Date of Hearing: May 1, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1160 (Wilson) – As Amended March 24, 2025

PROPOSED AMENDMENTS

SUBJECT: Military equipment

SYNOPSIS

This bill, sponsored by the California Police Chiefs' Association, would establish baseline restrictions for law enforcement agencies in California that are using drones that are manufactured in other countries. The bill is primarily in response to recent concerns raised by both the federal government and several members of the Legislature that the continued use of drones made in China by Da-Jiang Innovations (DJI), the dominant drone manufacturer, represents an unacceptable national security risk.

Last session, two bills (SB 99 (Umberg, 2024) and AB 740 (Gabriel, 2023)) sought to prohibit law enforcement agencies (LEAs) from purchasing and using military-style drones that were primarily manufactured in a country that the federal government considers a country of concern. This bill takes a different approach, however. Rather than prohibit the use of drones made by a company that dominates the U.S. drone market, this bill seeks to protect the data that the devices collect by requiring that LEAs contract with U.S-based companies to store the data.

The proposed Committee amendments, detailed in Comment #6, strengthen the provisions in the bill by requiring that LEAs shift existing data storage contracts to a U.S.-based company and that all future data collected by drones be stored with a U.S. company. In addition, the amendments require that the contract between the LEA and the storage company prohibit the use, sharing, or sale of the data by that company.

Oakland Privacy has a "support if amended" position. The bill is opposed by the Association for Uncrewed Vehicle Systems International(.

This bill was previously heard by the Public Safety Committee, where it passed on an 8-0-1 vote.

THIS BILL:

1) Prohibits a law enforcement agency (LEA) from purchasing an unmanned, remotely piloted, powered aerial or ground vehicle unless:

    a) The vehicle contains an option to turn off any data collection programs that are not necessary for the vehicle to function; or

    b) The LEA uses an American data storage company to house all data collected, including, but not limited to, video and photographic images.

2) Makes this bill effective on January 1, 2027, and specifies that this bill does not restrict a LEA's ability to maintain ownership or possession of a remotely powered vehicle purchased before January 1, 2027.

3) Defines an "American data storage company" to mean a partnership, corporation, limited liability company, or other business entity formed under the laws of, and headquartered in, this state or the laws of any other state of the United States or the District of Columbia, that provides services related to storing digital data, including, but not limited to, through cloud storage, and has adopted security measures to protect stored data from unauthorized access, modification, or destruction, and that has dedicated servers or hard drives located in the U.S.

EXISTING LAW:

1) Defines the following terms:

   a) "Unmanned aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. (Gov. Code § 853.5(a).)

   b) "Unmanned aircraft system" means an unmanned aircraft and associated elements, including but not limited to, communication links and the components that control the uncrewed aircraft, which are required for the pilot in command to operate safely and efficiently in the national airspace system. (Gov. Code § 853.5(b).)

   c) "Military equipment" means, among other things, unmanned, remotely piloted, powered aerial or ground vehicles, or weaponized aircraft, vessels, or vehicles of any kind. (Gov. Code § 7070 (c)(1) & (6).)

   d) "Law enforcement agency (LEA)" means a police department, sheriff's department, district attorney's office, or county probation department. (Gov. Code § 7070 (b)(1)-(4).)

   e) "Governing body" means the elected body that oversees a LEA or, if there is no elected body that directly oversees the law enforcement agency, the appointed body that oversees a LEA. (Gov. Code § 7070 (a).)

2) Requires an LEA to obtain approval of the governing body, by an ordinance adopting a military equipment use policy at a regular meeting of the governing body before, among other things, requesting, acquiring, or seeking funds for military equipment. (Gov. Code § 7071 (a).)

3) Requires an LEA to submit a proposed military equipment use policy to the governing body and make those documents available on the LEA's internet website at least 30 days prior to any public hearing concerning the military equipment at issue. (Gov. Code § 7070 (b).)

4) Provides that the governing body shall only approve a military equipment use policy if it determines all of the following:

   a) The military equipment is necessary because there is no reasonable alternative that can achieve the same objective of officer and civilian safety.

b) The proposed military equipment use policy will safeguard the public's welfare, safety, civil rights, and civil liberties.

c) If purchasing the equipment, the equipment is reasonably cost effective compared to available alternatives that can achieve the same objective of officer and civilian safety.

d) Prior military equipment use complied with the military equipment use policy that was in effect at the time or, if prior uses did not comply with the accompanying military equipment use policy, corrective action has been taken to remedy nonconforming uses and ensure future compliance. (Gov. Code § 7071 (d)(1).)

COMMENTS:

1) **Author's statement**. According to the author:

> Law enforcement agencies large and small have progressed in the last decade to implement varying types of drone programs due to the operational and safety advantages provided by these technologies, which cannot be understated. Law enforcement agencies also already take precautions to ensure that the data they collect remains secure. While the specific protocols vary by agency, they include mitigations such as using drones without internet, downloading third-party software to avoid interacting with the manufacturer's software, and adhering to municipal and state data retention and storage policies as appropriate. Whether used in search and rescue operations, for reconnaissance purposes, or to improve real-time awareness, law enforcement use of drone technology has become ubiquitous throughout California and credited with saving lives.
>
> However, as is the case with all emerging technology, the use of these devices has not come without unique challenges and debates. AB 1160 establishes minimum security requirements for law enforcement agencies to adhere to prior to any future purchase of drone technology. These protections include 1) a requirement that each vehicle contains an option to turn off any data collection programs that are not necessary for the vehicle to function, and 2) that the law enforcement agency uses an American data storage company to house all data collected, including, but not limited to, video and photographic images. By establishing these requirements, California can limit unnecessary data collection, and ensure the data collected by local and state law enforcement is housed domestically, limiting access to all information by foreign entities.

2) **Foreign-made drones.** This bill seeks to address the privacy and security concerns associated with certain non-U.S. drone manufacturing companies, primarily Da-Jiang Innovations (DJI), a private company located in Shenzhen, China. DJI is the world's largest-selling manufacturer of consumer and commercial drones. The company's drones are the tools of choice used by first responders throughout the United State, including those used by many California law enforcement agencies.[1] Along with their headquarters in China, DJI has offices in the United States, Germany, the Netherlands, Japan, South Korea, Beijing, Shanghai, and Hong Kong.[2]

---

[1] Kate Kelly, "A Chinese Firm Is America's Favorite Drone Maker. Except in Washington." *New York Times* (Apr. 25, 2024) https://www.nytimes.com/2024/04/25/us/politics/us-china-drones-dji.html
[2] https://www.dji.com/company

3) **Federal government concerns.** In June 2024, the Chair of the House Select Committee on the Chinese Communist Party, John Moolenaar (R-MI), and Congresswoman Elise Stefanik (R-NY) released a statement of support following the announcement that the Department of Commerce had placed Chinese drone maker, Autel, on its blacklist that prohibits U.S. companies from doing business with them. In the press release, the two Congressmembers urged the passage of a bill that would add DJI to the Federal Communication Commission's list of foreign companies that pose an unacceptable risk to national security.[3]

In addition, in 2023, a bipartisan group of sixteen U.S. Senators sent a letter to The United States Cybersecurity & Infrastructure Security Agency's (CISA) Director regarding DJI drones, which provided:

> We write today regarding the cybersecurity risks posed by the widespread use of drones manufactured by Shenzhen DJI Innovation Technology Co., Ltd. ("DJI") to operators of critical infrastructure and state and local law enforcement in the United States. In short, we believe that given the company's identified connections to the Chinese Communist Party ("CCP"), the use of its drones in such sensitive contexts may present an unacceptable security vulnerability. We ask that the [CISA] evaluate this concern and make the results of its evaluation available to the public through the National Cyber Awareness System.[4]

German researchers in 2022 found 16 security vulnerabilities in four DJI drone models; these included "bugs allow[ing] an attacker to gain extended access rights" and a finding that "transmitted data is not encrypted, and that practically anyone can read the location of the pilot and the drone with relatively simple methods."[5]

There are also conflicting reports on whether DJI drones have been used to turn information over to the Chinese government. According to one 2023 article, "[C]laims [are] thus far unsubstantiated…that the firm's [unmanned aerial vehicle] operating systems allow private, potentially sensitive user data to be transmitted to authorities in China's government for exploitation."[6] That said, the Senate letter quoted above cites a 2017 U.S. Immigration and Customs Enforcement (ICE) report which claims:

> [T]he Chinese government is likely using information acquired from DJI systems as a way to target assets they are planning to purchase. For instance, a large family-owned wine producer in California purchased DJI UAS to survey its vineyards and monitor grape production. Soon afterwards, Chinese companies began purchasing vineyards in the same area. According to the [source of information], it appeared the companies were able to use DJI data to their own benefit and profit.[7]

---

[3] "Moolenaar, Stefanik Statement on Chinese Drone Maker, Autel, Being Blacklisted" (Jun. 21, 2024) https://selectcommitteeontheccp.house.gov/media/press-releases/moolenaar-stefanik-statement-chinese-drone-maker-autel-being-blacklisted

[4] https://www.warner.senate.gov/public/_cache/files/c/8/c8dbcd57-7d3c-4842-85f2-466dc2b70f66/B56DAFD9C216FD3E54239A3E14E281EF.final-2023.03.15-letter-to-cisa-re-dji.pdf

[5] Julia Weiler, *Security vulnerabilities detected in drones made by DJI* (Mar. 2, 2023), https://news.rub.de/english/press-releases/2023-03-02-it-security-security-vulnerabilities-detected-drones-made-dji.

[6] Bruce Crumley, *German research finds security flaws in four leading DJI drones* (Mar. 5, 2023) Drone DJ, https://dronedj.com/2023/03/05/german-research-finds-security-flaws-in-four-leading-dji-drones/

[7] ICE, *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government* (Aug. 9, 2017) https://info.publicintelligence.net/ICE-DJI-China.pdf

The basic problem lies with the People's Republic of China's (PRC) National Intelligence Law of 2017. As summarized by the United States Department of Homeland Security:

> This law forms the baseline of the modern data collection regime, and compels all PRC firms and entities to support, assist, and cooperate with the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC. Article 7 of this law states "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the [National Intelligence] Law, and keep the secrets of the national intelligence work from becoming known to the public." A PRC intelligence agency may request that any PRC firm or entity secretly share access to a U.S. business or individual's data, or otherwise face penalties. In addition, the National Intelligence Law may compel PRC firms to create backdoors and other security vulnerabilities in equipment and software sold abroad so that the PRC government can easily access data not controlled by PRC firms. The law further establishes a system of incentives for compliance and penalties for non-compliance, stating that the PRC "commends and rewards individuals and organizations that have made significant contributions to national intelligence work" and that, "whoever… obstructs the state intelligence work organization and its staff from carrying out intelligence work according to law" shall be dismissed, investigated, and/or detained.[8]

In other words, the Chinese government has the legal ability to demand data from Chinese companies without any of the due process protections required under American law, and to require these companies to build in security vulnerabilities to facilitate data extraction.

CISA has published a series of reports on Chinese cyber-attacks against the United States. Its findings are summarized as follows:

> Malicious cyber activities attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms.[9]

The sources quoted above were published by federal agencies during both the Biden and first Trump Administrations.

In their "support if amended" position letter, Oakland Privacy provides the following list of federal agencies that have found DJI to be a national security risk and have prohibited their use:

- The U.S. Commerce Department blacklisted DJI in 2017.
- The U.S. Department of the Interior grounded its DJI drone fleet in 2019.

---

[8] U.S. Dept. of Homeland Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China* (Dec. 20, 2020) https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

[9] CISA, *China Cyber Threat Overview and Advisories*, https://www.cisa.gov/china.

- The Department of Defense issued a list of approved U.S. and European drone makers, known as the Blue drone list where DJI is notably absent.

- The U.S. General Services Administration announced it would only buy drones from the Blue UAS list for government purposes in 2021.

- The Pentagon stated that DJI drones still constitute a threat to national security and blacklisted the company in 2022.

Despite federal government concerns and attempts at limiting the use of DJI drones over the last seven years, they remain the dominant drone manufacturer, holding 80% of the U.S. market share and 54% of the global market share in 2024.[10]

4) **Related legislation.** Last session, two bills sought to prohibit law enforcement agencies from purchasing and using military-style drones that were primarily manufactured in a country that the federal government considers a country of concern. SB 99 (Umberg, 2024) would have prohibited a local governing body from approving a military equipment use policy if it contained military equipment that federal law or regulation prohibits the United States Armed Forces from purchasing. Similarly, AB 740 (Gabriel, 2023) would have required the Department of Technology to issue regulations meant to ensure the security of data collected, transmitted, and stored by government drones. The regulations, at a minimum, would have banned the use of drones made by certain entities identified by the federal government. These regulations would have applied to both state and local governmental entities. Both bills stalled, however.

5) **What this bill would do.** As an alternative to an outright ban on DJI and other Chinese manufactured drones, this bill takes a more nuanced approach. The bill, with the amendments included in the following section, would work as follows:

1. Require that all uncrewed vehicles purchased by LEAs after January 1, 2027 comply with two requirements:

    - Include an options to turn off any data collection capabilities.

    - Use a U.S.-based company to house all of the data collected by the vehicle.

2. Require that as of January 1, 2026 that all vehicles either purchased in 2026 or already acquired by the LEA either have all of their surveillance data stored in a U.S.-based company, or that the next time the LEA enters into a contract for data storage, it be with a U.S.-based data storage company.

3. Requires that LEA contracts with data storage companies include a clause prohibiting the data storage company from using, selling, renting, trading, or otherwise sharing the data with any other entity. In addition, it must explicitly state that the data remains under the sole ownership and control of the law enforcement agency that collected the data.

---

[10] Barry Elad, *Drones Statistics By Revenue, Market Size, Usage and Manufacturers* (Mar. 10, 2025) https://www.coolest-gadgets.com/drones-statistics/

6) **Amendments.** In order to strengthen the protections in the bill, the author has agreed to the following amendments:

7073.5. (a) ***(1)*** A law enforcement agency shall not purchase an~~unmanned,~~ ***uncrewed,*** remotely piloted, powered aerial or ground vehicle unless ~~one or~~ both of the following conditions are met:

~~(1)~~

(A) The vehicle contains an option to turn off any data collection programs that are not necessary for the vehicle to function.

~~(2)~~

(B) The law enforcement agency uses an American data storage company to house all data collected, including, but not limited to, video and photographic images.

~~(b)~~

(2) The restriction and conditions pursuant to ~~subdivision (a)~~ ***paragraph (1)***shall only apply to an ~~unmanned,~~ ***uncrewed,*** remotely piloted, powered aerial or ground vehicle purchased on or after January 1,~~2027, and shall not restrict a law enforcement agency's ability to maintain ownership or possession of an unmanned, remotely piloted, powered aerial or ground vehicle purchased prior to January 1, 2027.~~ ***2027.***

(b) For uncrewed, remotely piloted, powered aerial or ground vehicles purchased by a law enforcement agency on or after January 1, 2026, and before January 1, 2027, the law enforcement agency shall use an American data storage company to house all data collected, including, but not limited to, video and photographic images.

(c) Law enforcement agencies that maintain ownership or possession of an uncrewed, remotely piloted, powered aerial or ground vehicle prior to January 1, 2026, shall exclusively use an American data storage company to house all data collected, including, but not limited to, video and photographic images after the current contract to house this data expires.

(d) For contracts entered into pursuant to this section, the contract shall prohibit the American data storage company that is under contract to house the data collected by the unmanned vehicles from using, selling, renting, trading, or otherwise sharing the data with any other entity. The data remains under the sole ownership and control of the law enforcement agency that collected the data.

ARGUMENTS IN SUPPORT: The California Police Chiefs' Association, sponsors of the bill, write in support:

AB 1160 addresses security concerns by ensuring the data collected is only what is necessary for the operation of the equipment, and that the limited data collected is housed by an American based data storage company.

Law enforcement agencies large and small have progressed in the last decade to implement varying types of drone programs due to the operational and safety advantages provided by

these technologies, which cannot be overstated. Law enforcement agencies also already take precautions to ensure that the data we collect remains secure. While the specific protocols vary by agency, they include mitigations such as using drones without internet, downloading third-party software to avoid interacting with the manufacturer's software, and adhering to municipal and state data retention and storage policies as appropriate. Law enforcement would not operate drones if they believed there was any risk to our communities.

Oakland Privacy, with a "support if amended" position, requests the following three amendments to the bill:

> We are very pleased that California law enforcement has recognized that national security is part of public safety and that PORAC is putting forth this bill to address the security threat CCP UAS/drones pose to Americans. Furthermore, California law enforcement will be following the lead of other states and agencies across the country to have already discontinued or prohibited the use of CCP drones.
>
> To further strengthen protections we ask the bill be amended in the following fashion:
>
> - **Require that all CCP drones currently in possession by law enforcement agencies be modified within 6-12 months of the enactment of this bill.**
>
> - **State that modifications can only be made to CCP drones currently in possession by law enforcement**
>
> - **When CCP drones currently in possession by law enforcement must be replaced or become obsolete, limit replacements to Blue list approved drones, and prohibit the further purchase of CCP drones.**

ARGUMENTS IN OPPOSITION: In opposition to the bill, Association for Uncrewed Vehicle Systems International (AUVSI), "association represents corporations and leaders from more than 60 countries across industry, government, and academia in the defense, civil and commercial sectors," argues:

> AUVSI's Partnership for Drone Competitiveness is a coalition of U.S. and Allied drone and drone component manufacturers and enterprise users who are committed to strengthening the U.S. drone industry. The Partnership is built on a simple premise: that stronger U.S. leadership in the drone industry is better for everyone. You can read more about the Partnership in AUVSI's Whitepaper published on our website.
>
> We write to express our strong opposition to AB 1160 (Wilson), as amended. We have strong concerns over allowing the use of adversary drones with software mitigations. Specifically, AB 1160 would create new and ongoing loopholes by enabling drones manufactured by Chinese military companies, as designated by the U.S. Department of Defense, to be purchased by California state and local entities. Sending Californian tax dollars to the Chinese military is a position we cannot and will not support. To put it simply, the bill is a wolf in sheep's clothing. By pretending to safeguard, the bill would provide a backdoor for our adversaries. California's law should strive to protect the state's cybersecurity and data. The language in this bill would take California backwards.

The risks of operating foreign drones from adversarial nations and Chinese military companies are not new and are very well understood. In 2017, the U.S. military began removing these systems from their Arsenal. In 2020, Congress codified the ban on Chinese drones for the U.S. military. In 2023, Congress enacted the American Security Drone Act extending the ban to the entire federal government. Congress continued this work in 2024 and enacted language which established a year-long transitional period that will begin prohibiting Chinese military drone manufacturers from selling new products in the United States. The U.S. Congress has not provided a carve out for adversarial systems with American software or those operated in local only mode. Congress knows that such actions would not address the national security concerns.

REGISTERED SUPPORT / OPPOSITION:

Support

California Police Chiefs Association (Sponsor)

Opposition

Association for Uncrewed Vehicle Systems International
California Chapter of Association of Uncrewed Vehicle Systems International (AUVSI)

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200