1-3-2017

Drones and Privacy in the Golden State

Brandon Gonzalez

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Intellectual Property Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol33/iss2/3

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized editor of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
DRONES AND PRIVACY IN THE GOLDEN STATE

Brandon Gonzalez†

There will be over 7 million drones in the hands of U.S. consumers by the end of 2020. The federal government plans to regulate drone flight exclusively, leaving one critical question unanswered: who will protect people’s privacy from this invasive technology? One story has already surfaced about a Kentucky homeowner taking the law into his own hands after seeing a consumer drone hovering over his property. Believing the aircraft was spying on his 16-year-old daughter while she was sunbathing, he took out his shotgun and blasted the drone out of the sky. In a state like California, which has the highest number of drone incidents reported to the FAA to date, similar privacy disputes will undoubtedly arise. California lawmakers have hurriedly responded to drone-related privacy concerns by amending a civil anti-paparazzi statute that is of little use to the general public, and by attempting to enact several pieces of trespass-related legislation that all failed for being too restrictive on drone flight. This article proposes a new legislative approach to the regulation of drone use in California, arguing the state can achieve its privacy-related objectives by utilizing its penal code, together with local law enforcement, to police unlawful privacy violations committed through the use of a drone.

† B.A., Political Science, University of California San Diego, 2012. J.D., Santa Clara University School of Law, 2016. I would like to thank my family and friends for their love and support throughout law school, especially Andra Gheorghiu. I would also like to thank Professor David Ball of Santa Clara University School of Law for not only giving me his invaluable direction and insight on this article, but also his time and patience throughout.
TABLE OF CONTENTS

_Toc467518798_ INTRODUCTION ................................................................. 290
I. CONSUMER DRONE TECHNOLOGY POSES A NEW THREAT TO PERSONAL PRIVACY IN CALIFORNIA ........................................... 292
   A. Drones Potentially Invade Privacy ............................................. 293
      1. Flight Capabilities .................................................................... 294
      2. Camera Capabilities ................................................................ 296
      3. Possible Drone-Related Privacy Invasions ................................. 297
      4. The Public’s Concerns .............................................................. 298
   B. Consumer Drones Are Coming Sooner Than You Think .............. 299
      1. The Sheer Numbers .................................................................. 299
      2. The Market Growth Rate ......................................................... 301
      3. Affordability .......................................................................... 301
   C. FAA Not Regulating Drone-Related Privacy Issues .................. 302
      1. The FAA Modernization and Reform Act of 2012 ...................... 303
      2. Model Aircraft Remain Fairly Unregulated ............................... 304
      3. States Must Regulate Privacy Issues on Their Own ................. 305
II. CALIFORNIA’S LEGAL LANDSCAPE IS INSUFFICIENT TO MEET THE POTENTIAL THREAT OF CONSUMER DRONE TECHNOLOGY .......... 306
   A. California’s Privacy Framework Does Not Yet Apply to Drone Technology ................................................................. 307
      1. California’s Penal Code ............................................................. 308
      2. California’s Civil Code ................................................................ 309
   B. Invasion of Privacy: The Standalone Statute that Doesn’t Protect the Public at Large ........................................................ 310
      1. California’s Anti-Paparazzi Statute .......................................... 310
      2. Drone-Spurred “Constructive Invasion” Amendment .............. 311
      3. Drone-Spurred “Physical Invasion” Amendment .................... 312
      4. Incompatibility of § 1708.8 with Drone Technology .............. 313
III. CALIFORNIA CANNOT ENACT DRONE LAWS THAT INTERFERE WITH FEDERAL FLIGHT REGULATIONS ........................................ 314
   A. The Drone/Private Property Trespass Law ................................ 315
   B. The Drone/School Trespass Law ............................................... 316
   C. Problems with Restricting Drone Flight at the State Level ........ 316
      1. FAA’s Exclusive Authority for the NAS ................................. 317
      2. Fractionalizing FAA’s control of the NAS ............................. 317
III. ACHIEVING CALIFORNIA’S PRIVACY OBJECTIVES THROUGH THE PENAL CODE ............................................................. 319
   A. A Baseline Level of Protection Against Drone-Related Privacy Invasions ................................................................. 319
      1. Amending the State’s Existing Criminal Laws To Encompass Drones ................................................................. 319
      2. The Role of State & Local Law Enforcement ............................ 320
INTRODUCTION

The number of drones operating in the airspace above the United States is at an all-time high.¹ A “drone,” known by its technical term “unmanned aerial vehicle,” is an aircraft that operates without a human pilot onboard.² Drones were once used solely for military purposes by the United States, but in the last decade, drone technology has found domestic purpose in a variety of civilian and government applications in the states.³ As a result, domestic and foreign technology manufactures are now producing drones on a large scale for the consumer market.⁴ FAA forecasts predict that there will be over seven million more drones in the hands of U.S. consumers by the end of 2020.⁵

The Federal Aviation Administration (FAA) has signaled that it does not intend to regulate issues unrelated to drone flight and safety.⁶ Therefore, issues such as privacy will be left to the states to regulate. As a result, lawmakers in California have scurried to find a legislative solution for the protection of its citizens’ privacy from this potentially invasive technology.⁷ Currently, California’s legal landscape is insufficient to meet the potential threat of drone technology as is pertains to personal privacy because drone technology could not have been anticipated when many of California’s traditional privacy protections came of age in the 1960s and 1970s.⁸ Not surprisingly, the

¹. FED. AVIATION ADMIN., FAA AEROSPACE FORECASTS: FISCAL YEARS 2016-2036 (Mar. 24, 2016) [hereinafter FAA AEROSPACE FORECASTS].
³. In the early 2000s, drones started to become domestically repurposed for non-military uses, such as the U.S Customs and Border Protection Agency patrol of the U.S.-Mexico border, law enforcement surveillance operations, and NASA environmental research programs. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-12-987, UNMANNED AIRCRAFT SYSTEMS: MEASURING PROGRESS AND ADDRESSING POTENTIAL PRIVACY CONCERNS WOULD FACILITATE INTEGRATION INTO THE NATIONAL AIRSPACE SYSTEM 4 (2012).
⁴. Currently, interested purchasers can choose from about 146 different types of small drones being manufactured by about 69 different companies in the U.S. Id. at 11.
⁵. FAA AEROSPACE FORECASTS, supra note 1.
⁸. California began recognizing all of the common law privacy torts after the Privacy was
majority of recent drone-related proposals by the legislature have focused on protecting individual privacy rights.9

“Consumer drones,” the focus of this article, pose a number of difficult challenges to lawmakers. As used here, the term “consumer drones” refer to drones that are purchased and operated by civilians, either for hobby or commercial/business purposes.10 In other words, a “consumer drone” is any drone that is not operated by a government or civil authority.11 This distinction is important because the government is limited in its ability to ability to intrude into a person’s constitutionally protected space, whereas consumer drone operators are not.12 Nonetheless, the right to exclude the government from conducting aerial surveillance is inextricably tied to whether a private citizen would have had the right to make the same observation.13

Consumer drones are generally small, lightweight, and propelled by multi-rotor propellers.14 They are remote-controlled and semiautonomous, meaning that they fly with little operator control.15 Almost all consumer drones are equipped with advanced camera technology that allows the operator to capture high-resolution pictures and video from a bird’s eye view.16 The majority of the recent privacy related proposals by the state’s legislature that pertain to consumer drone technology are too restrictive on lawful consumer drone flight in the national airspace, which is within the exclusive jurisdiction of the United States.17 In other words, California’s proposals have focused on

---

10. The terms “recreational-use drone,” “commercial-use drone,” “civilian drone,” and “model aircraft,” refer to different types of drones, but they all fit within this article’s definition of a “consumer drone,” because each type is operated by a civilian pilot. These terms are used interchangeably throughout this article.
11. Governmental drone use is beyond the scope of this article.
12. Civilian drone operators are not restricted by the Fourth Amendment’s privacy protections, which only apply to government actors. See Katz v. United States, 389 U.S. 347, 353 (1967).
13. In the Fourth Amendment context, a court will look to whether a person had a “reasonable expectation of privacy,” to determine whether the government’s search was unconstitutional. Id. at 360. Likewise, a court in a civil case will use the same test to determine whether a private party invaded another person’s privacy. See Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1072 (Cal. 2009) (to prove an intrusion, a plaintiff must show their expectation of privacy was “objectively reasonable”).
15. Id.
16. Id.
17. See 49 U.S.C. § 40103(a)(1)-(2) (The federal government has exclusive sovereignty of
placing property-based trespass restrictions on drone operators where they should have a lawful right to fly.18

Additionally, the only law on the books in California that currently speaks to drone technology, California’s invasion of privacy statute, does not provide a meaningful amount of privacy protection to the public at large.19 The invasion of privacy statute provides a civil cause of action that has certain characteristics that are generally incompatible with drone technology.20 This article surveys the existing legal framework in California, or lack thereof, as it relates to consumer drone technology. It then proposes a more sensible legislative approach to the regulation of consumer drone use in California, arguing that the state can achieve its privacy related objectives by utilizing its penal code, together with local law enforcement, to police unlawful privacy violations committed through the use of a drone.

I. CONSUMER DRONE TECHNOLOGY POSES A NEW THREAT TO PERSONAL PRIVACY IN CALIFORNIA

On July 26, 2015, William Merideth, a resident of Hillview, Kentucky, saw a drone hovering over his house where his 16-year-old daughter was sunbathing.21 Merideth grabbed his shotgun and blasted the drone out of the sky. As Merideth later explained to reporters:

You know, when you’re in your own property, within a six-foot privacy fence, you have the expectation of privacy. We don’t know if he was looking at the girls. We don’t know if he was looking for something to steal. To me, it was the same as trespassing. I didn’t shoot across the road, I didn’t shoot across my neighbor’s fences, I shot directly into the air.22

Shortly after the incident, Merideth received a visit from four men who claimed to be responsible for the drone, who explained that Merideth owed them $1,800 for the destroyed property.23 Merideth says he stood his ground: “I had my 40mm Glock on me and they started toward me and I told them, if you cross my sidewalk, there’s gonna be another shooting.”24

---

20. Id.
22. Id.
23. Id.
24. Id.
The police eventually arrived, and Merideth was arrested for felony wanton endangerment and criminal mischief. At trial, Merideth denied the charges, asserting he was protecting his family’s privacy rights and preventing a trespass. The judge dismissed the criminal charges against Merideth, concluding that because at least two witnesses could see the drone flying below Merideth’s tree line, it was an invasion of privacy. As the judge proclaimed: “He had a right to shoot at this drone, and I’m gonna dismiss this charge.”

The owner of the drone, David Boggs, recently brought an action for declaratory judgment and damages in the United States District Court for the Northern District of Kentucky. In his complaint, Boggs seeks a finding from that court that he was operating his drone within the navigable airspace of the United States, and not within Meredith’s property, that the operation of his drone in that manner did not violate any reasonable expectation of privacy that Meredith may have had, and that a property owner cannot shoot a gun at a drone operating within the navigable airspace of the United States.

This story is important to the legal issues that will be discussed in this article. If and when this case proceeds to the merits, it will necessarily require the resolution of novel questions of law relating to drones. These issues include the boundaries of airspace surrounding real property, a person’s reasonable expectation of privacy as viewed from the air by a private party, and the right to damage or destroy an aircraft in-flight, all in relation to the exclusive federal regulation and protection of air safety, air navigation, and control over the national airspace. This is just a taste of the complex issues raised by drone technology. However, as far as privacy is concerned, this is just the beginning of what is yet to come.

A. Drones Potentially Invade Privacy

Consumer drones are potentially privacy-invading for four reasons. First, consumer drones operate in the sky and can fly over traditional property boundaries such as fences and walls. Second,
consumer drones come equipped with high-resolution cameras,\textsuperscript{31} which allows a pilot to capture images and video at high altitudes from the drone’s point of view. Third, this flight/camera technology can be easily used to invade another person’s privacy in a number of troubling ways. Lastly, the advancement of consumer drone technology is causing concern among the general public with regards to their privacy.\textsuperscript{32} This is demonstrated by recent polls and news reports, resulting in a pressing need for a legislative response.\textsuperscript{33}

1. Flight Capabilities

The motivating privacy concern with consumer drone technology is that it can be easily used to invade people’s privacy. Consumer drones can be flown over traditional property boundaries with a camera to view people or things that would not ordinarily be visible to the human eye. Consumer drones are small, lightweight, fast, and capable of sustained flight at high altitudes.\textsuperscript{34} They are usually equipped with advanced camera technology that allows the operator on the ground to see from the drones point of view in the sky.\textsuperscript{35} The drone’s onboard camera can record high-resolution pictures and video from a bird’s-eye view.\textsuperscript{36} This combined flight/camera technology presents a new and unique threat to personal privacy because a drone operator can easily capture images of a person under circumstances in which the person has a right to privacy.

Although there are many different definitions of the “right to privacy,” the definition as used in this article is “the right to be let alone.”\textsuperscript{37} This right “is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose.”\textsuperscript{38} When it comes to

\begin{footnotesize}
\begin{itemize}
\item[34.] Popper, supra note 14.
\item[35.] Id.
\item[36.] Id.
\item[37.] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARP. L. REV. 193, 193 (1890) (emphasis added). The origin of the common law right to privacy stems from Warren’s and Brandeis’ article in which they propose that a tort for invasion of privacy should be created.
\item[38.] Hill, 865 P.2d at 642 (argument in favor of Proposition 11, to amend the California Constitution to provide a constitutional right to privacy against both private and governmental actors). Hill quotes the California Ballot Pamphlet, Proposed Statutes, and Amendments to the California Constitution with arguments to voters for the November 7, 1972, General Election. Id.
\end{itemize}
\end{footnotesize}
consumer drones, a person’s right to privacy can be easily violated, and as of now, there are practically no meaningful laws keeping a drone operator from doing so.

To understand how pervasive the technology can be if used improperly, consider a popular consumer drone manufactured by the Chinese technology company DJI. DJI is currently at the forefront of the worldwide consumer drone industry and manufactures both recreational and commercial drones.39 One of the most popular selling drones currently on the consumer drone market is DJI’s “Phantom III Advanced” (Phantom), which currently sells for $720.00.40 Many people do not know just how technologically advanced consumer drones can be. The Phantom is a good indicator of the current state of consumer drone technology.

The Phantom is lightweight and compact, weighing 2.8 pounds and measuring 7.5 x 14 inches.41 It has a maximum flight speed of 35 miles per hour, a maximum flight time of approximately 25 minutes, and can climb to an altitude of 6000 feet above sea level.42 The Phantom utilizes GPS to determine its exact location and relation to the operator, and when unobstructed, the aircraft can fly parallel to the ground 3.1 miles from its operator’s location.43 Additionally, the Phantom’s pilot can control the aircraft with any iOS compatible device such as an iPhone or iPad using the “DJI GO” application, which allows the operator to set a flight path, input certain points of interest, and command the aircraft to follow a moving object at the touch of a finger.44

The Phantom’s onboard camera streams live video to the screen of the operator’s iOS device, allowing the operator to see what the drone’s camera is viewing in real-time, high-definition picture quality, from up to 3.1 miles away.45 You can imagine the shock of seeing a Phantom operating outside of your bedroom window, not knowing why it is there, what it is looking at, or who is operating it. At the very least you might feel annoyed, possibly angered, or even scared. These reactions are understandable, because as of now, there is little you can do to stop something like this from happening to you.

41 Phantom 3 Advanced Specs, supra note 31.
42 Id.
43 Id.
45 Id.
For better or worse, consumer drones are also becoming more autonomous. DJI released the next of its Phantom series in March 2016. The “Phantom IV” adapts to its physical surroundings by detecting and rerouting around any obstacle in its flight path. The Phantom IV’s onboard camera will also distinguish between specific objects in its viewing path, allowing the pilot to select a moving object for the aircraft to track. Once the moving object is selected, the Phantom IV then follows and records it at speeds of up to forty-five miles per hour.

2. Camera Capabilities

Consumer drones are usually equipped with cameras that have high-resolution picture and video capabilities. These capabilities enable an operator to capture high definition footage from hundreds of feet above ground. Modern advances in camera technology, starting with the “GoPro,” have made high definition video cameras incredibly small and lightweight. As a result, a variety of different professional-quality cameras can now be attached to the drone to capture high-resolution images and video during flight. Many consumer drone manufacturers also provide a stabilizer to attach the camera to the aircraft so that the picture will stay steady in turbulent flight conditions.

The camera technology is advancing just as fast as the drone technology itself. Consumer drone manufacturers are now developing and manufacturing their own professional-quality cameras with an array of technological capabilities. Some manufacturers are offering cameras with digital and optical zoom capabilities. This means that certain consumer drones will be able to capture clear images and video from a much farther distance than before.

47. Id.
48. Id.
49. Id.
50. Id.
52. Popper, supra note 14.
55. Id.; see also Zenmuse X5R, DJI STORE (2016), http://bit.do/ZenmuseX5R.
Other consumer drone manufactures are offering cameras with thermal imaging technology.\(^{56}\) With this technology, a consumer drone operator can use the infrared camera to see temperature profile of humans in the dark of night, and in some instances even behind closed doors.\(^{57}\) This is a disturbing development, because not only can a drone be used to view a person over a fence or through a window of a home, but it can also be used to view people through an actual wall of a house or building.\(^{58}\)

3. Possible Drone-Related Privacy Invasions

Taking flight and video recording capabilities into consideration, together with a little bit of devious imagination, one can start to see the immediate threats that consumer drone technology poses to personal privacy if and when it is used in the wrong way. For example, a consumer drone can be piloted over another person’s private property without permission to capture pictures or video of the person or the person’s family members in or around their home, a place where they have a reasonable expectation of privacy.\(^{59}\) The aircraft could also be sent to hover outside a window of a home to view or record a person unclothed or engaged in intimate activities, allowing for privacy offenses such as invasion of privacy, peeping, and voyeurism, which will be mentioned below.

Now that consumer drones have the capability to track moving objects miles away from the operator, a drone can be used to follow a person from destination to destination. Since consumer drones are becoming faster, and can fly at speeds over 45 miles per hour, the aircraft can even track a person traveling by way of motor vehicle.\(^{60}\) These capabilities can lead to other types of privacy related offenses like stalking or harassing. In a recent BBC article, a private investigator from Anaheim, California, acknowledged that she frequently uses drones in her investigatory work.\(^{61}\) She has used drones during


\(^{57}\) Id.

\(^{58}\) In Kyllo, a federal agent used a thermal-imaging device to determine whether the amount of heat emanating from a home was consistent with the high-intensity lamps typically used growing marijuana. The Supreme Court held that the use of sense-enhancing technology to obtain information from the interior of a home that could not be obtained through visual observation constitutes a violation of the homeowner’s reasonable expectation of privacy. Kyllo v. United States, 533 U.S. 27, 29 (2001).


\(^{60}\) See United States v. Jones, 132 S. Ct. 945, 954-57 (2012) (whether a GPS device attached to a defendant’s vehicle by police to monitor his movements constituted a search within the framework of the Fourth Amendment).

\(^{61}\) Rose Eveleth, The Private Investigator Who Spies Using Drones, BBC (Mar. 18, 2015),
stakeouts, for aerial surveillance of places difficult for her to access on
foot, to observe meetings between people in a public place, or even to
follow delivery trucks from a delivery location to their depot.\footnote{62}
Lastly, consumer drones can be used to commit crimes that
partially relate to privacy rights such as theft or corporate espionage. A
potential burglar could easily use a consumer drone to case a house or
a building to see if anyone is inside or if a window or door is open. A
business could engage in corporate espionage by using a consumer
drone to capture sensitive images of a competitor’s manufacturing
plant or product. The potential for wrongdoing is real and dangerous.

4. The Public’s Concerns

A recent online survey asked 1,007 adults from all over the
country what they know and think about drones.\footnote{63} The term “drone”
was commonly recognized: 78.4% said they are very aware or
somewhat aware of the technology.\footnote{64} Of those who were interested in
owning a drone, the leading reason cited was that they see it as “a fun
hobby.”\footnote{65} In fact, 73.2% were drawn to the hobby idea, 32.7% said they
want to see their “own property from heights,” 28.7% selected
“safety/security interests,” and 11.7% actually admitted to wanting “to
observe my neighbors.”\footnote{66} The majority of survey respondents didn’t
necessarily like the notion of drones becoming prevalent: 73.1% said
they are somewhat concerned or very concerned about drones in U.S.
airspace.\footnote{67} Importantly, the top concern selected by respondents was
personal privacy issues at 64.4%.\footnote{68} In answer to a different question, a
resounding majority of 81.9% somewhat or strongly agreed that drones
should be prohibited from photographing one’s backyard, house, and
family.\footnote{69}

As for the public’s growing concern with drone technology, one
logical explanation is the rising number of drone incidents making
national news headlines. For example, a recent NPR story told of a San
Francisco resident whose wife was sitting in the living room of their

\footnotetext{62}{Id.}
\footnotetext{63}{Payne, supra note 33.}
\footnotetext{64}{Id.}
\footnotetext{65}{Id.}
\footnotetext{66}{Id.}
\footnotetext{67}{Id.}
\footnotetext{68}{Other concerns included potentially dangerous interference with airplanes (57.8 %);
weaponized domestic drones (56.4 %); spying by the government on citizens (50.7 %); devices
susceptible to hacking (50.3 %). Id.}
\footnotetext{69}{Sydell, supra note 32.}
home and saw a drone with a camera hovering outside the window.\textsuperscript{70} The lady’s husband recounted the incident: “She started hiding behind furniture because something’s looking in at you . . . and you’re very self-conscious about that all of a sudden,” said the husband.\textsuperscript{71} “I found myself doing the same thing. You’re hiding behind your own furniture in your own house where you just had privacy prior.

\textbf{B. Consumer Drones Are Coming Sooner Than You Think}

In a state like California, which has approximately thirty-nine million citizens,\textsuperscript{72} the proliferation of consumer drone technology is especially worrisome. First, California currently leads the nation in near-misses between drones and manned aircraft.\textsuperscript{73} The state also has the highest number of drones approved for commercial-use in operation today.\textsuperscript{74} Second, the consumer drone market is rapidly expanding, and sales are expected to surpass millions of units by the end of 2016.\textsuperscript{75} That is in addition to the millions that already exist today.\textsuperscript{76} Third, consumer drone prices are dropping at an impressive rate and are now affordable to many people. With more drones in the hands of Californian consumers, the possibility that the technology will be misused increases significantly.

1. The Sheer Numbers

The FAA estimates that millions of consumer drones are already in the hands of the general public. Prior to 2015, the FAA estimates that there were approximately 200,000 recreational-use drones (lightweight consumer drones flown by civilians for recreational purposes) in the hands of U.S. consumers.\textsuperscript{77} The FAA also estimates

\begin{itemize}
\item \textsuperscript{70} Id.
\item \textsuperscript{71} Id.
\item \textsuperscript{74} Scott Kesselman & David Klein, \textit{The First 1000 Commercial UAS Exemptions}, ASS’N FOR UMNANNED VEHICLE SYS. INT’L (Sept. 10, 2015), http://bit.do/First1000Commercial. (Section 333 exemptions are being leveraged by the FAA to grant case-by-case authorization for certain unmanned aircraft to perform commercial operations prior to the finalization of the Small Unmanned Aircraft Systems Rule, which will be the primary method for authorizing small unmanned aircraft systems operations once it is complete).
\item \textsuperscript{75} FAA AEROSPACE FORECASTS, supra note 1.
\item \textsuperscript{76} Id.
\end{itemize}
that 1.6 million recreational-use drones were sold to U.S consumers in 2015. Since the FAA has not yet approved all commercial-use drones for flight, there are very few employed commercially today. However, the number of commercial drones is expected to grow exponentially once the FAA’s rulemaking is finalized in mid-2016.

The precise number of recreational-use drones that already exist in California is unknown. The FAA recently imposed mandatory registration requirements on all recreational-use drones due to a rise in near-miss incidents between drones and manned aircraft, so the FAA will have this information in the near future. For now, we can rely on other indicative data to get an idea of how many consumer drones we can expect to be operating in California.

According to a report released by Senator Dianne Feinstein (D-CA) in October of 2015, California leads the nation in drone-related incidents reported to the FAA to-date. The majority of the incidents consist of close contact between drones and manned aircraft. The most serious incident included a drone actually impeding emergency response efforts. The report analyzed data on all reported drone incidents that occurred in California between April 2014 and August 2015, and found that of the 1,000 incidents reported nationwide, 1 in 5 incidents occurred in California (more than any other state). Since the majority of drones currently operating in the National Airspace System (NAS) are recreational-use drones, it is safe to assume recreational-use operators are to blame.

As for commercial-use drones, a report by the Association for Unmanned Vehicle Systems International analyzed the first 1000 commercial-drone flight exemptions granted by the FAA, and broke

78. The FAA recognizes that their projections are subject to considerable uncertainty because this is a nascent market, the regulatory environment is evolving, and the pace of technology development is unknown. Id.
79. Id.
80. Since 2015, reports of potentially unsafe drone operations have more than doubled, and many of these reports indicated that the risk to manned aviation or people and property on the ground was immediate. Id.
81. Sen. Dianne Feinstein, supra note 73.
82. Id.
83. The report also found that the frequency of incidents steadily increased from one per month starting in April 2014, to an average of more than twenty per month in the spring and summer of 2015. Id.
84. The “National Airspace System” is the common network of U.S. airspace—air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information and services; rules, regulations, and procedures; technical information; and manpower and material. See Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, U.S. DEPT. OF TRANSP., FED. AVIATION ADMIN. (2013), http://bit.do/IntegrationOfCivilUAS.
them down by state and industry.\textsuperscript{85} The report found that California currently leads the nation in commercial-use exemptions granted by the FAA, with 114 approved commercial operators.\textsuperscript{86} California’s commercial exemptions include the following industries by number: 52 aerial photography; 36 real estate; 32 aerial survey; 27 filmmaking; 20 agriculture; and 13 construction.\textsuperscript{87}

Importantly, these reports demonstrate that California is already experiencing a high number of consumer drone operations. The state currently leads the nation in recreational-use near misses and commercial-use interest. These are startling facts for California, considering the drone industry is in its infancy. In the next few years the number of drones in the airspace above California will drastically increase.

2. The Market Growth Rate

The projected growth of the consumer drone market as a whole is astonishing. On the recreational-use side, the FAA expects 1.9 million drones of this type to be sold by the end of this year alone, with an annual growth rate thereafter averaging 23\% for the next five years.\textsuperscript{88} This is in addition to the drones already in consumers’ hands. By the end of 2020, the FAA projects recreational-use drone sales to reach 4.3 million units.\textsuperscript{89} On the commercial side, the FAA expects 600,000 units to be sold after its proposed commercial rulemaking is finalized mid-2016.\textsuperscript{90} Sales for commercial-use applications are expected to rapidly accelerate with different growth rates in different applications.\textsuperscript{91} Commercial sales are projected to grow from very few today, to nearly 11 million units by 2020.\textsuperscript{92}

3. Affordability

As consumer drone sales increase, and the market expands, there will inevitably be a drop in the purchase price of drones. The consumer

\textsuperscript{85} Kesselman & Klein, supra note 74.
\textsuperscript{86} Id.
\textsuperscript{87} Id. at 6.
\textsuperscript{88} FAA AEROSPACE FORECASTS, supra note 1, at 9.
\textsuperscript{89} The FAA’s forecast is not far off the mark when compared to similar reports released by industry experts. Business Insider Intelligence (BII) projects the consumer drone market to grow at a compound annual growth rate of 19% between 2015 and 2020. See Business Insider Intelligence, The Drones Report: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications, BUS. INSIDER, (Jun. 10, 2015), http://bit.do/MarketForecastsDrones.
\textsuperscript{90} FAA AEROSPACE FORECASTS, supra note 1, at 9.
\textsuperscript{91} Id.
\textsuperscript{92} Id.
drone market is nascent, and analyzing the fluctuation of drone prices with precision is not yet possible because there is no historical data for experts to analyze. Consumer drones do not yet have a unique trade classification, and they can be classified as helicopters, toys, or even cameras.\textsuperscript{93} However, industry experts are looking to U.S. Census Bureau data on “light weight helicopters” to get preliminary clues on pricing trends.

According to the US Census Bureau data, U.S. buyers bought at least 24,070 helicopters weighing less than 2200 pounds in 2015.\textsuperscript{94} Most drones weigh significantly less than 2200 pounds (many are less than five pounds), so this category of goods is broader than just unmanned helicopters, and includes certain light, manned helicopters.\textsuperscript{95} However, consumer drones likely make a significant part of it, as the average price of the goods imported under this category has dropped to levels far below that of even the cheapest manned craft.\textsuperscript{96} The average price of goods imported under this heading have historically been measured in hundreds of thousands of dollars.\textsuperscript{97} However, around the year 2010, the prices dropped dramatically, and the prices reached a record low in 2015 at around $1,000 per unit.\textsuperscript{98}

A quick survey of Amazon.com underscores the point. The most popular drone with video recording capabilities sold on Amazon.com is the “DJI Phantom III Standard,” currently priced at $450.00.\textsuperscript{99} A year ago, that same model was priced at $800.00,\textsuperscript{100} a significant price decrease. Thousands of drones with similar capabilities are available from online retailers at a variety of different prices.\textsuperscript{101} As the consumer drone market continues to grow, and economic competition among the many consumer drone manufacturers drives prices down, more and more consumer drones will make their way into the hands of the general public.

C. FAA Not Regulating Drone-Related Privacy Issues

\textsuperscript{93} David Yanofsky, How Rapidly Drones are Coming to the U.S., QUARTZ.COM (Dec. 23, 2015), http://bit.do/DronesComingToUS.
\textsuperscript{94} Id.
\textsuperscript{95} Id.
\textsuperscript{96} Id.
\textsuperscript{97} Id.
\textsuperscript{98} Id.
\textsuperscript{100} Phantom 3 Standard, DJI (2016), http://bit.do/Phantom3StandardDJI.
\textsuperscript{101} Quadcopters and Multirotors, AMAZON.COM (2016), http://bit.do/QuadcoptersAmazon.
Recognizing the inevitable rise of consumer drone technology, Congress enacted the Federal Aviation Administration Modernization and Reform Act of 2012 (Act), which directed the FAA to establish a framework for safely integrating unmanned aircraft into the NAS. As will be demonstrated, the FAA does not intend to regulate drones flown for hobby purposes as heavily as other types of drones. Naturally, most of the drones that the states are concerned about fall under this lightly regulated designation. Additionally, the FAA does not intend to regulate issues unrelated to flight and safety, meaning issues such as privacy will be left to the states to regulate. Therefore, California must act alone if it wants to protect its citizens’ privacy from consumer drone technology.

1. The FAA Modernization and Reform Act of 2012

The Act defines “unmanned aircraft” as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. The Act also divides unmanned aircraft into three distinct categories. The first category is “public unmanned aircraft,” which is roughly defined as an aircraft owned or operated by a government or state entity. The second category is “civil unmanned aircraft,” which is defined as any aircraft that is not a public unmanned aircraft. This category encompasses all drones flown for commercial purposes. The third category is “model aircraft,” which is defined as an unmanned aircraft that is (1) capable of sustained flight in the atmosphere; (2) flown within the visual line of sight of the person operating the aircraft; and (3) flown for hobby or recreational purposes.

The Act essentially shut down the NAS to all civil and public unmanned aircraft until the FAA can establish requirements for the safe operation of these systems. The Act does, however, permit certain civil unmanned aircraft operations to take place before the FAA’s framework is implemented. Section 333 of the Act authorizes the FAA

---

103. As will be explained below, the FAA has created its own drone terminology that separates drones into separate classifications, with “model aircraft” defined as drones that are flown for hobby or recreation.
104. FAA AEROSPACE FORECASTS, supra note 1.
105. FAA Modernization and Reform Act § 331(8).
108. FAA Modernization and Reform Act § 336(c).
109. Id.
to establish special interim requirements for the operation of these aircraft by designated operators, provided the aircraft and their operators meet certain minimum standards and have applied for a “commercial use exemption.”

To date, thousands of commercial operators have received this exception, meaning they may permissibly fly commercial drones in the NAS. The commercial operators include a variety of businesses such as film production, construction, surveying, inspection, and real estate. The Act contains a similar exemption for public unmanned aircraft, allowing governmental entities operate drones upon application, provided the aircraft and their operators also meet certain minimum criteria.

2. Model Aircraft Remain Fairly Unregulated

Unlike with civil and public unmanned aircraft, the Act expressly prohibits the FAA from promulgating any rule affecting model aircraft, so long as the aircraft meets certain limited criteria. The model aircraft must (1) be flown strictly for hobby or recreational use; (2) be operated in accordance with a community-based set of safety guidelines; (3) weigh less than fifty-five pounds; (4) give way to other aircraft; and (5) not be flown within five miles of an airport. If the model aircraft meets all of these criteria, the FAA essentially lacks the ability to control when, where, and how model aircraft are to be operated. To be sure, most consumer drones fit within these criteria, which is why state lawmakers across the country are concerned with this type of drone in particular. Consumer drones already vastly outnumber other drone types. They are also the ones most commonly purchased by ordinary civilians.

To compare the difference between how model aircraft and other types of drones will be regulated, it is helpful to look at the FAA’s proposed rulemaking for “Small Unmanned Aircraft” (SUA). The FAA essentially defines this subclass of drone as any drone weighing...
less than fifty-five pounds that is not a model aircraft. The FAA requires SUA operators to be certified before they can take to the skies. To receive certification, the operator must pass a knowledge test, must obtain an airman operator certificate, and must be vetted by the Transportation Security Administration. Once certified, SUA operators must abide by a comprehensive list of operational limitations that state where, when, and how they may operate their drones.

The FAA recently acted unilaterally in finding that the Act granted it the authority to promulgate flight safety rules regarding all “aircraft.” Citing a dramatic rise in potentially unsafe consumer drone operations (pointing the finger mainly at model aircraft operators), the FAA mandated that all aircraft weighing less than fifty-five pounds must register with the FAA’s civil aviation registry. Although the registration process itself is rather lax (you only have to be over the age of thirteen and provide your name, address, and telephone number to the FAA Registry), the registration does allow the FAA and law enforcement agencies to address non-compliance by providing the means by which to identify an aircraft’s owner and operator.

3. States Must Regulate Privacy Issues on Their Own

The FAA has exclusive authority to regulate the areas of airspace use, management and efficiency, air traffic control, safety, navigational facilities, and aircraft noise at its source. It also has exclusive authority to prescribe air traffic regulations on the flight of aircraft for navigating, protecting, and identifying aircraft; protecting individuals and property on the ground; using the navigable airspace efficiently; and preventing collision between aircraft, between aircraft and land or water vehicles, and between aircraft and airborne objects.

Congress brought consumer drones within the regulatory reach of the FAA by directing it to establish requirements for the safe operation of the drones.

---

117. This subclass only includes drones that are flown for commercial or governmental purposes. Id.
118. Id.
119. Id.
120. The Secretary and the Administrator recently affirmed that all unmanned aircraft, including model aircraft, are aircraft consistent with congressional direction in Title III, Subtitle B of Public Law 112-95 and the existing definition of “aircraft.” Id.
121. FAA AEROSPACE FORECASTS, supra note 1.
122. Id. at 5.
of drones in the NAS.\textsuperscript{125} Aside from that grant of power, the FAA has no authority to regulate any other issues than the ones discussed above.\textsuperscript{126} In fact, the U.S. Government Accountability Office reports that “FAA officials and others have suggested that regulating privacy issues in connection with equipment carried on [drones], such as surveillance sensors that do not affect safety, is outside the FAA’s mission, which is primarily focused on aviation safety.”\textsuperscript{127} Therefore, it will be up to states like California to tackle issues such as these on their own.

Lastly, although the FAA is not regulating privacy as it relates to drones, states are not free to enact legislation that interferes with FAA flight regulations for the purposes of protecting privacy. The FAA has an exclusive mandate to manage the NAS safety and effectively, and any state regulation that directly or indirectly interferes with drone flight will necessarily be interfering with that mandate. If California is going propose meaningful drone-related legislation, it must take these points into consideration.

II. CALIFORNIA’S LEGAL LANDSCAPE IS INSUFFICIENT TO MEET THE POTENTIAL THREAT OF CONSUMER DRONE TECHNOLOGY

California has traditionally provided its citizens with numerous privacy protections through its civil and criminal frameworks.\textsuperscript{128} However, the state’s existing civil and criminal laws do not yet meaningfully apply to consumer drone technology. California’s invasion of privacy statute is the one civil law that expressly applies to consumer drones. The law was recently amended to encompass the technology because of fears that drones would be used to invade privacy. However, the legal remedy of the invasion of privacy statute is not readily available to ordinary people because it was enacted for the purpose of protecting celebrities and not the general public. Therefore, the existing legal framework as a whole is insufficient to meet the potential threat of consumer drone technology to most privacy violations.

\textsuperscript{125} FAA Modernization and Reform Act § 336(c).
\textsuperscript{126} The FAA recently signaled to state and local governments that “laws traditionally related to state and local police power, including . . . privacy, trespass, and law enforcement operations, are not subject to federal regulation.” UAS Fact Sheet, supra note 6.
\textsuperscript{127} UNMANNED AIRCRAFT SYSTEMS, supra note 3.
A. California’s Privacy Framework Does Not Yet Apply to Drone Technology.

California’s Constitution expressly protects an individual’s right of privacy against both governmental and private actors. The right of privacy was added to the California Constitution in 1972 by an initiative adopted by California voters. It has since been interpreted by the California Supreme Court as creating a right of action against private as well as governmental entities. California recognizes each of the common law privacy torts, including (1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person’s name or likeness. The right of privacy is also embodied in many of California’s criminal statutes. Those statutes include criminal invasion of privacy, peeping, stalking, eavesdropping, and criminal trespass.

Consumer drone technology could not have been anticipated when many of California’s traditional privacy protections came of age in the 1960s and 1970s. In fact, nearly all of the laws on the books in California that seek to protect privacy do not contemplate violations that can be committed through the use of a consumer drone. Drones are not people, they do not operate on the ground, and they are not solely a camera or video recording device. They are technologically sophisticated aircraft that just recently became popular domestically. Consequently, neither a consumer drone nor its operator fit precisely within the statutory language of existing laws that relate to privacy.

131. Hill, 865 P.2d at 642.
132. Id. at 647 (citing Prosser, Privacy, 48 Cal. L. Rev. 381, 389 (1960)) (California common law has generally followed Prosser’s classification of privacy interests as embodied in the Restatement).
138. California began recognizing all of the common law privacy torts after the Privacy was published in 1960, and California later amended its constitution by ballot initiative in 1972 to guarantee its citizens the right of privacy against both governmental and private entries. Hill, 865 P.2d at 647.
1. California’s Penal Code.

On the criminal side, there are currently no laws that directly address drone technology. California’s criminal invasion of privacy statute is generally not applicable to consumer drones. California Penal Code § 647(j)(1) states that “any person who looks through a hole or opening, or otherwise views, by means of any instrumentality . . . any area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy of a person or persons inside,” is guilty of a misdemeanor.\(^{139}\) Since a drone is both an aircraft and a recording device, it does not fit well within the definition of an “instrumentality” (a periscope, telescope, binoculars, camera, motion picture camera, camcorder, or mobile phone).\(^{140}\)

California’s “Peeping Tom” statute cannot apply to drones because it requires a trespass element. California Penal Code § 647(j) states that “any person, who while loitering, prowling, or wandering upon the private property of another, at any time, peeks in the door or window of any inhabited building or structure, without visible or lawful business with the owner or occupant,” is guilty of a misdemeanor.\(^{141}\) Since a drone operates in the air and is not a person, it cannot loiter, prowl, or wander upon the private property of another within the meaning of the statute.\(^{142}\)

California’s eavesdropping statute is arguably the most applicable to drone technology, but it requires the recording to be between more than one person. California Penal Code § 632 applies to “every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication . . . “\(^{143}\) Although a drone may qualify as a “recording device,” the statute requires the recording of a conversation between two or more people, something a consumer drone is not yet capable of accomplishing easily.

Most obvious is California’s criminal trespass statute. California Penal Code § 602 makes it a misdemeanor to drive any vehicle upon the land of another without their permission,\(^ {144}\) or refusing to leave

\(^{139}\) Cal. Penal Code § 647(j)(1).
\(^{140}\) Id.
\(^{141}\) Cal. Penal Code § 647(j).
\(^{142}\) The word “loiter” means to delay or linger without a lawful purpose for being on the property for the purpose of committing a crime as opportunity may be discovered. Cal. Jury Instr.-Crim. 16.445 (2016).
\(^{143}\) Cal. Penal Code § 632.
\(^{144}\) Cal. Penal Code § 602(a).
another person’s land after being asked by a police officer or the owner.\textsuperscript{145} As will be discussed in detail below, a drone operates above traditional property boundaries, making it extremely difficult to determine when a trespass has in fact taken place.

2. California’s Civil Code.

As with California’s existing criminal laws, almost none of California’s civil laws apply to drone technology. The civil causes of action for both stalking and eavesdropping have the same requirements that the criminal statutes do, so it is not necessary to spell them out here. As for the civil cause of action for trespassing, the inquiry gets much more complicated. California recognizes the common law tort of trespassing, which requires a plaintiff to prove that: (1) he or she owns the property; (2) the defendant intentionally, recklessly, or negligently entered, or negligently caused another thing to enter plaintiff’s property; (3) the defendant did not have permission from the plaintiff; (4) the plaintiff was harmed; and (5) the defendant’s trespass was a substantial factor in causing plaintiff’s harm.\textsuperscript{146}

The complexity of the common law trespass cause of action lies in the question of how far one’s property rights extend into the sky. Property rights in California include rights to the “free or occupied space [above the property] for an indefinite distance upwards . . . subject to limitations upon the use of airspace imposed by law.”\textsuperscript{147} In other words, a California landowner has property rights above his land all the way up the point where the NAS begins. In most residential neighborhoods that do not have an airport nearby, a physical invasion could occur anywhere from the ground level to 500 feet in the air directly above a landowner’s property.\textsuperscript{148}

The trespass vs. airspace conundrum will become worse once the FAA redraws the vertical limits of the NAS to account for unmanned aircraft. Suffice it to say that determining the vertical boundaries of one’s property, and whether a drone in fact flew within those boundaries, and what type of harm it the drone caused the owner, if any, will not be an easy task. The civil trespass laws will not provide adequate privacy protection for the people of California. The one civil law that does speak directly to drone technology is California’s invasion of privacy statute, which will be discussed at length below.

\textsuperscript{145} Cal. Penal Code § 602(o).
\textsuperscript{146} CACI No. 2000, Judicial Council of California Civil Jury Instructions (2016).
\textsuperscript{147} Cal. Civ. Code § 659.
\textsuperscript{148} Id.
B. Invasion of Privacy: The Standalone Statute that Doesn’t Protect the Public at Large.

The only existing law in California that directly addresses drones is California’s invasion of privacy statute. Standing alone however, this law does not provide Californians with a meaningful amount of privacy protection against consumer drone technology. First, California’s invasion of privacy statute was envisioned as an anti-paparazzi law to protect the state’s celebrities. Second, the statute has undergone two amendments in recent years to specifically make it apply to invasions of privacy that are committed through the use of a drone. This makes the civil statute the only existing law in California that directly applies to drones. Third, although the statute now applies to drone technology, it does not provide an adequate baseline level of privacy protection to the general public, because many attributes of civil cause of action are not compatible with the nature of consumer drone technology.

1. California’s Anti-Paparazzi Statute

In 1998, in response to the death of Princess Diana, California became the first state in the country to pass legislation in an attempt to rein in overzealous and aggressive photographers and reporters known as “paparazzi.”149 In order to supplement the common law tort of invasion of privacy, the legislature created a statutory cause of action for invasion of privacy. This statute imposes liability on any person who intrudes upon the private space of another person, in order to capture images or recordings of that person engaging in a personal or familial activity, in a manner that is offensive to a reasonable person.150

The statute defined two distinct types of invasions. The first, a “physical invasion,” occurred where the defendant knowingly entered onto the land of another person without permission or otherwise committed a trespass, with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity, in a manner that was offensive to a reasonable person.151 The second, a “constructive

150. Cal. Civ. Code § 1708.8; see also § 1708.8(l)(1)(A)-(E) (as a civil cause of action, this statute provides damages for invasions of privacy involving the victim’s private, personal, or familial activities under circumstances in which the victim has a reasonable expectation of privacy).
invasion,” occurred where the defendant attempted to capture the same, “through the use of a visual or auditory enhancing device, regardless of whether there was a trespass, if the image...could not have been achieved without a trespass unless the device was used.”

As originally written, the statute would be fairly inapplicable to an invasion of privacy committed through the use of a drone. First, a drone operator could not technically commit a physical invasion of privacy without *physically entering onto the land of another person* to do so. Second, a drone isn’t necessarily a *visual or auditory enhancing device* (such as a telephoto camera lens or parabolic microphone).

In light of these drawbacks, California has subsequently modified its civil invasion of privacy scheme to apply to drone technology in two significant ways. First, state legislators amended the constructive invasion provision to make it applicable to “any device,” thus covering drones. Second, the state amended the physical invasion provision to account for invasions that occur “in the airspace above the land of another person,” to also cover drones. However, California’s civil invasion of privacy statute provides a civil cause of action that has certain characteristics that are generally incompatible with drone technology. The invasion of privacy statute as amended still does not provide an adequate baseline level of privacy protection to the public at large.

2. Drone-Spurred “Constructive Invasion” Amendment

The first drone related amendment to the invasion of privacy statute was signed into law on September 30, 2014. A.B. 2306 was specifically introduced for the purpose of expanding a person’s potential liability for constructive invasion of privacy by applying the statute to the use of *any device*, thus, removing the existing restrictions that a device must be “visual or audio enhancing.” As stated by the bill’s author:

As technology continues to expand, drones will not be limited to merely aerial devices. Instead, advances in robotics will pave the way for manufacturers to develop new devices capable of accessing previously

---

152. A person who violates the statute is subject to general, special, consequential, treble, and punitive damages, as well as a civil fine of not less than $5,000 and not more than $50,000. Cal. Civ. Code § 1708.8(d)-(e) (emphasis added).
155. Id.
inaccessible locations and performing otherwise difficult tasks from a
distance. These advancements will open new avenues of innovation and
productivity for our society, but will also have the potential to erode our
sense of privacy. A.B. 2306 will clarify California privacy laws to better
encompass future advances in technology.\footnote{157}

Importantly, A.B. 2306 does not place unnecessary restrictions on
a person’s ability to lawfully operate their drone in the NAS. This
amendment does not expressly create a trespass restriction for the
purpose of determining where an invasion of privacy occurred with the
use of a drone. Instead, the amendment shifts the focus to an invasion
that occurs through the use of any device, drone included, if that
invasion could not have occurred without a physical trespass. As
written, the bill only affects those who are committing a constructive
trespass for the purposes of invading another’s privacy. It does not
encompass the occasional drone operator who may be unintentionally
operating above private property.

Lastly, because the constructive invasion of privacy provision
only applies to an person who “attempts” to capture an offensive image
through the use of any device, the statute does not appear to apply to a
drone operator who happens to be recording everything and then later
discovers something racy.\footnote{158} Again, the aim of the statute is to stop
someone who “knowingly” or “attempts” to invade another person’s
privacy.\footnote{159}

3. Drone-Spurred “Physical Invasion” Amendment

The second drone related amendment to the invasion of privacy
statute was signed into law on October 6, 2015.\footnote{160} A.B. 856 was
specifically introduced to expand the scope of a physical invasion of
privacy to include a person that “knowingly enter[s] into the airspace
above the land of another person” without permission, or otherwise
commits a trespass in order to capture private images or recordings of
the plaintiff . . . .”\footnote{161} According to the bill’s author:

A.B. 2306 [the constructive invasion or privacy amendment] . . . failed to
prohibit the actual trespass onto the property when the drones come over
fences and past locked gates to spy on people in their yards, or peer into
their windows. AB 856 plugs this loophole in the law by clarifying that a
person will be liable for physical invasion of privacy when they actually
enter onto the property of another, including the airspace immediately

\footnotesize{\begin{itemize}
\item \footnote{157}{Id.}
\item \footnote{158}{Cal. Civ. Code § 1708.8(a).}
\item \footnote{159}{Cal. Civ. Code § 1708.8(a)-(b).}
\item \footnote{160}{A.B. 856, \textit{supra} note 154.}
\item \footnote{161}{Id.}
\end{itemize}}
above that property.\textsuperscript{162}

Importantly, like its predecessor amendment, A.B. 856 does not place unnecessary restrictions on a person’s ability to lawfully operate their drone in the NAS. The amendment does not expressly provide a flight restriction on all drones operating at a specific distance above private property such as between 0 and 350 feet. Like a constructive invasion of privacy, the amendment focuses on the operative act of invading another’s privacy. However, unlike a constructive invasion of privacy, the amendment does put a significant amount of focus on drone flight in the airspace above another’s private property.

4. Incompatibility of § 1708.8 with Drone Technology

Although it is a good start, California’s invasion of privacy statute as amended to apply to consumer drone technology does not provide an adequate baseline level of privacy protection to the general public. As a practical matter, civil lawsuits are expensive and lengthy, and unlike celebrities, the average Californian might not be able to afford to file a lawsuit and hire an attorney to bring pursue an invasion of privacy claim. The filing fee for a civil case in California is $435.00, and the average processing time of such cases is over two years.\textsuperscript{163}

To bring a successful invasion of privacy cause of action against a drone operator, it would also be necessary to have legal representation, and attorney fees are also very high.\textsuperscript{164} Additionally, these types of claims are not an easy sell to plaintiffs’ attorneys because the average recreational-use operator does not have deep pockets and cannot pay large damage awards.\textsuperscript{165} Therefore, one can assume that many non-celebrities, and many no-affluent citizens, will forgo pursuing this type of claim due to the high monetary cost, which has

\begin{itemize}
  \item \textsuperscript{163} 2013 Caseload Statistic Report, Statewide Caseload Trends, JUDICIAL COUNCIL OF CALIFORNIA, http://bit.do/2013CaseloadStatistic (case processing time for civil unlimited cases was 68\% within twelve months, 83\% in eighteen months, and 90\% in twenty-four months).
  \item \textsuperscript{164} In California, the median attorney hour rate starts at $350 for a small firm with 1-3 years of experience, and goes as high as $453 (average) for a large firm with 26-30 years of experience. United States Consumer Law Attorney Survey Report, NAT’L CONSUMER LAW CTR. (2014), http://bit.do/USConsumerLawSurveyReport.
  \item \textsuperscript{165} See H. Morley Swingle & Kevin Zoellner, Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Toms, 52 J. Mo. B. 345, 346 (1996) (suggesting that civil actions are inadequate because most defendants do not have the resources to pay large damage awards and most insurance policies do not cover intentional torts); see also Snakenberg v. Hartford Cas. Ins. Co., 383 S.E.2d 2, 8 (S.C. 1989) (holding that the defendant’s insurance policy did not cover a judgment rendered in a civil suit for intentional invasion of privacy, where the defendant surreptitiously filmed swimsuit models as they changed clothing).
\end{itemize}
the potential effect of leaving many Californians unprotected from this type of privacy violation.

Also, a civil invasion of privacy claim would be very difficult to prove against a drone operator. As discussed at length above, consumer drones are fast, small, and are capable of operating miles away from where its operator is located.\(^{166}\) It is very possible for a privacy invasion to occur through the use of a drone without the victim knowing. Even if the victim were to see a drone and suspect an invasion was afoot, consumer drones do not have identifying marks on the body of the aircraft like traditional aircraft.\(^{167}\) Therefore, actually determining whom the owner is, and where that person is located during the invasion, would be no easy task.

The fact that drone invasions are difficult to pursue civilly means that drone operators have limited incentives to avoid committing privacy invasions. Contrast this with a criminal law approach where drone operators would be on notice that law enforcement had the power to investigate and pursue criminal charges against them if they were to commit a privacy violation. The punishment in this scenario would of course be jail time and possible criminal fines. Unlike a civil invasion of privacy approach, a criminal law approach would serve as more of a deterrent against would-be privacy offenders, and would provide a higher level of stigma against the offenders.

III. CALIFORNIA CANNOT ENACT DRONE LAWS THAT INTERFERE WITH FEDERAL FLIGHT REGULATIONS

In 2015, lawmakers introduced at least eight bills related to drone technology. Five of those bills dealt squarely with privacy concerns such as trespass above real property, trespass above school property, trespass above jail grounds, physical and constructive invasion of privacy, and permissible law enforcement activities.\(^{168}\) So far, only two of the privacy related bills were signed into law, and both dealt with California’s invasion of privacy statute. The bills that were found to be excessive restrictions on drone flight were each vetoed by the Governor as will be discussed below. The efforts to restrict drone flight by state governments is seriously problematic for the FAA’s control of the NAS, because when one or more states begin enacting such legislation, fractionalized control of the NAS is the result.

\(^{166}\) Popper, supra note 14.


A. The Drone/Private Property Trespass Law

So far, California Senate Bill (S.B. 142) has turned out to be the most controversial drone bill introduced by the California legislature.  

The bill was intended to serve as a privacy protection for owners or real property against the threat of drone technology. It attempted to create a new property right in the airspace up to 350 feet above private property with regard to the use of a drone. Any drone operator who flew within that airspace would be subjected to traditional trespass liability for the wrongful occupation of real property. As stated by the bill’s author:

Drones have a lot of potentially useful and extremely innovative uses, but invading our privacy and property without permission shouldn’t be among them. When we’re in our backyards, with our families, we have an expectation that we have a right to privacy. This bill extends these long-established definitions of trespassing and privacy, and brings them into the 21st century by applying them to drones.

The bill received strong support within the legislature and was passed by both houses on October 28, 2015. Although it seemed as if privacy advocates had won the day, the bill was swiftly vetoed by Governor Brown, for fair reason. As written, the bill would enact trespass liability for anyone flying a drone between 0 and 350 feet above real property without the express permission of the property owner, whether or not anyone’s privacy was actually violated by the flight. Any consumer drone operator could potentially be liable for civil damages even if the trespass was unintentional. Importantly, by extending property rights into the airspace, and thus preventing drone operators from flying at certain altitudes, the legislature indirectly interfered with the FAA’s exclusive mandate to manage the NAS safety and effectively.

170. Id.
172. Id.
173. S.B. 142, supra note 169 (“a person wrongfully occupies real property and is liable for damages pursuant to Section 3334 if, without express permission of the person or entity with the legal authority to grant access or without legal authority, he or she operates an unmanned aircraft or unmanned aircraft system less than 350 feet above ground level within the airspace overlaying the real property”).
B. The Drone/School Trespass Law

California Senate Bill 271 (S.B. 271) attempted to make it a criminal misdemeanor to knowingly and intentionally operate a drone on the grounds of, or less than 350 feet above ground level within the airspace overlaying a public school providing instruction in kindergarten or grades 1 to 12, during school hours and without the written permission of a school official.\(^{175}\) Additionally, the bill provided that a first offense would warrant a warning, and a second offense would warrant the issuance of a misdemeanor and a fine of not more than $200.\(^ {176}\) According to the bill’s author:

S.B. 271 [was] intended to stay ahead of the technological curve by providing safeguard for our children while they are at school. By prohibiting drone flights over public schools grades K-12 and prohibiting data capture of activity on school grounds, this bill would provide an important layer of privacy to our students at a place that should be a sanctuary. In addition, it will help protect students from potential harassment, stalking, kidnap or other potential harm that could be facilitated through drones capturing their location, activities and movement patterns on campus.\(^{177}\)

S.B. 271 gained strong support by the legislature and was passed by both houses in September 2015.\(^{178}\) However, like the drone trespass bill S.B. 142, it was quickly vetoed by the Governor’s office.\(^{179}\) Although the Governor did not release a veto statement explaining his actions, the bill likely failed under the same reasoning as S.B. 142. The bill subjected any consumer drone operator who knowingly operated a drone over a school to a criminal misdemeanor. The bill also restricted a drone operator’s ability to operate a drone in the airspace above a school from 0 to 350 feet in the airspace above ground level. S.B. 271 drew upon the same property-based limitations on drone flight as S.B. 142, the difference being that the former uses criminal law, and the latter uses civil law.

C. Problems with Restricting Drone Flight at the State Level

It is important for the California lawmakers to understand that restricting drone flight at the state level interferes with federal flight
regulations and fractionalizes the FAA’s control of the national airspace. The FAA has exclusive authority to regulate aircraft within the NAS as a matter of federal law, and when a state like California attempts to restrict the operation of drones in the NAS, the FAA begins to lose its ability to maintain a safe and sound air transportation system. When one or more states begin enacting such legislation, fractionalized control of the NAS is the result.

1. FAA’s Exclusive Authority for the NAS

By enacting legislation that aims to restrict the ability of a drone to operate in the NAS for the purpose of protecting personal privacy, California lawmakers are doing more harm than good. Creating new property rights in the NAS to prevent drones from operating there is interfering with the federal government’s ability to effectively manage the flight of all aircraft within the NAS. The United States government has exclusive sovereignty over the airspace of the United States. The FAA is also granted exclusive authority to regulate the use of navigable airspace, and may promulgate any air traffic regulations on the flight of aircraft as it sees fit.

In the FAA Modernization and Reform Act of 2012, Congress placed drones within the regulatory reach of the FAA by redefining the term “aircraft” to include “unmanned aerial vehicles.” Thus, the same exclusive authority of the FAA to proscribe air traffic regulations on aircraft also applies to drones. Importantly, even though “navigable airspace” has traditionally included all airspace 500 feet above ground level, the FAA recently signaled its intention to expand this definition to include all airspace above ground level. This is because drones typically operate at altitudes that are less than 500 feet above ground level. Any state statute restricting the flight of a drone at any altitude above ground level will necessarily interfere with FAA regulations.

2. Fractionalizing FAA’s Control of the NAS

Significant airspace safety issues are raised when California attempts to regulate the flight of a consumer drone. To be sure, many of the legislative proposals made by the California legislature do just
that— they place operational restrictions on the flight altitude of drones, and they also attempt to regulate the navigable airspace in that regard. This becomes problematic for the FAA’s control of the NAS, because when one or more states begin enacting such legislation, fractionalized control of the NAS is the result. Unless the FAA can provide consistent airspace regulations, it cannot effectively control airspace and flight patterns, nor ensure safety and efficient air traffic flow.

Further, it is even more important that the California legislature ensures local municipalities within the state do not attempt to enact their own ordinances regulating consumer drones in the NAS. If one local municipality enacts restrictive legislation, and more municipalities follow suit, the NAS will become exponentially fractionalized. To prevent a nightmarish scenario like that from actually happening, it is important that the California legislature leads by example and does not attempt to enact haphazard legislation that signals to local governments that it is ok to do the same.

In the FAA’s own words, “a navigable airspace free from inconsistent state and local restrictions is essential to the maintenance of a safe and sound air transportation system.”\textsuperscript{185} To ensure the FAA’s directive, the Office of the FAA’s Chief Counsel advises state and local governments to refrain from enacting legislation such as “operational restrictions on consumer drone flight altitude or flight paths; operational bans; any regulation of the navigable airspace.”\textsuperscript{186} For example, “a city ordinance banning anyone from operating an unmanned aerial vehicle within the city limits, within the airspace of the city, or within certain distances of landmarks.”\textsuperscript{187}

Lastly, there is an argument to be made here about federal preemption of state law, that any law enacted by the California legislature that affects consumer drone flight or operation in the NAS is impliedly or expressly preempted by federal law.\textsuperscript{188} For now, however, it should be sufficient that California lawmakers appreciate that a consistent federal regulatory system for aircraft and the use of airspace has the broader effect of ensuring the highest level of safety for all aviation operations and California citizens.

\textsuperscript{185} UAS Fact Sheet, supra note 6.
\textsuperscript{186} Id. at 2.
\textsuperscript{187} Id. at 3.
IV. ACHIEVING CALIFORNIA’S PRIVACY OBJECTIVES THROUGH THE PENAL CODE.

California should utilize its criminal law to provide a baseline level of privacy protection from consumer drone technology. Like the recently amended civil invasion of privacy statute, the state’s existing criminal laws can be extended by way of amendment to encompass consumer drones. State and local law enforcement are also the best option for enforcing these laws and investigating privacy violations committed through the use of a drone. Lastly, California can use its constructive trespass approach for laws that require a traditional trespass element, because it does not unnecessarily restrict drone flight.

A. A Baseline Level of Protection Against Drone-Related Privacy Invasions

California can provide an adequate level of baseline protection against drone privacy violations through its penal code. First, the state’s existing criminal laws could easily be extended by way of amendment to encompass foreseeable drone-related crimes. Second, state & local law enforcement agencies are in the best position to deter, detect, investigate, and as appropriate, pursue criminal charges against drone perpetrators. Third, California can build upon its constructive trespass approach in the criminal context to regulate drone privacy invasions without being impermissibly restrictive on drone operation and flight.

1. Amending the State’s Existing Criminal Laws To Encompass Drones

California has long utilized its penal code to protect the personal privacy of its citizens and should not hesitate to make these laws applicable to consumer drones. The state’s criminal laws such as criminal invasion of privacy, peeping, harassing, and eavesdropping further the protection of personal privacy in some capacity. As with the California invasion of privacy statute, these laws can be easily amended to bring drone technology within their legal grasp. If accomplished, it will provide an adequate level of protection for drone offenses that are apt to occur.

More importantly, criminal laws can provide every citizen with a basic level of privacy protection regardless of whether or not they can afford to pursue an action in civil court to redress a privacy violation. Although the civil invasion of privacy statute is applicable to consumer drone technology, it is simply not enough. Not all Californians will have the means to pursue a civil action in court since they are not all high paid celebrities. Placing prosecution responsibilities on the state is a fair-minded solution to this particular disparity.

Further, by amending California’s privacy-related criminal laws, the legislature would provide law enforcement and prosecutors across the state with a clear mandate. As of now, there are no criminal laws that expressly encompass consumer drone technology. When a criminal violation does occur through the use of a consumer drone, there will be no clear avenue for enforcement or prosecution. The legislature should provide the means to punish privacy violators. In addition, amending the state’s penal codes would put all consumer drone operators on notice that if they commit a privacy related violation through the use of their aircraft, they will be criminally punished.

For example, California’s “Peeping Tom” statute, Cal. Penal Code § 647(j), states that “any person who, while loitering, prowling, or wandering upon the private property of another, at any time, peeks in the door or window of any inhabited building or structure, without visible or lawful business with the owner or occupant,” is guilty of a criminal misdemeanor.193 This statute can be amended to encompass drone technology using the constructive trespass approach. We could call it “constructive peeping,” if you will. The language could read: “any person, who peeks, or causes a device to peek into the door or window of any inhabited building or structure, without visible or lawful business with the owner or occupant, is guilty of a constructive peeping, regardless of whether there is a physical trespass, if the peeking could not be achieved without a trespass unless the device was used.” This eliminates the need to draw property-based boundaries into the airspace to establish a drone trespass.

2. The Role of State & Local Law Enforcement

State and local law enforcement are the best line of defense against criminal drone operators. Drone technology is inherently evasive, and it will be extremely difficult, if not impossible, for a civilian victim to detect a privacy invasion in progress and then identify and locate the perpetrator safely and effectively. In reality, law

---

enforcement agencies already have the basic investigatory tools available to them for use in identifying, contacting, and pursuing a drone operator who has committed a privacy violation. State and local law enforcement should be used to provide the necessary baseline protection.

Although all consumer drone operators are now required to register with the FAA, drones will rarely have identifiable markings like one sees on conventional aircraft. Drones also operate at high altitudes, so even if a drone did have identifiable markings it would be very hard to discern the identifying marks unless the drone happened to be flying at a close distance. This is where first responders come into play. First responders can locate and contact the suspected operator of the aircraft and any accomplices more effectively and safely than a civilian can. First responders can conduct witness interviews, victim interviews, and most importantly can collect evidence to be used in the prosecution of the perpetrators.

The FAA is already asking state and local law enforcement agencies to assist in enforcing federal flight safety regulations since the FAA does not have the capacity to do so alone. This being said, it is inevitable that state and local law enforcement agencies will need to be trained to handle various issues relating to drones. For issues such as the reckless operation of a drone, operation of a drone in restricted airspace, the commission of various crimes, or responding to a crash, the function of law enforcement in this capacity will be vital.

Additionally, placing enforcement responsibilities on state and local law enforcement can limit the need for self-help. Take for instance, the story at the beginning of this article of the Kentucky man who shot down the drone hovering over his home. This is a great example of a homeowner taking the law into his own hands when he believed a privacy invasion was afoot. The man thought that he was protecting his family’s privacy, and possibly preventing a trespass, but shooting at a flying object in the sky is a terrible way of handling the problem. He not only destroyed someone else’s personal property, but he could have accidentally shot a person, caused the drone to crash and injure a person or property, or the incident could have very easily


195. Although the FAA retains the responsibility for enforcing FAA’s regulations, FAA aviation safety inspectors, the agency’s principal field elements responsible for following up on these unauthorized and/or unsafe activities, will often be unable to immediately travel to the location of an incident. Id.

196. Matyszczek, supra note 21.
escalated into something worse when he confronted the owners of the drone with a handgun strapped to his hip.\textsuperscript{197}

A number of stories have surfaced on the Internet that have documented serious confrontations between people and drone operators.\textsuperscript{198} People have found other ways of damaging or destroying drones aside from shooting the drone with a gun.\textsuperscript{199} Technology manufactures are catching onto people’s concerns and are developing defensive drone technology such as: GPS jammers,\textsuperscript{200} drone guns,\textsuperscript{201} and drones that attack other drones.\textsuperscript{202} The point is that none of these self-help tactics or defensive measures are necessary if there are laws that people feel comfortable relying upon to protect them. Further, with law enforcement empowered to stop drone violations, the need for an individual to resort to self-help is significantly diminished.

3. A Criminal “Constructive Trespass” Approach

A constructive trespass approach alleviates the need to draw property-related boundaries in the sky for the purposes of establishing where a drone trespass above one’s property takes place. Again, a constructive trespass by a drone would occur where the drone was used to commit an impermissible act, where the impermissible act could not have been achieved without a physical trespass. This would restrict certain unlawful activities conducted with the use of a drone as opposed to restricting actual drone flight, thus eliminating the problem of conflicting state and federal regulation regarding consumer drones.

By shifting the regulatory approach to the unlawful activity, instead of the actual flight of the drone itself, the drone becomes just a mean to an end. The result is that the state achieves the same legislative

\begin{footnotes}
\textsuperscript{197} Id.
\textsuperscript{201} Battelle Drone Defender, BATTELLE (2016), http://bit.do/BattelleDroneDefender (Battelle’s DroneDefender system utilizes a non-kinetic solution that disrupts remote controls and GPS to defend airspace up to 400m against UAS such as quadcopters and hexacopters without compromising safety or risking collateral damage).
\textsuperscript{202} SkyJack: The drone that hijacks other drones in mid-air, GIZMAG (Dec. 8, 2013), http://bit.do/DroneHijacksDrones. (Once activated, Skyjack will detect any nearby wireless connections in range and identify the ones associated with another UAV. Skyjack will then automatically disconnect the drone from the owner’s control through raw packet injection, giving Skyjack complete access to the “zombie drone.” The new owner can individually change their course, adjust their speed, and even view the captured drone’s live video feed.)
\end{footnotes}
goal without interfering with federal aircraft regulation or dabbling in the perplexing issues of redrawning property boundaries into the air for the sake of protecting personal privacy. This is a more effective approach to the regulation of drone for the purpose of protecting the privacy of the public at large from the threat of consumer drone technology.

CONCLUSION

Although it is relatively early in the drone game, California should be taking a more sensible approach to regulating consumer drones as they relate to privacy. Civil causes of action are an appropriate remedy in many situations, but with the complexity of drone technology, another type of legal remedy may be the solution. As it currently stands, the invasion of privacy doctrine is not enough to ensure the public at large with an adequate amount of privacy protection. A more sensible approach for California to take is to utilize its penal code to deter possible drone perpetrators and provide a mechanism for the state’s prosecutors to pursue criminal charges against such individuals. Together with the utilization of state and local law enforcement to investigate, cite, and/or arrest drone perpetrators, the state can fulfill its constitutional mandate to protect the privacy of its citizens in the face of the coming drone threat.