: No **Fiscal:** No
Consultant: AB

Subject: *Law enforcement: facial recognition and other biometric surveillance*

HISTORY

Source: ACLU California Action

Prior Legislation: SB 1038 (Bradford, 2022), died on Senate Inactive File
AB 1281 (Chau, Ch. 268, Stats. of 2020)
AB 2261 (Chau, 2020), held in Assembly Appropriations Committee
AB 1215 (Ting, Ch. 579, Stats. of 2019)
SB 1186 (Hill, 2018), held in the Assembly Appropriations Committee
SB 21 (Hill, 2017), held in Assembly Appropriations Committee
AB 69 (Rodriguez, Ch. 461, Stats. of 2015)

Support: Access Reproductive Justice; Asian Americans Advancing Justice – Asian Law Caucus; Asian Law Alliance; California Association of Black Lawyers; California Attorneys for Criminal Justice; California Immigrant Policy Center; California Latinas for Reproductive Justice; California Public Defenders Association; California-Hawaii State Conference of the NAACP; Cancel the Contract; Citizens for Choice; Clergy and Laity United for Economic Justice; Communities United for Restorative Youth Justice; Council on American Islamic Relations, California; Courage Campaign; Democrats of Rossmoor; Electronic Frontier Foundation; Ella Baker Center for Human Rights; If/when/how: Lawyering for Reproductive Justice; Initiate Justice; Lawyers Committee for Civil Rights of The San Francisco Bay Area; MPower Change; Media Alliance; Muslim Democrats and Friends; National Action Network Orange County; National Lawyers Guild San Francisco Bay Area Chapter; Oakland Privacy; Orange County Rapid Response Network; Partnership for the Advancement of New Americans; People's Budget Orange County; Policing Project At Nyu Law School; Policylink; Positive Women's Health Network- USA; Resilience Orange County; San Francisco Public Defender - Racial Justice Committee; San Francisco Public Defender's Office; San Jose Nikkei Resisters; Secure Justice; St. James Infirmary; Starting Over INC.; Stop the Musick Coalition; Support Life Foundation; Tenth Amendment Center; Training in Early Abortion for Comprehensive Healthcare (TEACH); Transforming Justice Orange County; Transgender, Gendervariant, Intersex Justice Project; Urge: Unite for Reproductive & Gender Equity

Opposition: Arcadia Police Officers Association; Burbank Police Officers Association; California Association of Highway Patrolmen; California Reserve Peace Officers Association; California State Sheriffs' Association; City of Chino; Claremont

Peace Officers Association; Corona Police Officers Association; Culver City Police Officers Association; Deputy Sheriffs Association of Monterey County; Fullerton Police Officers Association; Los Angeles County Division of the League of California Cities; Los Angeles County Professional Peace Officers Association; Los Angeles County Sheriff's Department; Murrieta Police Officers Association; Newport Beach Police Association; Novato Police Officer Association; Palos Verdes Police Officers Association; Peace Officers Research Association of California; Placer County Deputy Sheriffs Association; Pomona Police Officers Association; Riverside Police Officers Association; Riverside Sheriffs Association; Santa Ana Police Officers Association; Security Industry Association; Upland Police Officers Association

Assembly Floor Vote:

41 - 17

PURPOSE

The purpose of this bill is to prohibit, until January 1, 2027, a law enforcement officer or agency from using any biometric surveillance system in connection with a law enforcement agency's body-worn camera or data collected from an officer camera.

Existing law, pursuant to the California Constitution, provides that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

Existing law provides that no person in the State of California shall, on the basis of sex, race, color, religion, ancestry, national origin, ethnic group identification, age, mental disability, physical disability, medical condition, genetic information, marital status, or sexual orientation, be unlawfully denied full and equal access to the benefits of, or be unlawfully subjected to discrimination under, any program or activity that is conducted, operated, or administered by the state or by any state agency, is funded directly by the state, or receives any financial assistance from the state. (Gov. Code §§ 11135 et. seq.)

Existing law declares that it is the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storing data recorded by a body-worn camera worn by a peace officer; these policies and procedures shall be based on best practices. (Pen. Code, § 832.18, subd. (a).)

Existing law encourages agencies to consider best practices in establishing when data should be downloaded to ensure the data is entered into the system in a timely manner, the cameras are properly maintained and ready for the next use, and for purposes of tagging and categorizing the data. (Pen. Code, § 832.18, subd. (b).)

Existing law encourages agencies to consider best practices in establishing specific measures to prevent data tampering, deleting, and copying, including prohibiting the unauthorized use, duplication, or distribution of body-worn camera data. (Pen. Code, § 832.18, subd. (b)(3).)

Existing law encourages agencies to consider best practices in establishing the length of time that recorded data is to be stored. States that nonevidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of 60 days, after which it may be erased, destroyed, or recycled. Provides that an agency may keep data for more than 60 days to

have it available in case of a civilian complaint and to preserve transparency. (Pen. Code, § 832.18, subd. (b)(5)(A).)

Existing law provides that evidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of two years under any of the following circumstances:

- The recording is of an incident involving the use of force by a peace officer or an officer-involved shooting;
- The recording is of an incident that leads to the detention or arrest of an individual; or,
- The recording is relevant to a formal or informal complaint against a law enforcement officer or a law enforcement agency. (Pen. Code, § 832.18, subd. (b)(5)(B).)

Existing law provides that the recording should be retained for additional time as required by law for other evidence that may be relevant to a criminal prosecution. (Pen. Code, § 832.18, subd. (b)(5)(C).)

Existing law instructs law enforcement agencies to work with legal counsel to determine a retention schedule to ensure that storage policies and practices are in compliance with all relevant laws and adequately preserve evidentiary chains of custody. (Pen. Code, § 832.18, subd. (b)(5)(D).)

Existing law encourages agencies to adopt a policy that records or logs of access and deletion of data from body-worn cameras should be retained permanently. (Pen. Code, § 832.18, subd. (b)(5)(E).)

Existing law encourages agencies to include in a policy information about where the body-worn camera data will be stored, including, for example, an in-house server that is managed internally, or an online cloud database which is managed by a third-party vendor. (Pen. Code, § 832.18, subd. (b)(6).)

Existing law instructs a law enforcement agency using a third-party vendor to manage the data storage system, to consider the following factors to protect the security and integrity of the data: Using an experienced and reputable third-party vendor; entering into contracts that govern the vendor relationship and protect the agency's data; using a system that has a built-in audit trail to prevent data tampering and unauthorized access; using a system that has a reliable method for automatically backing up data for storage; consulting with internal legal counsel to ensure the method of data storage meets legal requirements for chain-of-custody concerns; and using a system that includes technical assistance capabilities. (Pen. Code, § 832.18, subd. (b)(7).)

Existing law encourages agencies to include in a policy a requirement that all recorded data from body-worn cameras are property of their respective law enforcement agency and shall not be accessed or released for any unauthorized purpose. Encourages a policy that explicitly prohibits agency personnel from accessing recorded data for personal use and from uploading recorded data onto public and social media Internet websites, and include sanctions for violations of this prohibition. (Pen. Code, § 832.18, subd. (b)(8).)

Existing law requires that a public agency that operates or intends to operate an Automatic License Plate Recognition (ALPR) system to provide an opportunity for public comment at a public meeting of the agency's governing body before implementing the program. (Civil Code, § 1798.90.55, subd. (a).)

Existing law prohibits a public agency from selling, sharing, or transferring ALPR information, except to another public agency, and only as otherwise permitted by law. (Civil Code, § 1798.90.55, subd. (b).)

Existing law prohibits a local agency from acquiring cellular communications interception technology unless approved by its legislative body at a regularly scheduled public meeting, as specified. (Gov. Code, § 53166, subd. (c)(1).)

This bill sets forth several legislative findings and declarations, including the following:

- Police body cameras were intended to guard against police misconduct, not to be exploited for surveillance of Californians. Face surveillance would break this promise, transforming a tool for police accountability into a powerful surveillance system that will harm Californians and undermine civil rights.
- These are the exact type of dangerous interactions that would increase if police use of facial recognition were to expand. Body cameras produce low-quality footage that is blurry, skewed, and in near-constant motion. To date, at least four Black men have been wrongly arrested and accused of crimes because of facial recognition errors and misuse.
- The widespread use of facial recognition on police body cameras would be the equivalent of requiring every Californian to show their photo ID card to every police officer they pass. This new mass surveillance system would suppress civic engagement and inspire fear. People who are afraid of having their identities and locations recorded and potentially shared with out-of-state agencies will be discouraged from seeking reproductive health care, attending protests, or reporting public safety issues.
- While this violates everyone's rights, the danger is greatest for immigrants, over-policed Black and Brown communities, LGBTQIA people, and those coming to California for health care criminalized in their home states. Today there is strong and growing public consensus that face surveillance is simply too dangerous and corrosive to our rights to be used by law enforcement.
- Prominent technology companies like Microsoft, Amazon, and IBM, have forbidden sales of their face surveillance systems to law enforcement. Axon, the most prominent body camera maker, also rejected the use of facial recognition for body cameras, citing the potential inaccuracy and abuse.
- From January 1, 2020, to January 1, 2023, Section 832.19 of the Penal Code effectively protected privacy and freedom of speech and movement while preventing misidentification. Section 832.19 of the Penal Code was repealed pursuant to a sunset clause on January 1, 2023.

- While in effect, Section 832.19 of the Penal Code protected Californians from dangerous police surveillance. It prevented the face surveillance of thousands of protesters advocating for police reform and racial justice. And it ended dangerous and ineffective mobile facial recognition programs, including a San Diego-area facial recognition program that failed to produce a single arrest or prosecution in a seven-year period.
- These civil rights protections remain crucial for Californians. Just like when Section 832.19 of the Penal Code was enacted, the only appropriate standard for facial recognition on body cameras continues to be a prohibition on its use.

This bill establishes the following definitions for terms used therein:

- “Biometric data” means a physiological, biological, or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity.
- “Biometric surveillance system” means any computer software or application that performs facial recognition or other biometric surveillance.
- “Facial recognition or other biometric surveillance” means either of the following, alone or in combination:
 - An automated or semiautomated process that captures or analyzes biometric data of an individual to identify or assist in identifying an individual.
 - An automated or semiautomated process that generates, or assists in generating, surveillance information about an individual based on biometric data.
- “Facial recognition or other biometric surveillance” does not include the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information.
- “Law enforcement agency” means any police department, sheriff’s department, district attorney, county probation department, transit agency police department, school district police department, highway patrol, the police department of any campus of the University of California, the California State University, or a community college, the Department of the California Highway Patrol, and the Department of Justice.
- “Law enforcement officer” means an officer, deputy, employee, or agent of a law enforcement agency.
- “Officer camera” means a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a law enforcement officer.
- “Surveillance information” means either of the following, alone or in combination:

- Any information about a known or unknown individual, including, but not limited to, a person's name, date of birth, gender, or criminal background.
- Any information derived from biometric data, including, but not limited to, assessments about an individual's sentiment, state of mind, or level of dangerousness.
- "Use" means either of the following, alone or in combination:
 - The direct use of a biometric surveillance system by a law enforcement agency or officer.
 - A request, agreement, or practice by a law enforcement agency or officer that another law enforcement agency or other third party use a biometric surveillance system on behalf of the requesting officer or agency.

This bill provides that a law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera.

This bill provides that in addition to any other sanctions, penalties, or remedies provided by law, a person may bring an action for equitable or declaratory relief against a law enforcement officer or agency that violates the bill's provisions.

This bill specifies that its provisions do not preclude a law enforcement agency or law enforcement officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information.

This bill includes a sunset date of January 1, 2027.

COMMENTS

1. Need for This Bill

According to the Author:

For three years, a now-expired law prohibiting body camera face surveillance successfully helped prevent the misidentification and wrongful imprisonment of Californians, safeguarded our freedom of speech, impeded creation of dangerous biometric databases, and protected our privacy. AB 1034 would restore those protections under California law by prohibiting a law enforcement agency or officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer for 3 years.

2. Facial Recognition Technology

Facial recognition technology is capable of identifying an individual by comparing a digital image of the person's face to a database of known faces, typically by measuring distinct facial features and characteristics. Early versions of the technology were pioneered in the 1960s and

1970s, but true facial recognition technology as we understand it today did not come about until the early 1990s. In 1993, the United States military developed the Facial Recognition Technology (FERET) program, which aimed to create a database of faces and recognition algorithms to assist in intelligence gathering, security and law enforcement.¹ Since that time, advances in computer technology and machine learning have led to faster and more accurate recognition software, including real-time face detection in video footage and emotional recognition.

Today, facial recognition technology is used in a variety of applications. It is often a prominent feature in social media platforms, such as Facebook, Snapchat and TikTok. For instance, DeepFace, a “deep learning” facial recognition system created by Facebook, helps the platform identify photos of users so they can review or share the content.² Snapchat employs similar technology to allow users to share content augmented by “filters,” which can add features or alter an image of the user’s face. Facial recognition technology has also seen increasing use as a method of ID verification, such as with Apple’s Face ID and Google’s Android “Ice Cream Sandwich” systems.

As facial recognition technology has become more widespread, so have concerns about its shortcomings and potential for misuse. Many critics highlight that the use of facial recognition systems result in serious privacy violations, and that mechanisms to protect against the unwanted sale or dissemination of personal biometric data are insufficient.³ Others suggest that the technology is still too inaccurate and unreliable to be used in such a broad array of applications. For instance, studies suggest that while facial recognition systems have had increasing success identifying cis-gendered individuals, these systems get it wrong more than one-third of the time if the face belongs to a transgender person.⁴ However, even among cis-gendered individuals, research shows that facial recognition systems can be significantly less accurate when identifying women than when identifying men.⁵ Additionally, a growing body of research demonstrates that facial recognition systems are significantly less accurate in identifying individuals with dark complexions, particularly women.⁶

3. Law Enforcement Uses of Facial Recognition Technology

Despite growing concerns, law enforcement agencies at the federal, state and local level continue to use facial recognition programs. A recent Government Accountability Office report revealed that 20 federal agencies employ such programs, 10 of which intend to expand them over the

¹ “Facial Recognition Technology (FERET).” The National Institute of Standards and Technology, United States Department of Commerce. <https://www.nist.gov/programs-projects/face-recognition-technology-feret>

² Facebook has recently indicated that it would reduce its use of this technology, but its parent company, Meta, may continue to use it in other applications. See “Facebook is backing away from facial recognition. Meta isn’t.” 3 November 2021. <https://www.vox.com/recode/22761598/facebook-facial-recognition-meta>

³ Schwartz, Adam. “Resisting the Menace of Face Recognition.” *Electronic Frontier Foundation*. 26 October 2021. <https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition>

⁴ “Facial Recognition Software Has a Gender Problem.” *National Science Foundation*. 1 November 2019. https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=299486

⁵ Buolamwini, Joy, et al. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.” *PMLR* 81:77-91, 2018. <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

⁶ Najibi, Alex. “Racial Discrimination in Face Recognition Technology.” *Harvard University Graduate School of Arts and Sciences Blog*. 24 October 2020. <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>

coming years.⁷ Another recent study found that one in four law enforcement agencies across the country can access some form face recognition, and that half of American adults – more than 117 million people – are in a law enforcement face recognition network.⁸ Very few of these agencies have a formal facial recognition policy, but one such agency, the New York Police Department, defines the scope of its policy as follows: “Facial recognition technology enhances the ability to investigate criminal activity and increases public safety. The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads through a combination of automated biometric comparisons and human analysis.”⁹

The inaccuracy, biases and potential privacy intrusions inherent in many facial recognition systems used by law enforcement have led to criticism from civil rights advocates, especially in California. In March 2020, the ACLU, on behalf of a group of California residents, filed a class action lawsuit against Clearview AI, claiming that the company illegally collected biometric data from social media and other websites, and applied facial recognition software to the databases for sale to law enforcement and other companies.¹⁰ An investigation by BuzzFeed in 2021 found that 140 state and local law enforcement agencies in California had used or tried Clearview AI’s system.¹¹ The controversy surrounding law enforcement use of facial recognition has led many California cities to ban the technology, including San Francisco, Oakland, Berkeley, Santa Cruz and Alameda.

In September 2021, the Los Angeles Times reported that the Los Angeles Police Department had used facial recognition software nearly 30,000 times since 2009, despite years of “vague and contradictory information” from the department “about how and whether it uses the technology.” According to the Times, “The LAPD has consistently denied having records related to facial recognition, and at times denied using the technology at all.” Responding to the report, the LAPD claimed that the denials were just mistakes, and that it was no secret that the department used such technology. Although the department could not determine how many leads from the system developed into arrests, it asserted that “the technology helped identify suspects in gang crimes where witnesses were too fearful to come forward and in crimes where no witnesses existed.”¹²

Conversely, proponents of facial recognition technology see it as a useful tool in the law enforcement arsenal that has the ability, among other things, to help officials identify criminals. It was reportedly utilized to identify the man charged in the deadly shooting at The Capital

⁷ “Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks.” *United States Government Accountability Office*. 3 June 2021. <https://www.gao.gov/products/gao-21-518>

⁸ Garvie, Clare, et al. “The Perpetual Line-Up: Unregulated Police Face Recognition in America.” *The Georgetown Law Center on Privacy and Technology*. 18 October 2016. <https://www.perpetuallineup.org/>

⁹ “Facial Recognition Technology Patrol Guide.” *City of New York Police Department*. Issued 12 March 2020. <https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf>

¹⁰ “Clearview AI class-action may further test CCPA’s private right of action.” *JD Supra*. 12 March, 2020. <https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/>

¹¹ “Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here.” *Buzzfeed News*. 6 April 2021. <https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table>

¹² “Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show.” *Los Angeles Times*. 21 September 2020. <https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software>

Gazette's newsroom in Annapolis, Maryland in 2018.¹³ Advocates of the technology in the law enforcement context also tout its ability to find missing people, act as a deterrent, and improve security in sensitive places, such as schools, banks and airports. California's Security Industry Association, which has an oppose unless amended position on this bill, writes:

Crimes in progress are periodically recorded on body worn cameras, which could include relevant facial images of victims, suspects, or witnesses. Use of facial recognition software for comparison of such images has already been key to solving specific crimes and has the potential to help solve others. [...] Assertions that images recorded using such systems would *never* be suitable for facial recognition are incorrect. Most body-worn camera systems today record in high definition (HD). The suitability of a particular image for comparison using facial recognition software depends on several factors that vary situationally and is not dependent solely on the type of camera. This includes variant lighting, compression, and importantly, the pixel size of the facial image and certain areas within it.

4. Recent Legislation and Effect of This Bill

In 2019, the Legislature passed Assembly Bill 1215 (Ting), Chapter 579, Statutes of 2019, which banned the use of facial recognition technology and other biometric surveillance systems in connection with cameras worn or carried by law enforcement, including body-worn cameras (BWC), for the purpose of identifying individuals using biometric data. The ban covered both the direct use of biometric surveillance by a law enforcement officer or agency, as well as a request or agreement by an officer or agency that another officer or agency, or a third party, use a biometric surveillance system on behalf of the requesting party. The ban also included narrow exceptions for processes that redact a recording prior to disclosure in order to protect the privacy of a subject, and the use of a mobile fingerprint-scanning device to identify someone without proof of identification during a lawful detention, as long as neither of these functions result in the retention of biometric data or surveillance information. AB 1215 included a sunset date of January 1, 2023.

SB 1038 (Bradford), of the 2021-2022 Legislature, would have extended the ban on biometric surveillance and facial recognition systems in connection with cameras worn or carried by officers indefinitely. However, SB 1038 failed on the Senate Floor, and ultimately died on the Senate inactive file. At the time that SB 1038 passed through this committee, committee staff had not identified nor received any evidence demonstrating that the ban on facial recognition technology used in connection with officer-worn cameras had significantly hampered law enforcement efforts in the two years since it had become operative.

Like AB 1215 and SB 1038, this bill, at its core, involves a question of whether the privacy risks, technical flaws, and racial and gender biases outweigh the purported investigatory benefits of facial recognition technology. According to the Author, "adding face recognition technology to body cameras would transform a tool for accountability into a powerful mass surveillance system that would erode Californians' civil rights and exacerbate racial profiling. [...] There are no acceptable standards under which law enforcement can use face surveillance without worsening racial disparities in policing, repressing freedom of speech, undermining the right to protest, and

¹³ Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, New York Times, July 26, 2018, Available at: <https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?login=facebook>.

violating our privacy. The only responsible standard for face recognition on body cameras and other police equipment is a prohibition.” Accordingly, this bill reinstates the ban on facial recognition technology originally established by AB 1215, and prohibits a law enforcement officer or agency from installing, activating or using a biometric surveillance system solely in connection with a law enforcement agency’s body-worn camera or any other camera. While an earlier version of the bill extended the ban for 10 years, until 2034, recent amendments have shortened that sunset timeline and repeal the ban as of January 1, 2027.

5. Argument in Support

According to the California-Hawaii State Conference of the NAACP:

Biometric surveillance, such as facial recognition, would transform a tool for police accountability into a vehicle for one of the most potent and dangerous surveillance systems ever built. The result would be pervasive monitoring of Californians without their knowledge or consent, registering and reporting who we are and where we go, simply for the "crime" of being in public. Facial Recognition Technology has a history of mistaking innocent people for crimes. Citizens' livelihoods should not be placed in the hands of technology, especially when that technology is in the hands of a system that has historically oppressed Black, Brown, and other communities of color. It should not be deployed because there is so much room for error. The CA/HI NAACP’s principal objective is to ensure the political, educational, social, and economic equality of minority citizens in California and eliminate race prejudice.

By reviving a California civil rights law that prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera for ten years, AB 1034 stands to protect Californians. For these reasons, CA/HI NAACP proudly supports AB 1034 (Wilson).

6. Argument in Opposition

According to the Los Angeles County Division of the League of California Cities:

Facial recognition technology is one of many tools utilized in identifying an individual by comparing a digital image of the person’s face to a database of known faces, typically by measuring distinct facial features and characteristics. This technology does not by itself result in ultimate identification, but it may generate investigative leads necessary for combatting crime within our communities. Technology assists our law enforcement partners in doing their jobs more efficiently and ultimately improves public safety.

Cal Cities supports accountability on the part of law enforcement agencies concerning police technology and policies, as well as related oversight by local governing bodies. However, we do not support policies that restrict law enforcement agencies from utilizing technologies that would otherwise enhance their ability to prevent criminal activity in the communities they serve.