DRONES IN OUR FUTURE: OPPORTUNITY AND PRIVACY CONSIDERATIONS

Friday, August 8, 2014
10:00 a.m. – 1:00 p.m.
UCLA Faculty Center
480 Charles E. Young Drive East
Los Angeles, CA 90024

Background Paper
Prepared by
Thomas Clark, Counsel to the Assembly Judiciary Committee

INTRODUCTION

> *Imagine a helicopter capable of hovering just above an enclosed courtyard or patio without generating any noise, wind, or dust at all -- and, for good measure, without posing any threat of injury. Suppose the police employed this miraculous tool to discover not only what crops people were growing in their greenhouses, but also what books they were reading and who their dinner guests were*.

United States Supreme Court Justice William Brennan wrote the above words in his dissenting opinion in *Florida v. Riley* (1989).[1] In that case, the majority held that police did not need a warrant to fly a helicopter 400 feet over a partially covered backyard greenhouse that, the police rightly suspected, contained marijuana plants. Three years earlier the Supreme Court had similarly upheld warrantless "naked-eye" surveillance from a fixed-wing plane flying at 1,000 feet.[2] In both cases, the Court held that police officers do not need a warrant to see what could be seen by any member of the public from a place where the public (or a police officer) had a right to be. In an age where private and commercial flight in the public airways is routine, the Court reasoned, one does not have a reasonable expectation of privacy in anything that could be seen by the naked eye from a plane or a helicopter. Justice Brennan disagreed. That the police were in a place that they had a right to be was not, for Brennan, the critical issue; rather, the key question was whether the defendant had a reasonable expectation that the contents of the greenhouse were reasonably shielded from public view. Brennan conceded that helicopters had become common. But, Brennan wrote, "imagine" that the police had a helicopter capable of hovering just above a courtyard without noise, and imagine that this "miraculous tool" was capable of reading book titles from shelves or identifying dinner guests.

The "miraculous tool" that Brennan could only "imagine" in 1989 has apparently arrived in the form of highly maneuverable, pilotless aerial vehicles. The public and private use of "unmanned aerial vehicles" – commonly known as drones – is expected to explode in the next few years, thanks in large part to the Federal Aviation Administration (FAA) Modernization and Reform Act (FMRA) of 2012.[3] FMRA requires the FAA to develop, no later than September 2015, a plan and a set of regulations that will facilitate the integration of Unmanned Aircraft Systems (UAS)[4] into our national airspace, for both private and public uses. A recent federal audit concludes that FAA will probably not meet the 2015 deadline, despite the FMRA mandate and increasing pressure from the UAS industry to expedite the process.[5] With or without final FAA rules, some companies are already using drones for commercial purposes. Although the FAA considers such commercial uses illegal, a recent ruling by an administrative law judge on behalf of the National Transportation and Safety Board (NTSB) calls into

question FAA authority to regulate commercial drones, at least until the Congressionally-mandated rules are finally promulgated.[6] The NTSB administrative law judge has stayed his ruling pending the outcome of the FAA appeal; but whatever the outcome of this appeal, one thing seems certain: once FAA rules are completed many more private and public entities will be submitting applications to FAA to operate drones for an array of purposes. FAA estimates that it will issue 7,500 authorized operators within five years of issuing the final rules; others estimate that the number will be as high as 30,000 if not more.[7]

The potential benefits of drones are undeniable, as many of the witnesses in this legislative hearing will no doubt persuasively testify. In addition to the many potential commercial uses – product delivery, crop dusting, film-making, aerial photography, pipeline and oil platform inspection, to name just a few – drones can also serve as a highly useful and cost-effective law enforcement surveillance tool. Other important public functions include fire detection and firefighting, search-and-rescue missions, ecological monitoring, traffic control, and weather forecasting. Inevitably, creative minds will devise many more uses. But along with these benefits, the very pervasiveness of drones – especially when equipped with high-resolution cameras or other sensory devices – will inevitably create new threats to privacy and other constitutional rights and liberties. As is often the case, new technologies create new forms of human interaction, new kinds of conflict, and, invariably, new and complex legal questions.

The purpose of this background paper, and the hearing for which it is written, is to briefly survey some of the legal and policy implications of expanded drone use in California, in both the public and private sphere. Part One discusses the current (and apparently evolving) status of FAA's authority to regulate UAS and the Congressional mandate that FAA devise regulations with an eye toward integrating drones into our national airspace by September of 2015. Part Two considers the likely use of drones by public agencies – especially law enforcement agencies – and whether the 4th Amendment appears to adequately protect our reasonable expectations of privacy from increasing drone surveillance. Part Three considers the potential impact of commercial drone use on personal privacy, and the extent to which existing state privacy statutes and common law privacy torts appear to offer adequate protection. Part Four turns to possible legislative responses, including an overview of what other states have done in an effort to try to set parameters around both public and private drone use.

PART ONE: FEDERAL LEGISLATION AND REGULATION OF DRONES

FAA Authority over the National Airspace System: The Federal Aviation Administration (FAA) is the principle agency responsible for regulating the National Airspace System (NAS) – a term which includes not only the "airspace" within our national political boundaries, but the entire network of air navigation facilities, airports, aeronautical information providers, and personnel who operate this integrated network to ensure the safety of those in the air and on the ground. In addition to licensing pilots, regulating the commercial airline industry, and overseeing operation of our national Air Traffic Control System, the FAA issues "certificates" that authorize public and private persons to operate specific aircraft within the NAS. Public aircraft operators must obtain a "Certificate of Waiver or Authorization" (COA), while operators of civilian aircraft must obtain an "Airworthiness Certificate" before the aircraft may operate within the NAS. No aircraft, public or civilian, may operate in the NAS without FAA certification or authorization of some sort. It is sometimes falsely assumed that FAA does not regulate small unmanned vehicles – such as remote-control model planes – that fly below 400 feet, but as FAA notes on its website, this is one of many "myths" surrounding FAA jurisdiction.[8] In fact, FAA regulates all airspace "from the ground up." The common assumption that

FAA does not regulate airspace below 400 feet apparently derives from a 1981 FAA advisory circular (AC 91-57) that authorized the use of small remote control aircraft (less than 55 lbs.) for *recreational* purposes without a certificate, so long as the aircraft are operated below 400 and at least five miles from an airport. Thus, small recreational remote control planes may fly below 400 feet without an airworthiness certificate only because the FAA created an exemption to the general rule that requires certification, not because FAA lacks the authority to regulate remote control aircraft below a certain altitude.

FAA Authority over Commercial UAVs: Regardless of size or altitude capacity, the FAA regulates both manned and unmanned aerial vehicles. Certification of "unmanned aerial vehicles" – UAVs or "drones" – is generally treated in the same manner as certification of manned vehicles: public drone operators must obtain a COA from FAA while civilian UAV operators must obtain an "Airworthiness Certificate." Thus far, the FAA has issued several hundred COAs, and as of December, 2013, there were over 500 active COAs. Among COA recipients are a variety of public law enforcement agencies, from the U.S. Customs and Border Patrol to local police departments. Other public recipients include public universities conducting research designed to develop beneficial uses of drones, including agricultural uses, weather forecasting, and ecological monitoring. Thus far, FAA has granted only a handful of civilian "Airworthiness Certificates" on an "experimental" basis, and none for purely commercial purposes. (One certificate was issued to Conoco Phillips for monitoring an Alaska oil pipeline, but on a limited and experimental basis.)[9]

As discussed, a recent decision by an Administrative Law Judge with the National Transportation and Safety Board raises questions about FAA's ability to enforce its ban. That decision, however, has been stayed pending an FAA appeal. In the meantime, as FAA has always maintained, commercial drone use without a certificate is a violation of federal law and FAA regulations. As drone technology developed in the 1990s and early 2000s, and as drones became more affordable, an increasing number of persons purchased drones and began using them for commercial purposes notwithstanding FAA policy; indeed, many even openly advertised these services. FAA lacked the capacity to police such uses in a comprehensive manner, but it did occasionally issue warning letters to the commercial operators that came to its attention. FAA concluded that many of these commercial users operated under the false assumption that AC 91-57 authorized their activity so long as they were using small drones and flying them below 400 feet. In response, in 2007 FAA published a notice in the *Federal Register* "clarifying" that AC 91-57 only applied to *recreational* uses and that operating drones for *commercial* purposes violated FAA rules and regulations, no matter the size of the drone or the altitude flown.[10]

The Federal Aviation Administration Modernization and Reform Act of 2012: FAA's 2007 "clarification" that commercial drone use was unlawful without a FAA "Airworthiness Certificate" – and the fact that FAA only grants these certificates for experimental, non-commercial purposes – did not sit well with the rapidly emerging UAS industry or with Congress. Reflecting growing pressures to integrate more drones into the NAS, Congress recently enacted, and President Obama signed, the FMRA of 2012. FMRA requires the FAA to develop rules and regulations to facilitate the "safe integration" of UAS into the NAS by September of 2015. As part of the general charge, FMRA also sets forth a series of preliminary steps that FAA must complete by specified deadlines.

Although the FAA initially estimated that there could be 30,000 drones by the end of the decade, it recently revised that figure significantly downward, estimating that by 2020 (within five years of the promulgation of rules) there will be just 7,500 commercial drones. Industry and other advocates of

UAS integration continue to favor the 30,000 figure, contending that UAS will eventually become a $90 billion dollar business employing as many as 100,000 people.

Recent Auditor's Report: Whichever estimate is most accurate, both are premised on FAA completing its rules and requirements by the September 2015 deadline and issuing certificates to operators that meet the requirements. However, a recent audit by the Office of the Inspector General concludes that FAA "faces significant barriers" to integrating UAS into the NAS by the September, 2015, deadline.[11] Most of the impediments to UAS integration, the audit concluded, are technological. Underlying the technological barriers is the simple fact that UAS have no pilots on board. For all of the high-tech safety and collision-avoidance equipment used on modern aircraft – and it is considerable – the final avoidance technique remains the ability of a human pilot to "see and avoid" a potential collision. Experts informed the auditor that this is the most pressing technical challenge, for "there is currently a lack of mature UAS technology capable of automatically detecting other aircraft operating in nearby airspace and successfully maneuvering to avoid them." A second and closely related technological barrier involved so-called "lost link" scenarios, where the radio or electronic software linking aircraft and the ground operator is temporarily disrupted, even if only for a matter of seconds. For example, the report noted a 2010 incident in which the U.S. Navy lost contact with a UAS helicopter due to a software problem, which resulted in the UAS helicopter entering restricted airspace in Washington, D.C. In March 2012, a UAS operating at 20,000 feet lost contact with ground control for several minutes and descended to 19,000 feet without authorization from air traffic control.[12] The Auditor found other barriers that were not strictly technical in nature, including a failure to meet consensus on defining minimum performance and design certification standards or establishing standardized training standards for air traffic controllers to manage UAS. In light of these barriers, the Auditor concluded that FAA will not meet the September, 2015, deadline for developing final rules on UAS integration.[13]

Overall, the Auditor concluded that until FAA "addresses these barriers, UAS integration will continue to move at a slow pace, and safety risks will remain." The Auditor recommended that FAA, in cooperation with stakeholders, establish new milestones and timelines on a number of specific issues, but the Auditor did not specify dates for these milestones, let alone speculate on when, or if, new target dates would be established for either the completion of comprehensive rules or the preliminary rule on "small" UAS.[14]

FAA's Primary Mission: Safety or Privacy? Agency Says Its Safety, Not Privacy: Although the primary purpose of FMRA is to establish rules and regulations that will permit the "safe integration" of an increasing number of UAVs into the NAS, the recently published Roadmap identifies two goals: safety and privacy. However, while identifying privacy as a goal, the Roadmap says very little about privacy. The Inspector General's Audit Report similarly mentions dual goals of safety and privacy, but like the Roadmap, only mentions privacy as one of the obstacles that is preventing FAA from meeting its deadlines. Despite pressure by some members of Congress and privacy advocates, FAA continues to maintain that its chief mission is to ensure safety in national airspace. At a very fundamental level, FAA's responsibility is to ensure that the thousands of new UAVs that will eventually operate in an already-crowded airspace do not crash into each other or, more important, do not collide with manned aircraft carrying human crews and passengers. This is by no means a hypothetical concern, as there have already been reports of near misses between drones and commercial airliners. Even a small drone, which might not do much damage to large commercial airline, can nonetheless be sucked into a jet engine. As more drones enter the airspace, the probability of such problems will only multiply. Not unreasonably, then, it appears that the primary objective of the FAA is to ensure that drones

operate safely once in the crowded airspace, rather than the reasons for drones entering the airspace or the kinds of information they collect while there.

In response to pressure from Congress and privacy advocates, however, FAA required the six test sites authorized by FMRA to adopt and post privacy policies and allow for public input on privacy concerns. Specifically, the final draft of the privacy regulations for the test sites (1) require test site operators to maintain a record of all UAS operating in the test sites; (2) require every UAS operator within the test site to have a written plan for the operator's use and retention of data collected by UAS; (3) require the test site operator to make these privacy plans publicly available; and (4) require the test sites to conduct an annual review of test site operations in order to verify compliance with stated policies and share the outcome of the review in a public forum with an opportunity for public feedback.[15]

Two points should be stressed in regard to the privacy policy for the test sites. First, the policy only calls for transparency on use and retention of data; it does not impose any limits as to how the test site or any UAV operating in the test range may use or retain data. Second, these transparency requirements only apply to the test sites and UAV operating within the test range; they are not intended as general rules that will apply to UAV that will eventually operate in the national airspace once final rules are adopted and certifications granted. Although privacy advocates have asked the FAA to include privacy policies as part of the proposed final rules, the FAA has not yet indicated that it will do so. In its September 2013 *Comprehensive Plan,* the FAA recognizes the importance of privacy issues, but it suggests that *other* federal agencies and stakeholders should address those issues. While stressing that the privacy policies governing the test site are not meant for general applicability, FAA nonetheless claims that "lessons learned and best practices established at the test sites may be applied more generally to protect privacy in UAS operations throughout the NAS. This incremental approach will provide an example to both private and public sectors on a safe and secure way to employ UAS that is consistent with the need for privacy."[16] In short, FAA's primary concern is safety, and while it recognizes significant privacy concerns, it appears to believe that other federal agencies and individual states, through their laws and policies, may be better equipped to address privacy concerns.

While FAA seems reluctant to do so, some members of Congress want FAA to incorporate privacy regulations in its final rules. For example, in opening remarks to hearings on "The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations," Senate Commerce Committee Chairman Jay Rockefeller noted that while safety issues were the FAA's "most important problems," we cannot "ignore the threat that [drones] pose to our personal privacy." Rockefeller noted that consumers are "already under assault" from the multi-billion dollar data broker industry "dedicated to tracking our health status, our shopping habits, and our movements. If the data brokers of today controlled the UASs, I don't know what about American consumers' habits or choices would remain private. People are right to worry that drones in our national airspace could be yet another way for private companies to track where we are and what we are doing."[17] Motivated by similar concerns, U.S. Senator Edward Markey introduced legislation that would amend FMRA so as to prevent FAA from implementing its final rules until certain privacy protections are in place. Specifically, the pending Drone Aircraft and Transparency Act of 2013 (S. 1639, 2013-2015 session) would (1) require every applicant for a UAS certificate to include in its application information on how it intends to collect, use, and retain information; (2) require FAA to make these applications available on its websites; (3) prohibit law enforcement from using UAS for investigation or intelligence purposes without a warrant, subject to certain exceptions; and (4) require any UAS application by law

enforcement to include a "data minimization" statement.[18]

In sum, the FAA is feeling pressures from both sides: on the one hand, the industry wants to accelerate rules; on the other hand, privacy advocates and some members of Congress want FAA to include privacy protection in the final rules. U.S. Senator Markey's bill usefully highlights that privacy concerns apply to both public and private use of drones. The next two parts of this paper turn to each in turn.

PART TWO: PUBLIC AGENCY USE OF DRONES AND THE 4TH AMENDMENT

While commercial drone use is still emerging – and in theory awaiting FAA final rules – the FAA has authorized drone use for various public domestic purposes for more than two decades, and the use of drones have become more common.[19] For example, United States Customs and Border Protection maintain a large fleet of drones that monitor the U.S. border and, at times, fly missions on behalf of other public agencies, federal and local. According to FAA director Michael Huerta, as of January of this year, FAA had authorized 36 law enforcement agencies to operate UAS, while several public universities use UAV to conduct research into weather, agriculture, and industrial uses. These public uses have included firefighting, disaster relief, search and rescue, law enforcement, border security, and military training among others.[20] However, one of the more controversial areas involves the use of drones by law enforcement agencies, which raise substantial Fourth Amendment issues.

The Fourth Amendment to the United States Constitution secures the right of the people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It further provides that warrants shall not be issued except "upon probable cause" and the warrant must particularly describe the person or place to be searched. What this means, as developed by two centuries of case law, is that a search is unconstitutional if it is "unreasonable" and constitutional if it is "reasonable." A search that is conducted pursuant to a properly executed warrant is presumed to be reasonable and therefore constitutional. A warrantless search, on the other hand, is unreasonable unless if fits within the definition of one of several judicial recognized "exigent circumstances." Generally, exigent circumstances allow law enforcement to conduct a search where there is some imminent threat that evidence will be destroyed or harm caused.[21]

Although the U.S. Supreme Court has not directly considered whether drone surveillance would constitute a violation of the Fourth Amendment, the closest analogy, most legal scholars seem to suggest, are the so-called "fly-over" cases involving traditional manned aircraft. In *California v. Ciraolo* (1986), the Supreme Court upheld warrantless "naked-eye" surveillance of a back yard from a fixed-wing plane flying at 1,000 feet. The Court held that police officers do not need a warrant to see what could be seen by any member of the public from a place where the public had a right to be. Private and public planes had become routine, the Court reasoned, and therefore one does not have a reasonable expectation of privacy in anything that could be seen by the naked eye from a plane. Three years later, in *Florida v. Riley* (1989), the majority applied the same reasoning in holding that police did not need a warrant to fly a helicopter 400 feet over a backyard greenhouse.[22] The fact that the helicopter was more intrusive than a fixed-wing plane because it could hover at a lower altitude, did not, the majority concluded, make a *constitutional* difference. A reasonable person understands that, in a world where planes and helicopters are common, a fenced backyard is visible to the public from above.

Most legal analysts cautiously conclude that if the U.S. Supreme Court were to consider a drone surveillance case, the "fly over" cases suggest that it would probably be upheld. To the extent that a drone could capture the same images that could be captured by someone in a plane or helicopter, there is no *constitutional* reason to treat a drone differently simply because it lacks a pilot. Some critics of drone use by law enforcement, including the ACLU, contend that because drones are cheaper than planes and pilots, such surveillance will become more prevalent. This may be true, but given the reasoning of the fly-over cases, it may not matter. The key issue for the Court is whether someone can have a reasonable expectation of privacy in something that can be seen from above, whether by a plane, helicopter, or drone.

Yet, the greater privacy threat posed by the affordability and greater pervasiveness of drones may justify statutes and policies that offer greater protection than that provided by the Fourth Amendment, but it is not clear how it would be relevant in a constitutional analysis. If anything, the relative affordability and corresponding pervasiveness of drones may result in *less* protection under the Fourth Amendment. In *Kyllo v. U.S.*, the court held that warrantless use of thermal imaging to detect drug-related equipment inside of a home was an unreasonable search within the meaning of the Fourth Amendment.[23] However, the Court based its holding in substantial part on the fact that the thermal imagining devices of the sort used were not in common usage; thus people have a reasonable expectation that the inside of the home cannot be "seen" by thermal imaging. The implication of the holding, however, is that if thermal imaging devices were commonly used by private parties, then the Fourth Amendment would provide less protection because ones expectation that their activities would be shielded from thermal imaging would be less "reasonable." As applied to drones, the *Kyllo* reasoning leads to an ironic, and potentially very troubling, conclusion and privacy conundrum: As drones become *more* pervasive, as is expected, the Fourth Amendment could offer *less* protection against them.

While fly-over cases suggest that the Court might uphold law enforcement use of drones for aerial surveillance, a recent decision involving GPS devices suggest that certain kinds of drone surveillance could be deemed unreasonable.[24] In sum, it seems reasonable to conclude that, the current Court at least, would only find that drone surveillance constituted an unreasonable search if (1) it physically invaded the defendant's property or obtained information that otherwise could only have been obtained by a physical invasion; or (2) the drone surveillance was sufficiently constant and of a sufficiently long duration.

PART THREE: PRIVACY IMPLICATIONS OF COMMERCIAL DRONE USE

In theory, as discussed above, commercial drones cannot operate legally in the U.S. until FAA develops its final rules and issues certificates to operators. In fact, drones are already being used for commercial purposes and their services are openly advertised on the Internet and elsewhere. National Public Radio (NPR) recently ran a story about a Los Angeles-based company called "Drone Dudes." On its website – www.dronedudes.com – Drone Dudes describes itself as "a unique collective of filmmakers, designers and flying robots. With our custom fleet of Cinema-Drones, we are able to achieve shots previously deemed impossible. Our systems and workflow have been carefully crafted to meet the demands and aesthetics of the motion picture industry, allowing for what we believe is the best overall aerial experience and tools for capture. With over a decade of combined experience in aerial cinematography and motion picture robotics, the Drone Dudes team is led by some of the highest regarded pilots and aerial cinematographers in the industry." Its list of "projects" includes not only feature films, but, among others, a video advertisement for Nature Valley Breakfast Biscuits that was

apparently filmed with the use of drones. According to the NPR report, Drone Dudes has used drones to make videos for use in advertisements by Kawasaki, Hyundai, and PacSun.[25] Whether Drone Dudes is unaware of the FAA position banning commercial drone use, believes that its use of small drones is not subject to FAA policy, or is simply ignoring FAA policy is not entirely clear. Some advocates of commercial drones point to the ALJ's *Pirker* decision noted above to claim that FAA rules and regulations do not prohibit using small drones for commercial purposes, but they ignore the fact that the decision was stayed pending FAA appeal. A more common tactic is to claim that the drone operator is not charging for the drone flights but for the editing or processing photographic images. In any event, FAA policy has clearly not stopped entrepreneurs from using drones for a variety of commercial purposes.

Claims for the Commercial Value of Drones: According to the Association for Unmanned Vehicle Systems International (AUVSI), "the potential benefits for UAS cannot be underestimated." AUVSI estimates that the industry will "create more than 100,000 jobs and $82 billion in economic impact in the first decade following integration." Yet, AUVSI claims, the FAA has left a regulatory void that has left "American entrepreneurs and others either sitting on the sidelines or operating in the absence of appropriate safety guidelines." AUVSI wants FAA to use its existing authority to issue certifications in advance of the final rules, which would at least allow "a portion of the promising commercial sector to begin operating safely and responsibly."[26]

The promising commercial uses of drones are, according to AUVSI, almost endless. Of particular interest to the California economy, some claim that drones will "revolutionize" the film industry.[27] For example, Aerial Media Pros – a company based in Costa Mesa, California – designs and assembles drones that carry cinema-quality cameras into spaces previously inaccessible to traditional manned aircraft. In addition to having more agility than traditional aircraft, drones are much less expensive and carry no risk to the life of pilot and crew. Notwithstanding the FAA's policy banning commercial use of drones in American airspace, drones made by Aerial Media Pros have been used in the making of motion pictures – including the blockbuster, "The Hobbit" – and popular music videos. Aerial Media Pros reportedly makes nearly two dozen models, ranging in price from less than $1,000 to nearly $30,000. Even the more costly models are a relative bargain given that production companies can pay anywhere from $5,000 to $10,000 per hour to rent manned planes or helicopters. According to the founder and CEO of Aerial Media Pros, there is "no other way to capture some of the shots we get. We're getting footage that blows away everyone else. . . With these copters, a camera can close in 10 feet away from the subject or pull out 400 feet away. It can fly through windows or the door of a house, or fly across the water. . . The possibilities really get the creative juices going."[28]

While aerial cinematography may turn on the creative juices of filmmakers and music video producers, more staid professions are also enthusiastic. For example, drone-based aerial photography is already being used in the real estate industry. As reported by the *San Francisco Chronicle* earlier this year, "aerial photos and videos are popping up in ads for moderately priced places, thanks to the relatively inexpensive use of drones."[29] Realtors find that aerial photography and videos can be attractive selling points. As to the FAA regulations that would appear to prohibit these uses, one drone videographer told the *Chronicle* that many drone photographers try to circumvent FAA restrictions "by not charging for the flight but charging for the editing." When asked to comment on this, Les Dorr, an FAA spokesperson, rejected that line of reasoning, asserting that if "the unmanned aircraft is being used as a part of a business . . . it cannot qualify as a hobby or recreation." Dorr claimed that when FAA learns of violations, it sends warning letters or, if those do not work, cease-and-desist orders. Dorr claimed

that FAA has only issued two fines, including one levied in the *Pirker* case, and both of those involved flying in a careless and reckless manner.

Real estate and film-making do not exhaust the possibilities. According to Gavin Schrock, associate editor with *Professional Surveyor* magazine, drones will be especially useful for mapping and surveying. According to Schrock, drones can reach locations that are difficult or even dangerous to access, citing open-pit mines as just one example. Oil companies believe that drones will be extremely useful for the monitoring of pipelines and mines. Jeff Bezos of Amazon famously claimed that his company will someday deliver packages by drone instead of by mail. A San Jose drone videographer hopes to someday offer his services to building inspectors looking for easier access to roofs. According to a report in the *San Jose Mercury News*, "big-data companies see tremendous potential in unmanned and even automatically programmed aircraft for gathering information from the air, whether its counting plants in an Iowa cornfield or using sensors to detect pipeline gas leaks." A Sunnyvale, California, mechanical engineer told the *Mercury News* that this "market is going to be huge. The possibilities are endless; I know so many people getting into this field now so that they can pounce once the FAA comes up with its rules."

Privacy Implications of Commercial UAS: The very characteristics that make drones so promising for commercial purposes – especially their maneuverability and capacity to carry various kinds of recording or sensory devices – are the same characteristics that make them a potential threat to privacy. While Justice Brennan's image (quoted at the beginning of this paper) of a hovering device that could peer into windows and read book titles assumed a device operated by government, a privately operated device could do the same thing. While the private operator could not arrest or incarcerate a person based on what was discovered, it would create an equally intrusive invasion of privacy. Private operators could, conceivably, use a small bird-sized drone equipped with a high resolution camera to obtain private and even intimate images of unsuspecting subjects. Even more mundane pieces of personal information – the presence of absence of certain products, the time of day that one exits or enters one home, the route one takes to work, etc. – could be collected by a drone and, in our digitally connected world, linked to the array of personal information that is collected by data brokers, retailers, and others from a variety of other sources. Indeed, it is not inconceivable that data brokers themselves could use information collected by a drone to supplement their existing consumer profiles. Of course, one should not overstate the threat posed by drones. For example, powerful cameras and sensory devices on conventional aircraft or mounted on street poles or on the roofs of neighboring buildings could pose the same kinds of privacy threats. However, the maneuverability of drones relative to stationery cameras, and their affordability and small size relative to traditional aircraft, clearly make them potentially more pervasive and intrusive.

While drones will inevitably pose novel privacy threats, it is unclear whether existing privacy protection laws in California will need to change, and new statutory approaches added, in order to protect against such threats, because neither existing privacy statutes nor the common law of privacy torts are technology specific. Under both statute and common law, as well as under state constitutional law, a person commits an invasion of privacy if that person violates another person's "reasonable expectation of privacy." Under California's "constructive invasion of privacy" statute, for example, a person who captures a visual image or sound recording of another person engaged in a "private familial activity," as defined, may be liable for a constructive invasion of privacy provided that certain other conditions are met. Specifically, a plaintiff bringing an action under the statute would need to show that the defendant captured the image in a manner that is highly offensive to a reasonable person and that the image was captured using an enhanced visual or auditory recording device, such that, in the

absence of the device, the image could only have been obtained by a physical trespass. It does not matter whether one takes the photograph from a helicopter, from the rooftop of a nearby building, or by means of a camera attached to a drone – a violation has occurred if all of the elements are met.

Similarly, it may not be necessary to legislatively modify common law privacy torts in order to address the novel threats posed by drones. Consistent with long-standing common law tort principles, California case law – aspects of which have been codified – recognizes and imposes liability for four kinds of invasion of privacy: (1) Intrusion upon the plaintiff's seclusion or into his or her private affairs; (2) Public disclosure of private facts about the individual; (3) Publicity that places the plaintiff in a false light in the public eye; and (4) Misappropriation, for the defendant's advantage, of a person's name or likeness.[30] It is the first of those – intrusion into private affairs – that would appear to be most likely implicated by private drone surveillance; however, information obtained by such an intrusion could be used in a manner that causes a violation of the other three.

In order to prevail on an "intrusion into private affairs" claim in California, the plaintiff must show that (1) he or she had a reasonable expectation of privacy in the place intruded upon; (2) the defendant intentionally intruded upon that place; (3) the intrusion was committed in a manner that would be highly offensive to a reasonable person; (4) the plaintiff was harmed by the intrusion; and (5) the defendant's conduct was a substantial factor in causing the harm. California jury instructions elaborate on these elements and inform jurors that in deciding whether the plaintiff had a "reasonable expectation of privacy" they should consider the extent to which others could see or hear the plaintiff (the more likely others could see or hear, the less likely the defendant committed an intrusion) and the means by which the intrusion occurred. In deciding whether the intrusion was "highly offensive to a reasonable person" jurors are instructed to consider the extent of the intrusion, the motives and goals of the defendant, and the setting in which the intrusion occurred.[31] None of the elements are technology specific and would not appear to preclude a plaintiff from bringing an action or prevailing upon that action if a drone was used to commit the intrusion.

Finally, in addition to statutory and common law protections, the California Constitution expressly guarantees a right of privacy; moreover, it guarantees this right against *both* private and public actors. The California Supreme Court has held that the privacy provision in the California Constitution "creates a legal and enforceable right of privacy for every Californian."[32] Despite this express protection, however, just what is included in the state's constitutional right to privacy has necessarily been developed in a body of case law. These cases tend to be very fact-specific. As a general rule, however, in order to maintain a claim for infringement of one's right of privacy under the California Constitution, the plaintiff must (1) identify a legally protected privacy interest; (2) establish that he or she had a "reasonable expectation of privacy" under the circumstances; and (3) that the defendant's conduct constituted a "serious" invasion of privacy. If a plaintiff establishes all three of these elements, the defendant may still show the invasion of privacy was justified if it furthers a legitimate and competing interest.[33] As with the statutory provisions and common law elements, the elements necessary to make a constitutional claim are not technology-specific.

In short, it does not appear that the privacy threats created by drone use *necessarily* require modification of existing privacy law, as the critical issues most often concern whether the plaintiff has a "reasonable expectation of privacy" and the defendant's conduct was either "highly offensive" or amounted to a "serious" invasion of the constitutionally protected privacy right. However, the statutory, common law, and constitutional causes of action arise only *after* a breach of privacy and some damage has occurred. Thus, nothing would appear to prevent the Legislature from taking

prophylactic steps to limit damages before they occur, such as regulating the conduct of drones, the kinds of personal information that drones can or cannot collect, and the length of time that drone operators may retain any personal information collected. Indeed, as discussed in the next part, other states have already enacted or proposed such limitations.

PART FOUR: LEGISLATIVE RESPONSES IN THE STATES

Thus far, legislation concerning drones has been introduced in at least 43 states, according to the NCSL, and it appears that other states have recognized both the promise and perils of drone use. Some of those states, more taken with the promise, have sought to encourage UAS development. This has generally taken the form of appropriations for research and development or in efforts to obtain one of the six FAA test sites. Others, more taken by the perils, have sought to limit the use of UAS. For the most part, these limitations focus on law enforcement use of drones, most commonly by requiring law enforcement to obtain a warrant before using drones for law enforcement surveillance or in the course of criminal investigations. The relative paucity of legislation restricting drone use by private parties may suggest that these states believe that existing privacy laws and common law torts already provide adequate protection. It may also reflect that fact that, thus far, the FAA has only issued UAS certificates to law enforcement, but has not as yet issued certificates from private commercial uses. Any conclusion as to why other states have enacted or failed to enact legislation on this matter would require an inquiry into legislative histories in 49 other states, which goes beyond the scope of this paper.

CONCLUSION: LOOKING FORWARD

As noted earlier, the purpose of this background paper is not to suggest specific legislative proposals. Rather, it has sought to survey the current state of drone regulation (or lack thereof), anticipate some of the legal and constitutional issues that the expansion of UAS is likely to raise, especially in regards to privacy rights and civil liberties, and to consider what other states have done. However, the above analysis does suggest a number of policy questions that could be addressed legislatively, regardless of if or when the FAA issues it final rules:

- ✓ SHOULD THE LEGISLATURE REQUIRE LAW ENFORCEMENT TO OBTAIN A WARRANT BEFORE USING DRONES FOR PURPOSES OF CRIMINAL INVESTIGATION?

As noted above, both U.S. Senator Markey and several state legislatures have proposed or have already enacted bills to require law enforcement to obtain a warrant before engaging in drone surveillance for criminal investigation purposes. As discussed above, based on the U.S. Supreme Court's "fly-over" cases, it seems likely that the court would uphold drone surveillance without a warrant, unless the surveillance was particularly invasive or of long duration. However, it is important to note that the Fourth Amendment establishes a constitutional minimum. State legislatures are free to offer more protection than the Fourth Amendment requires. Doing so might be wise given that existing case law suggests that the more widespread and common drones become, the less protection afforded by the Fourth Amendment. Thus it may be incumbent upon the California Legislature to provide that protection.

- ✓ SHOULD (OR CAN) THE LEGISLATURE IMPOSE LIMITS ON THE ABILITY OF COMMERCIAL DRONE OPERATORS TO COLLECT, USE, AND RETAIN INFORMATION THAT IT COLLECTS?

Senator Markey's legislation (though GovtTracks.com gives a 1% chance of becoming law) would require a private drone operator to include within its application for certification a privacy policy statement setting forth the kinds of information the drone will collect, how it will be used, and how long it will be retained. The proposed federal legislation would also require FAA to post these policies on its website. Federal preemption principles would certainly prevent California from imposing requirements on the FAA application process. Less clear, however, is the extent to which California could require a company operating within the state to develop and publish privacy policies if that company is operating under FAA authority. On the one hand, a court may well find that FAA rules and regulations occupy the field and any state legislation would be preempted. On the other hand, one could argue that California is free to regulate the information collection practices of a company operating within its jurisdiction as has already been the case, for example, with the state's Shine the Light law.

- ✓ DO THE SAFETY AND ECONOMIC BENEFITS OF PUBLIC AND PRIVATE DRONE USE APPEAR TO OUTWEIGH ANY ADDITIONAL THREATS THAT DRONES WILL POSE TO PRIVACY AND CIVIL LIBERTIES?

In answering this question, it is important not to overstate either the benefits or the threats. On the benefits side: Will aerial videos really sell more houses than old-fashioned photographs and flyers? Will drones really "revolutionize" the film industry, or are they simply the latest step in the evolution of film technology? On the privacy side: To what extent will drones pose greater threats to personal privacy than planes or helicopters or 24-hour surveillance cameras on mounted on buildings, in employee bathrooms, on street lamps, or on telephone poles? Will drones allow data brokers to obtain any more information than they can already obtain from the Internet, smartphones, or mobile applications? To be sure, drones will cause additional threats to personal privacy, but does it make sense to single out drones from among other modern technologies that collect, use, and store our personal information?

- ✓ DO EXISTING PRIVACY PROTECTIONS– CONSTITUTIONAL, STATUTORY, AND COMMON LAW – PROVIDE ADEQUATE PROTECTION AGAINST PRIVACY INTRUSIONS COMMITTED BY DRONES, OR WILL LAWS NEED TO BE MODIFIED OR ADDED TO TAKE ACCOUNT OF ANY UNIQUE FEATURES OF DRONE SURVEILLANCE?

As noted above, California privacy laws already provide civil and criminal remedies where a person unreasonably intrudes upon the privacy of another person. These remedies are not necessarily technology-specific. For example, "peeping Tom" statutes in the Penal Code make it unlawful to spy upon persons in certain intimate places, whether this is done by the naked eye or with the aid of a device, including drones. The critical elements are not the nature of the technology but the nature of the intrusion and the motive of the intruder. Similarly, civil remedies for various privacy torts generally impose liability where the defendant acted in a highly offensive manner and the plaintiff, under the circumstances, had a reasonable expectation of privacy. The technological means may be considered in determining reasonableness or offensiveness, but it is not a core element of the tort. It is nonetheless the case, however, that statutes and common rules developed in another time could not have anticipated new technology, and they may contain words or phrases that, when applied to the new technology creates an unfair burden for the plaintiff in seeking recovery for a real harm. In those instances, it may be necessary to modify old language, to account for a drastically changing new reality without making our laws technology-specific.

[1] *Florida v. Riley* (1989) 488 U.S. 445, 462-463 (Brennan, J., dissenting.)

[2] *California v. Ciraolo* (1986) 476 U.S. 207. Brennan was not the first to imagine such a helicopter. In his 1949 dystopian novel, *1984*, George Orwell wrote: "In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a blue-bottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows." Orwell quoted in Robert Molko, *The Drones are coming! Will the Fourth Amendment Stop Their Threat to Our Privacy?* 78 BROOKLYN L. REV. 1279, fn. 13 (2013). On the prophetic nature of Brennan's comments, see Philip Hiltner, *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implications,* 3 WAKE FOREST J. L. & POL'Y 397 (2013). The similarities in the titles of these two articles is apparently a coincidence.

[3] FAA Modernization and Reform Act of 2012 (Public Law 112-095)

[4] The literature – popular, academic, and governmental – uses the acronyms UAS or UAV, sometimes interchangeably, to describe drones. Technically, however, the UAV (Unmanned Aerial Vehicle) is a component of a UAS (Unmanned Aircraft System). That is, UAV refers to the vehicle (or drone) itself; UAS refers to the vehicle together with all of the other operational equipment used to fly the vehicle remotely, including any control station or data link. The FAA defines UAV as "a device used or intended to be used for flight in the air that has no pilot on board." The FAA expressly excludes from this definition missiles, weapons, or exploding warheads, but includes all classes of airplanes, helicopters, airships, and powerlifted aircraft without a pilot on board. UAV does not include balloons, rockets, tethered aircraft, and un-powered gliders. (USDOT, Federal Aviation Administration, *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap* (2013), p. 8. Hereafter, FAA *Roadmap*.)

[5] Office of the Inspector General. Audit report. *FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System*. Report Number: AV-2014-061, June 26, 204. [Hereafter Audit Report.]

[6] See "Decisional Order," *Huerta v. Pirker*, NTSB, Office of Administrative Law Judges, Docket CP-217, March 6, 2014. A decision issued earlier this year by an Administrative Law Judge (ALJ) for the National Transportation and Safety Board (NTSB) further complicates FAA's struggle to meet the FMRA mandates. On June 17, 2013, the FAA fined Raphael Pirker $10,000, alleging that he recklessly operated his Ritewing Zephyr unmanned model aircraft while taking aerial photographs of the University of Virginia campus. In addition to operating the UAV recklessly – for example, by flying too close to buildings and people on the ground – Pirker had received compensation from a communications company that was apparently producing a promotional video about the University. FAA claimed that this violated FAA regulations prohibiting the use of UAV for commercial purposes without an FAA Airworthiness Certificate. (See "Decisional Order," *Huerta v. Pirker*, NTSB, Office of Administrative Law Judges, Docket CP-217, March 6, 2014.) Pirker contested the fine, claiming that the FAA regulations authorizing the fine did not apply to his "model aircraft." The ALJ agreed, noting that, historically, FAA had never required operators of small model aircraft to acquire an Airworthiness Certificate as is generally required of other "aircraft" under Federal Aviation Regulations. (Specifically, Federal Aviation Regulations (FAR) Part 21, Section 21.171 *et seq.* and FAR Part 47, Section 47.3, requires Airworthiness and Registration Certification for an "aircraft.") The ALJ concluded that the only "reasonable inference" was that FAA meant to distinguish "model aircraft" from the "aircraft" that are subject to FAA regulations. The ALJ claimed that this inference was further supported by AC 91-57, the advisory circular entitled "Model Aircraft Operating Standards" with its stated purpose of "encouraging voluntary compliance with safety standards for model aircraft operators." As for the 2007 "clarification" issued by FAA asserting that AC 91-57 only authorized the use of model aircraft for "recreational" purposes, the ALJ held that this notice – though published in the *Federal Register* – did not constitute an enforceable rule, because any FAA rule must be noticed and subject to a public comment period before it can become binding. (*Huerta v Pirker*.) Apparently, no such comment period was ever provided. FAA appealed the ALJ's ruling, and the ALJ agreed to stay his decision pending outcome of the appeal. In the appeal, FAA contended that the ALJ's reasoning that Pirker's model aircraft was not "aircraft" under FAA regulatory definitions was "both illogical and deeply flawed." FAA contended that "model aircraft" is obviously a subset of the more general category of "aircraft" and thus subject to FAA regulation. As for the ALJ's claim that AC 91-57 exempted model aircraft, the FAA contended – as it had in its 2007 clarifying notice – that the exemption only applied to model aircraft that were used for "recreational" purposes. In short, FAA maintains that it has authority overall all "aircraft" operating in national airspace, including "model aircraft." Any commercial use of a UAV, regardless of size, is prohibited unless the operator obtains proper certification from the FAA – which, of course, Pirker did not possess because FAA does not currently grant UAV certification for commercial purposes. ("Administrator's Appeal Brief," *Huerta v. Pirker,* CP-217, April 7, 2014.) While it is uncertain what will become of the FAA appeal, one could argue that FMRA indicates that Congress assumes that commercial operators cannot operate without FAA certification. The purpose of the legislation, after all, is to require FAA to develop a plan and rules and regulations that will accelerate the integration of commercial UAS into the nation's airspace. The legislation thus presumes that commercial use is not presently permitted without FAA certification. (On the other hand, one could plausibly argue that, whatever Congress' intent or understanding, FMRA

unwittingly supports the ALJ conclusion insofar as it suggests that there are currently no binding rules or regulations for FAA to enforce.)

[7] FAA Fact Sheets.

[8] From FAA Website re "myths:" http://www.faa.gov/news/updates/?newsId=76381

[9] FAA Fact Sheet

[10] Federal Register

[11] Office of the Inspector General, *FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System.* Audit Report Number AV-2014-061, June 26, 2014. [Hereafter, *Audit Report*.]

[12] Audit Report, pp. 5-6.

[13] The Auditor acknowledged that FAA had completed some of the preliminary steps set forth in FMRA. For example, the FAA issued a mandated "UAS Roadmap" in November of 2013. One of the required preliminary steps toward integration, the Roadmap contains general goals, metrics, and target dates. However, the Auditor found that the Roadmap still "lacks the detail or authority of a formal implementation plan."[13] Second, FAA reviewed 25 proposals (from 24 different states) and selected six "test sites" to conduct research and trials that will be used to develop standards for the final rules.[13] In advance of the 2015 deadline for the development of comprehensive rules, the Roadmap claimed that FAA develop an interim rule governing "small" UAS operators, which will allow small UAS (under 55 pounds) in the NAS so long as they remain within line-of-sight of the ground operator and are flown below 400 feet. Presumably, this rule will go beyond AC 91-57 by allowing *commercial* use of small UAVs. This interim rule should satisfy somewhat demands to accelerate integration of commercial drones. However, the FAA informed the Auditor that the small UAV rule would not be completed by the August, 2014, target date, and indeed will most likely not be completed by the end of this year.

[14] The Auditor concluded that until the FAA can establish preliminary standards and develop a plan to work more effectively with other public and private stakeholders, "it will remain unclear when, and if, FAA can meet its goals to safely integrate UAS." Audit Report, p. 16.

[15] Joint Planning and Development Office. *Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward.* September 2013.

[16] JPDO, *Comprehensive Plan, supra note*

[17] Rockefeller Statement

[18] For a summary of this bill see http://thomas.loc.gov/cgi-bin/bdquery/z?d113:s.1639

[19] Statement of Michael Huerta before the Senate Committee on Commerce, Science, and Transportation, January 15, 2014.

[20] Id.

[21] Before a court considers whether or not a search was reasonable, it must first determine if the government action constituted a "search" within the meaning of the Fourth Amendment. Before *U.S. v. Katz* in 1967, a "search" usually required a *physical* invasion into a clearly private, non-public space, especially the home. In *Katz*, however, the police had placed a bugging device on the outside of a telephone booth and recorded the defendant's side of the conversation. With this evidence, the police were able to show that the defendant was engaged in illegal betting. Under the pre-*Katz* reasoning, the courts would not likely have found a search since there was no invasion of Katz's property or even of the telephone booth (i.e. the device was on the outside of the booth) and the telephone booth itself was clearly in a public, not a private, space. Yet in *Katz*, the Court found that the defendant has reasonable expectation that, once inside the booth, no one could hear the content of his conversation. The *Katz* ruling revolutionized Fourth Amendment law by eliminating the need for a physical invasion of a person's property or a private space. Instead, the court concluded in *Katz*, that there is a search wherever the government action intrudes upon a person's "reasonable expectation of privacy." As subsequently interpreted and developed, *Katz* was credited with creating a two-prong test. First, the defendant must have had a "subjective" expectation of privacy, genuinely believing that his or her conduct was shielded from public exposure. The second, or "objective," prong is that the defendant's expectation of privacy must be one that society recognizes as "reasonable." *Katz* is particularly relevant when considering Fourth Amendment issues raised by the use of drones. Camera-equipped drones, for example, do not need to physically invade property or a private space in order to capture images unbeknownst to the subject, and they can surreptitiously conduct detailed surveillance of a private person in public places by secretly following that person. As was the case with the electronic bugging device in *Katz*, new technologies create new ways of invading a person's expectation of privacy, and often in advance of whether society could recognize the expectation as "reasonable" in light of the technological landscape.

[22] *Florida v. Riley* (1989) 488 U.S. 445, 462-463 (Brennan, J., dissenting.)

[23] *Kyllo v. U.S.*

[24] In *Jones v. U.S.*, the Court unanimously held that when police attached a GPS device to a suspected drug dealer's car it was a "search" within the meaning of the 4th amendment and required a warrant (or some exigent circumstance) in order to be reasonable. In *Jones*, the police continuously monitored the whereabouts of the vehicle for about one month. The state, relying on an earlier opinion, argued that because movements of a vehicle are open to public observation, the police did not need a warrant to track its movements in public streets. However, the justices found that the action in *Jones* constituted a

search, though for different reasons. Five of the justices joined Justice Scalia in holding that placing the device on the underside of the car was effectively a trespass and therefore a search. The Court did not need to consider whether the defendant had a reasonable expectation in the movements of the vehicle, because the trespass alone made it a search. Five other justices – with one Justice joining both opinions –held that it was a "search" because the constant, month-long surveillance violated defendant's "reasonable expectation of privacy." One may not have a reasonable expectation of privacy when driving on public streets, the concurring justices held, but one does have a reasonable expectation that one's movements will not be monitored 24 hours per day for 28 days. (Id.) *Jones* is thus significant for any analysis of drones because, under the Scalia analysis, the use of drones would arguably not constitute a search unless it amounted to a physical invasion of privacy or obtained evidence which otherwise could only have been obtained by a physical invasion in the absence of the use of technology. However, the concurring opinion – which also received five votes – suggests that a court could find that the use of a drone would constitute an unreasonable search if it was pervasive and long-term.

[25] NPR. "Are Filmmakers Using Drones Illegally? Looks Like it." Available at http://www.npr.org/blogs/alltechconsidered/2014/05/16/312487924/are-filmmakers-using-drones-illegally-looks-like-it.

[26] AUVSI letter to Huerta and website.

[27] "Revolutionizing the Film Industry with Remote-Controlled Drones," *Entrepreneur* January 27, 2014.

[28] Id.

[29] "Drone Videos Help Home Sales Take Off," *San Francisco Chronicle* May 15, 2004.

[30] 5 Witkin, Summary of Cal. Law (10th ed.) Torts, Section 651.

[31] California Civil Jury Instructions. Section 1800. "Intrusion into Private Affairs." For interpretations of these elements and the tort of intrusion more generally, see also *Shulman v. Group W Productions* (1998) 18 Cal. 4th 200; *Saunders v. American Broadcasting Co.* (1999) 20 Cal. 4th 907; *Hernández v. Hillsides* (2009) 47 Cal. 4th 272, especially pp. 286-287.

[32] (*White v. Davis* (1975) 13 Cal. 3d 757, 775.) The relationship between the common law privacy tort and the constitutionally protected right to privacy is not entirely clear, especially as to whether the constitutional right constitutes an independent, self-executing cause of action could provide sole and direct support for a damages claim. *See Katzberg v. Regents of University of California* (2002) 29 Cal. 4th 303, 313, fn. 13; and *Hernández, supra note 18,* at 286-288.

[33] *Hill v. National Collegiate Athletic Association* (1994) 7 Cal. 4th 1, at 39-40.