To: Governor Edmund G. Brown, Jr.

From: Elizabeth E. Joh, Professor of Law, U.C. Davis School of Law
eejoh@ucdavis.edu (530) 752-2756

Margot E. Kaminski, Assistant Professor of Law, Ohio State University Moritz College of Law; Affiliated Fellow, Information Society Project at Yale Law School
kaminski.217@osu.edu (614) 292-2092

Date: July 29, 2014

Re: AB 1327 (Gorell): Law enforcement should be required to obtain a warrant to use drones in California, except under exigent circumstances.

As law enforcement agencies demonstrate interest in employing drones (unmanned aerial vehicles), California has the opportunity to enact meaningful legislation that recognizes the benefits of this technology to law enforcement, while putting in place limitations that protect the civil liberties of Californians.

The requirement in AB 1327 that law enforcement officers obtain a warrant before using a drone reflects the recognition—in Fourth Amendment jurisprudence and its California equivalent—of the heightened threat to civil liberties posed by new surveillance technologies. AB 1327 ensures that law enforcement drone use does not violate Californians' rights to be free from unlawful searches and seizures and to freedom of speech and association. AB 1327 also establishes an easily administrable rule for law enforcement officers and relieves them of the uncertainty—and inevitable costs—of waiting for judicial review of the Fourth and First Amendment implications of drone surveillance.

Who We Are

We are law professors who research and write on surveillance technologies, and have each written about the civil liberties implications of drone use.

Elizabeth E. Joh is a professor of law at U.C. Davis, whose scholarship focuses on criminal procedure and policing, with a special emphasis on DNA collection, undercover policing, and new surveillance technologies. Before joining the Davis faculty in 2003, Professor Joh served as a law clerk to the Honorable Stephen Reinhardt of the Ninth Circuit Court of Appeals. She received both her Ph.D. in Law and Society and J.D. from New York University, and her B.A. from Yale University.

Margot E. Kaminski is an assistant professor of law at Ohio State University. From 2011 to 2014, she served as the executive director of the Information Society Project at Yale Law School, where she remains an affiliated fellow. Professor Kaminski is a graduate of Harvard University and Yale Law School. She clerked for The Honorable Andrew J. Kleinfeld of the Ninth Circuit Court of Appeals, and has been a Radcliffe Research Fellow at Harvard and a

Google Policy Fellow at the Electronic Frontier Foundation. Her research focuses on media freedom, online civil liberties, international intellectual property law, and surveillance.

Warrantless Drone Surveillance May Be Proscribed by the Fourth Amendment

The Supreme Court's Fourth Amendment jurisprudence increasingly suggests that a substantial amount of drone surveillance may be subject to a warrant requirement. If drones are used to spy on people in their homes or other private spaces, to deploy sense-enhancing technologies, or to conduct dragnet surveillance either directly or by aggregating information over time, Supreme Court jurisprudence suggest that courts may require a warrant. AB 1327 would clarify this requirement for law enforcement and proactively protect Californians' constitutional liberties rather than wait for judicial review.

i. Drones Carry New Technologies That May Invade the Privacy of the Home

Although the Supreme Court held in *Dow Chemical v. United States* that the warrantless aerial photography of an industrial plant was not a search prohibited by the Fourth Amendment, the Court was careful to note that "the photographs here are not so revealing of intimate details as to raise constitutional concerns . . . [because] they remain limited to an outline of the facility's buildings and equipment." 476 U.S. 227, 238 (1986). The Court recognized that other forms of aerial surveillance—including surveillance from a satellite or surveillance using an "electronic device to penetrate walls or windows so as to hear and record confidential discussions"—would raise "very different and far more serious questions" and could be "constitutionally proscribed absent a warrant." *Id*. at 239.

The Court later held in *Kyllo v. United States* that warrantless surveillance that could reveal details within a home violated the Fourth Amendment. 533 U.S. 27, 40 (2001). It did not matter that the search was performed by an officer on a public street or that the surveillance could not reveal "conversations or human activities" or "intimate details" of a person's life. *Id*. at 30. The fact that the thermal imaging device at issue in *Kyllo* could collect information about the "interior of the home that could not otherwise have been obtained without physical intrusion" mandated constitutional protection. *Id*. at 34.

Kyllo stands for the broader proposition that courts will step in to preserve privacy against new and more intrusive technology, especially when that technology "is not in general public use." When faced with technologies that substantially expand police power, the Supreme Court has adjusted Fourth Amendment protection to preserve the prior balance engaging in what Orin Kerr calls "equilibrium adjustment." Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011). As Justice Scalia noted in his opinion for the Court in *Kyllo*, courts attempt to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted." Chief Justice Roberts, writing for the majority this year in *Riley v. California*, similarly noted that the new technology that allows for storage of massive amounts of information in cell phones "does not make the information any less worthy of the protection for which the Founders fought." 134 S. Ct. 2473, 2495 (2014).

Drones will take advantage of the many technological advances that will permit cheap, sophisticated, and sometimes surreptitious monitoring that goes far beyond the police powers of the past. Drones are increasingly equipped with cameras that have the capacity to gather more and better information than the unaided human eye through the use of high-powered zoom lenses and infrared imaging that can detect heat as well as visible light. *See e.g.*, William Saletan, "Nowhere to Hide," Slate.com, Sept. 17, 2008;[1] Greg Miller and Julian E. Barnes, "Special drones pursue militias," Los Angeles Times, Sept. 12, 2008.[2] Drones are also often equipped with powerful directional microphones and can even carry devices allowing them to intercept and track cell phone communications. Drones are already small enough and maneuverable enough to peer in the windows of a house, and may one day be small enough to explore hidden spaces and even enter homes without being observed. *See e.g.*, Erica Heartquist, "Drone Accused of Peeping into Woman's Window Was Photographing Aerial Views," USA Today, June 24, 2014; W.J. Hennigan, "It's a bird! It's a spy! It's both," Los Angeles Times, Feb. 17, 2011.[3] These current and future capabilities distinguish today's drones from the planes and helicopters used for surveillance in cases like *Dow Chemical*.

ii. **Drones Can Enable Dragnet Surveillance**

In addition to recognizing Fourth Amendment protections for the home and from invasive new technologies, the Supreme Court has recently noted concerns over low-cost dragnet surveillance—concerns that courts could easily raise with respect to drone surveillance.

The Court has recognized that modern technology and the ability to aggregate data can reveal much more about us, and thus be much more privacy invasive, than ever before. In *United States v. Jones*, the Supreme Court held that using a GPS device to track a car traveling on public streets was unconstitutional absent a warrant. 132 S. Ct. 945 (2012). Five justices on the Court recognized in concurrences that the collection of data on a person's movements over time revealed significant and intimate details about that person's life. *Id*. at 955 (Sotomayor, J., concurring); *id*. at 965 (Alito, J., concurring). The justices also recognized that this kind of surveillance, and the amount of data collection possible with GPS tracking technology, was different in kind from anything the Court had confronted in the past. As in *Kyllo*, the court was forced to address "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 35.

Just this past term, in holding that law enforcement must get a warrant before searching a cell phone, the Court recognized that the quantity and quality of data available on cell phones distinguishes them from other objects a person may have in his pockets. *Riley*, 134 S. Ct. at 2489. This difference poses several interrelated threats to privacy. Cell phones can store so much data for such a long period of time that the exposure of one individual type of data (for example, all the photographs on a phone) could allow law enforcement to reconstruct in aggregate "the sum of an individual's private life." *Id*. Further, the variety of data available on a phone can "reveal much more in combination than any isolated record." *Id*. Finally, cell phones have

[1] http://www.slate.com/articles/health_and_science/human_nature/2008/09/nowhere_to_hide.html.
[2] http://articles.latimes.com/2008/sep/12/world/fg-pakistan12.
[3] http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217.

become so pervasive that allowing their search without a warrant would impact a much wider swath of Americans than in the past. *Id*. at 2490.

Jones and *Riley* are instructive in analyzing the privacy implications of warrantless unmanned aerial surveillance. For years, law enforcement took the position that GPS tracking devices could be installed on a suspect's vehicle without a warrant because the device would merely track the suspect moving about on public streets. Similarly, law enforcement regularly searched cell phones without a warrant incident to arrest. Privacy advocates argued that a warrant was required in both contexts, and it took years for the Supreme Court to settle the debate, which it finally did, unanimously, in 2012 and 2014, on the side of privacy advocates. But in the intervening period, untold numbers of individuals were investigated without the judicial protections of a warrant.

Drones allow for surveillance as pervasive and continuous as the GPS tracking at issue in *Jones*, and could obtain data just as sensitive as that available on the "flip" phones protected in *Riley*. To avoid similar privacy invasions from drone use while constitutional law undergoes the often slow process of adapting to technological change, and to avoid the risk that courts will exclude drone-based evidence in a criminal trial under the Fourth Amendment, the state should require a warrant for criminal investigative use of a drone.

iii. Drones Diminish Practical Constraints on Surveillance

Drones also circumvent the practical constraints on surveillance that the Court has recognized as important to Fourth Amendment analysis. Like GPS monitoring, drone surveillance will soon become "cheap in comparison to conventional surveillance techniques." *Jones*, 132 S. Ct. at 956 (Sotomayor, J. concurring). By design, it will also "proceed[] surreptitiously [and will evade] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" *Id*. (citing *Illinois v*. *Lidster*, 540 U.S. 419, 426 (2004)). Commenters have interpreted the *Jones* concurrences to suggest that "a new surveillance technique is likely to violate an expectation of privacy when it . . . disrupts the equilibrium of power between police and suspects by making it much less expensive for the government to collect information." Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v*. *Jones*, 123 Yale L. J. Forum 335, 337 (2014). Similarly, the low cost and flexibility of drones erode the natural limit on aerial surveillance imposed by the costs and limitations on human pilots of traditional aircraft, and thus invite constitutional scrutiny.

Even if the Government can obtain some of the same data with a manned aircraft as with a drone, that does not render warrantless drone surveillance constitutional. Drone surveillance can enable permit sophisticated, comprehensive, and surreptitious data collection on a vastly greater scale than traditional surveillance techniques would permit. That *some* of this data could be obtained by "conventional surveillance techniques" like a manned aircraft does not end the Fourth Amendment analysis. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing *Kyllo*, 533 U.S., at 35, n.2).

The California Constitution Provides Even Greater Privacy Protections

Article I, Section 13 of the California Constitution offers even greater protection against unlawful searches and seizures than the federal constitution, as state case law on manned aerial surveillance demonstrates. In *People v. Cook*, the California Supreme Court held that warrantless aerial surveillance of a backyard was an unconstitutional search. 41 Cal. 3d 373 (1985). Later, in *People v. Mayoff*, the court explicitly distinguished federal aerial surveillance cases like *Dow Chemical*, and recognized that *Cook* sets forth a different rule than the Supreme Court's Fourth Amendment decisions. 42 Cal. 3d 1302, 1312 (1987). Thus, even for *manned* aerial surveillance, the California Constitution requires a warrant to collect information about a homeowner's backyard.

California's constitution also differs from the federal constitution in that it provides an express right to privacy. *See* Cal. Const. Article I, Section 1. Voters added the Privacy Initiative to the California Constitution in November 1972. As the ballot pamphlet advocating for the initiative stated, this amendment creates "a legal and enforceable right of privacy for every Californian." Ballot Pamp., Gen. Elec. (Nov. 7, 1972) Argument in Favor of Prop. 11, p. 26. It was also intended to "prevent[] government and business interests from collecting and stockpiling unnecessary information . . . and from misusing information gathered for one purpose in order to serve other purposes . . . [because t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives...." *Id*. at 27. Drones, with their low cost and sophisticated data collection devices, have the capacity to collect vast amounts of information about Californians without the operational constraints that limit the potential harms of traditional surveillance. This is precisely the kind of data collection the Privacy Initiative was intended to address.

Drone Surveillance Implicates Freedom of Expression and Association in Public

Surveillance outside the home also implicates First Amendment rights and parallel state constitutional protections for speech and association. In *United States v. Jones*, Justice Sotomayor recognized that "[a]wareness that the Government may be watching chills associational and expressive freedoms." 132 S. Ct. at 956. This is especially true where surveillance can generate "a comprehensive record of a person's public movements" because it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id*. at 955.

Justice Sotomayor was referencing a long line of cases that use the First Amendment to protect not only the right to speech and to protest on public streets, but also the right to do so anonymously. *See e.g., Talley v. California*, 362 U.S. 60 (1960); *Schneider v. State of New Jersey*, 308 U.S. 147, 162 (1939); *McIntyre v. Ohio*, 514 U.S. 334 (1995); *Buckley v. Am. Constitution Law Found*., 525 U.S. 182 (1999); *Watchtower Bible v. Village of Stratton*, 536 U.S. 150, 167 (2002).

Freedom of expression and freedom of association in public places are values on which American society was forged. The United States has a long history of anonymous pamphleteering and advocacy. *See Talley v. California*, 362 U.S. 60, 64 (1960); *McIntyre v.*

Ohio, 514 U.S. 334, 360 (1995). Without privacy, it would be very difficult to speak freely, join and support causes, and assemble to criticize government and safeguard democracy. Anonymity allows individuals to speak without fear of reprisal from the government or private actors. *See e.g., Talley v. California*, 362 U.S. 60 (1960) (striking down a ban on anonymous handbills, noting that "(p)ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws . . . anonymously"); *McIntyre* at 357 ("[a]nonymity is a shield from the tyranny of the majority"). The Supreme Court has found that anonymity fills an important purpose: "to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society." *Id*.

Privacy also protects freedom of association. "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449, 465 (1958). Scholars have warned against the First Amendment harms of relational surveillance, especially those posed by newer data mining technologies. *See e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 Boston College L. Rev. 741 (2008).

First Amendment privacy protections for speech and freedom of association can extend even to those who are acting undisguised and in public. The Supreme Court has recognized a First Amendment right to anonymity even where door-to-door petitioners revealed their faces in a public place. The Court found that the "fact that circulators revealed their physical identities did not foreclose our consideration of the circulators' interest in maintaining their anonymity." *Watchtower Bible v. Village of Stratton*, 536 U.S. 150, 167 (2002). What a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967).

The California Supreme Court has also recognized that excessive government surveillance can have a severe impact on protected expression and associational rights. In *White v. Davis*, the Court recognized that covert surveillance of college classes not only impacted the plaintiffs' right to privacy, it also created a "substantial probability" of chilling the exercise of First Amendment rights. *White v. Davis*, 13 Cal. 3d 757, 761 (1975). This was true even though the police had a "legitimate interest in gathering information to forestall future criminal acts." *Id*. at 766.

The California Attorney General's office has also recognized the impact of excessive government surveillance on privacy and free speech and has stated that *White v. Davis* "is a warning to law enforcement in California that it cannot operate from the premise that it can gather intelligence on citizens' activities regardless of any articulable connection to unlawful action." *Criminal Intelligence Systems: A California Perspective,"* California Department of Justice, Division of Law Enforcement, 16-17 (September 2003).[4]

Absent a warrant requirement, the use of drones for surveillance purposes can threaten freedoms of expression and association. The warrant requirement -- and its command that a search be conducted only with probable cause to believe that evidence of a crime will be found -- prevents

[4] https://www.aclunc.org/sites/default/files/criminal_intelligence_systems_a_california_perspective.pdf.

the use of drones to monitor protests, rallies, and other expressive activities without any suspicion of wrongdoing. The particularity requirement of a warrant, and its associated mandate to minimize data collection and retention not related to the purposes of the warrant, further protect Californians' rights to anonymity and freedom of expression and association. A warrant requirement would thus help law enforcement to protect the public and investigate crime while minimizing the impact of drones on fundamental rights guaranteed by the United States and California constitutions.

Conclusion

Californians' privacy rights do not end at their front doors. Californians are not required to "erect opaque cocoons" just to be able to conduct their affairs in private. *People v*. *Cook*, 41 Cal. 3d 373 (1985); *see also Delaware v*. *Prouse*, 440 U.S. 648, 663 (1979) ("[P]eople are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks.").

Legislatures are well-positioned to fine-tune the law to new technologies. They can provide clarity with respect to complicated and rapidly changing circumstances.

If drones are to be used for criminal law enforcement and intelligence-gathering purposes, there should be strict restrictions on the circumstances under which they may be used. Drones pose privacy and freedom of expression concerns qualitatively different from those raised by traditional forms of aerial surveillance because of their relative inexpensiveness, surreptitiousness, and the invasiveness of the new technology they will likely include. Law enforcement should be required to obtain a warrant based on probable cause to use a drone.