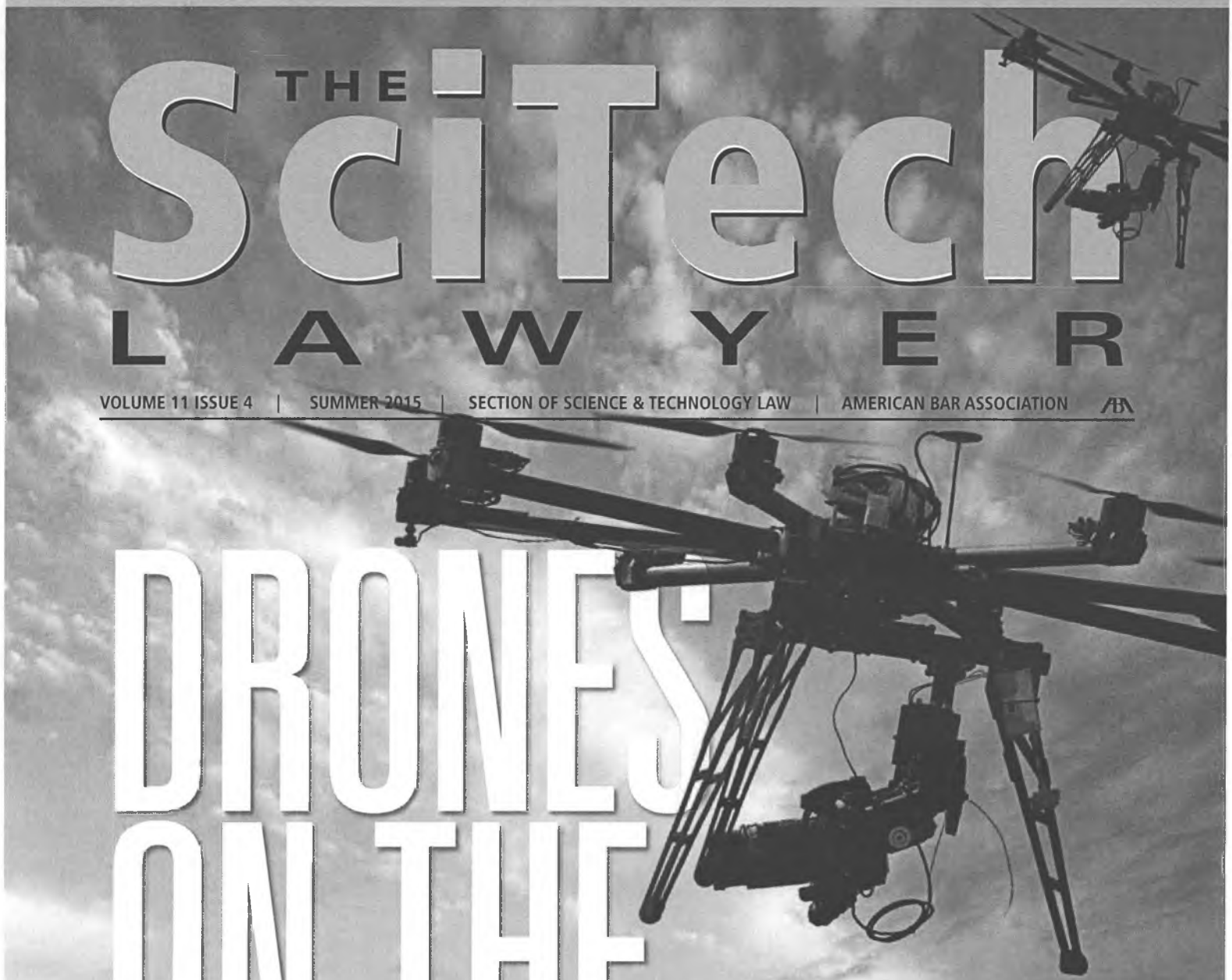
# Drones on the Horizon: SciTech Lawyer (2015)

<TARGET><BILL></BILL><SUBJECT>Drones on the Horizon  SciTech Lawyer (2015)</SUBJECT><COMM><TARGET></COMM></TARGET>

**IN THIS ISSUE** NEW FAA RULES • PRIVACY CONCERNS • REGULATIONS

# THE SciTech LAWYER

VOLUME 11 ISSUE 4 | SUMMER 2015 | SECTION OF SCIENCE & TECHNOLOGY LAW | AMERICAN BAR ASSOCIATION



# DRONES ON THE HORIZON!

## GET READY FOR UNMANNED AERIAL VEHICLES

**MATTHEW HENSHON AND GILBERT F. WHITTEMORE, ISSUE EDITORS**

THE SciTech LAWYER



*The SciTech Lawyer* (ISSN 1550-3003) is published quarterly as a service to its members by the Section of Science & Technology Law of the American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598. It endeavors to provide information about current developments in law, science, medicine, and technology that is of professional interest to the members of the ABA Section of Science & Technology Law. Any member of the ABA may join the Section by paying its annual dues of $35. Subscriptions are available to nonmembers for $55 a year ($65 for foreign subscribers). Some back issues are available for $12 plus a $3.95 handling charge from the ABA Service Center, American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598; 1-800-285-2221. Requests to reprint articles should be sent to ABA Copyrights & Contracts, copyright@americanbar.org; all other correspondence and manuscripts should be sent to *The SciTech Lawyer* Managing Editor at the address above. For more information, visit www.americanbar.org/publications/scitech_lawyer_home.html. The material published in *The SciTech Lawyer* reflects the views of the authors and has not been approved by the Section of Science & Technology Law, the Editorial Board, the House of Delegates or the Board of Governors of the ABA. 

# MESSAGE FROM THE CHAIR

## Michael Hawes

Legislators tend to take out the pen quickly when presented with technology bugaboos. Whether we refer to them as drones, unmanned aircraft, or human-free aerial vehicles (I am going to call them HFAVs, though it is far too late at this stage to coin a new term), the ever-shrinking creations of this flourishing industry face potential new laws and regulations aimed at safety, privacy, and other concerns.

Although HFAVs are not bringing about Orwell's dystopian *1984*, their military origins don't do much to quell concern. Casey Civiello gives us a starting point for understanding why the industry faces significant regulatory pressures in an excellent review of a book that details how HFAVs were developed. Of course, naming an example of a new technology "Predator" will have predictable consequences in the court of public opinion.

Knowing that history, our SciTech members then move to the upcoming challenges at this new intersection of science, technology, and law. Lois Mermelstein guides us through the FAA's proposal for new rules in this area. Before we buy a tiny quadcopter with a gyroscopically stabilized camera to film a family water skiing event, or advise a client who wants to do so, it pays to know the regulations that will soon apply to such toys. Matthew Henshon and Gil Whittemore also step in to help identify how to safely comply with new regulations.

Not sure that the quadcopter really has the capacity to do such filming? Donna Dulo helps us understand the technical capabilities of HFAVs. And, assuming it can, Richard Balough steps us through a possible encounter with a client who wants to be on the cutting-edge of assisted aerial photography. Clients who like to push forward at the technological edge are always in need of SciTech lawyers who keep them from falling. Our section, through *The SciTech Lawyer*, books, webinars, and live conferences, gives our members the tools to serve those clients.

After the clients who want to play come the clients who are concerned about the consequences—and the concern that is the current priority is privacy. Hillary Farber, Janna Lewis, and Lauren Caplan work together to present the different privacy issues resulting not only from an HFAV that can't get above a couple hundred feet in altitude, but also from aerial data collection platforms ranging as high as satellites that collect observation data of unprecedented accuracy. At SciTech, we want to make sure our members have access to the information needed to look at all sides of an issue, and this issue of *The SciTech Lawyer* certainly gives you that. ◆

# TABLE OF CONTENTS

BY MATTHEW HENSHON
AND GIL WHITTEMORE

# DRONES ON THE HORIZON!

## GETTING READY FOR UNMANNED AERIAL VEHICLES (UAVs)

It is now likely that some of you will be advising clients within 12 months on how to safely and legally comply with new regulations governing unmanned aerial vehicles (UAVs, or more colloquially, "drones").

The UAV story begins back in the early part of the 20th century, but it has really accelerated in the past few years. In the last few months, UAVs have burst into the national consciousness. From General Atomics' Predators circling high above the tribal areas in Pakistan, to last summer's private operator flying his quadcopter through exploding July 4th fireworks,[1] new flying systems were seen everywhere. And from Amazon's proposed package delivery systems to a private operator crash-landing his DJI Phantom on the White House grounds, drones were also over the front-pages and home pages of America's news outlets.

Thanks to a 2012 bill, the Federal Aviation Administration (FAA) is in the process of accelerating the speed of introducing drones into the national airspace. As of press time, more than 489 one-off permits have already been granted. Also, in February the FAA unveiled proposed regulations for light (less than 55 pound) UAVs.

This issue of *The SciTech Lawyer* is designed to familiarize you quickly with drone issues, and to give you a sense of where the industry—and the legal landscape—is headed. We have compiled a diverse and qualified collection of authors to help you understand—from all 360 degrees—where drones are going:

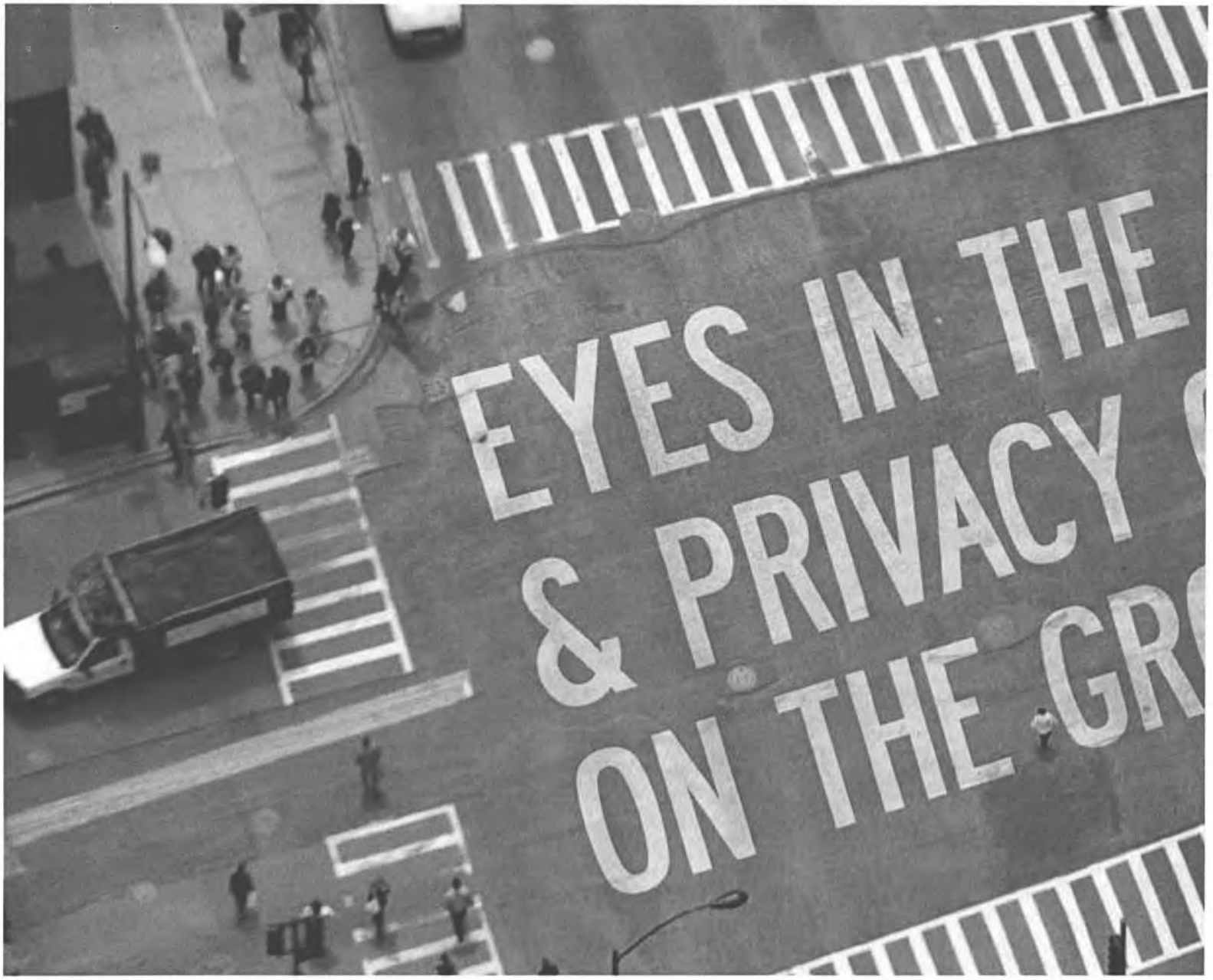
- Privacy issues are often raised in connection with UAVs, and Professor Hillary Farber's "Eyes in the Sky and Privacy Concerns on the Ground" will provide a good primer, as well as touch on what states are doing to protect privacy.
- UAVs are not the only flying objects that can raise privacy issues, however. "Drones to Satellites: Should Commercial Aerial Data Collection Regulations Differ by Altitude?" by Janna Lewis and Lauren Caplan explores the differences—and the similarities—in regulating UAVs and satellites.
- In February, the Federal Aviation Administration published draft regulations for certain (less than 55 pound) UAVs. Lois Mermelstein's "FAA's New Draft Drone Rules" walks you through the proposed rules.
- Related to the draft regulations, the question of defining a UAV is surprisingly complex. Donna Dulo lays out the various classifications of UAVs (and unmanned aircraft systems (UASs) in her "Unmanned Aircraft Classifications: The Foundation for UAS Regulations in the National Airspace."
- Bringing all of these articles back to a real world scenario is the subject of Richard Balough's article, "'So, You Want to Legally Fly a Drone?' How to Counsel a Client."
- And to provide a sense of the history of UAV technology, Casey Civiello reviews the new book, *Predator: The Secret Origins of the Drone Revolution* (Henry Holt and Company, 2014).
- Surely, 2015 is the "Year of the Drone." In addition to this issue, the Artificial Intelligence and Robotics Committee (ST-AIRC) and the SciTech Section will be providing many more opportunities for continued education over the next few months:
  - Many of the authors featured in this issue of *The SciTech Lawyer* will be featured at the ABA Annual Meeting in a Showcase Program entitled "Drones Incoming! Are You Ready for Unmanned Aerial Vehicles (UAVs)?" The program will take place on **Saturday, August 1, 2015, from 8:00–9:30 a.m.**
  - Some of the same issues will be previewed in a CLE teleconference to be held June 22 from 1:00 p.m. to 2:30 p.m. EST. Visit the SciTech website[2] to register.
  - And finally, two[3] of the articles in this issue are in fact excerpted chapters from the forthcoming book from the ABA: *Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law.*[4]

All in all, it's an exciting time to be a lawyer working with technology. We hope that you enjoy this special issue of *The SciTech Lawyer*, and hope you will continue to stay involved in this fast-moving area.◆

*Matthew Henshon is a partner in the boutique Boston firm of Henshon Klein LLP. He is chair of the Section's Artificial Intelligence and Robotics Committee and can be reached via email (mhenshon@henshon.com) or Twitter (@mhenshon). Gil Whittemore serves in an of counsel capacity in the Boston office of Rath, Young and Pignatelli, P.C. (www.rathlaw.com), and is a past Chair of the Section.*

## Endnotes

1. Set to music at https://youtu.be/zlXGU20F-ME.
2. http://www.americanbar.org/groups/science_technology.html.
3. Those written by Hillary Farber and Donna Dulo.
4. Available by visiting http://shop.americanbar.org/ebus/store.aspx.

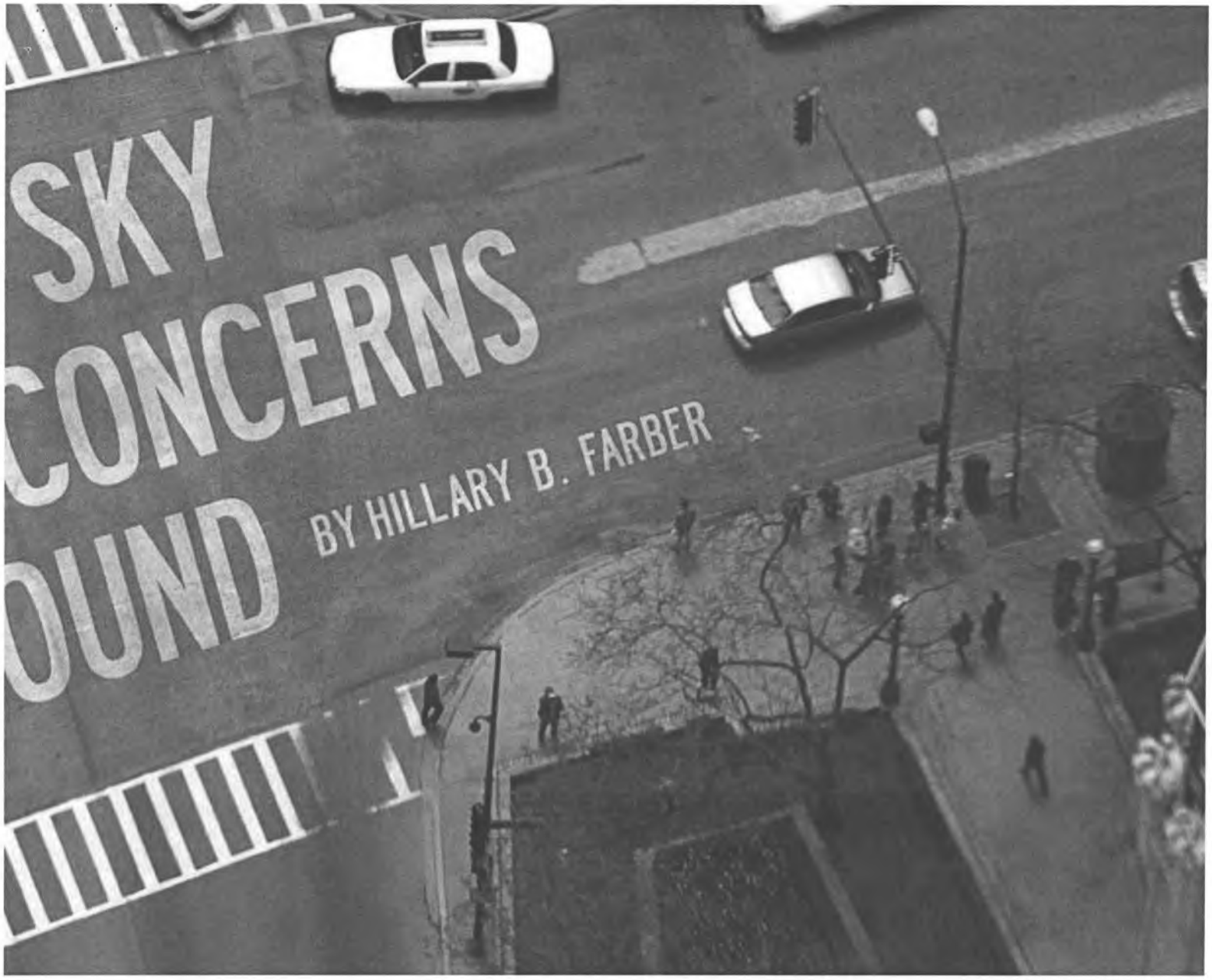



Unmanned aerial systems (UASs), as compared to planes and helicopters, can pose unique threats to society's expectation of privacy. The very essence of pervasive unmanned aerial surveillance enables users to track the movements of large numbers of people simultaneously, zeroing in on people and places on the streets, in their backyards, and even through the open blinds in their homes. The visual imagery gathered can be stored indefinitely, just like other digital data. In contrast to surveillance by manned aircraft, unmanned aerial vehicles (UAVs) are readily portable and have the ability to hover, fly at various altitudes, and stay aloft for hours or even days at a time. UAVs can be small enough that people on the ground are unaware that they are being watched. Moreover, the breadth and scope of the data a UAV can capture is far greater than the capability of traditional surveillance tools. These capabilities set these devices apart from planes and helicopters, or even closed circuit television (CCTV) and satellite surveillance. The aerospace and robotics industries are developing the technology faster than lawmakers and courts can regulate it. Without legislative action limiting aerial monitoring by unmanned aircraft, the privacy Americans have enjoyed in their movements and activities is threatened.

In 2012, Congress passed the Federal Aviation Administration Modernization and Reform Act, which required the Federal Aviation Administration (FAA) to promulgate regulations for the integration of UAVs into the national airspace.[1] In addition, the law directs the agency to create a five-year road map. In 2013, it was estimated that by 2020, there could be as many as 30,000 UASs occupying national airspace.[2] A significant portion of these remotely piloted vehicles will be owned and operated by law enforcement.

Because of the enhanced aerial perspective an unmanned system provides, law enforcement can amass large amounts of data concerning a target, as well as information on people and places about whom the police have no particularized suspicion. Moreover, the expense of operating and maintaining UAVs is estimated at one-fifth that of operating and maintaining manned aircraft.

Interest in using unmanned aircraft in the civil and commercial arenas is growing exponentially. Last year, Amazon,




one of the largest retail companies in the United States, revealed its intention to use unmanned aircraft to deliver packages as soon as the regulations permit. Film production companies, real estate agencies, farmers, and videographers are keenly interested in conducting aerial photography with unmanned systems. The Association for Unmanned Vehicle Systems International (AUVSI) has estimated that integrating UAVs into US airspace would have an economic effect worth more than $13.6 billion, and create more than 70,000 jobs in the first three years.[3]

The FAA has slowly responded to the chorus of manufacturers and owners of unmanned aircraft systems seeking an expansion of certificates for civil and commercial use. In June 2014, the FAA approved the first commercial use of an unmanned aircraft system for surveying the oil fields in and around the Alaskan pipeline.[4] Similarly, in September 2014 the FAA announced that it would permit six media aerial photo and visual production organizations to use unmanned aircraft.[5] Most notably, on February 15, 2015, the FAA set forth a framework of regulations for small UASs (less than 55 pounds) conducting nonrecreational operations.[6] This is discussed in detail by Lois Mermelstein in her article in this issue, found on page 14.

## Federal and State Legislative Activity

While the FAA proceeds with its proposed regulations, there is also activity on the legislative front. Constraints on the use of these powerful aerial observers have been initiated by the White House and lawmakers. On the federal level there is bipartisan concern over the potential for unmanned aircraft to erode personal privacy and civil liberties.[7] Despite a number of Congressional hearings, at present there is no federal legislation regulating the use of unmanned aircraft systems. Perhaps the most comprehensive legislation pending before Congress is the Drone Aircraft Privacy and Transparency Act (DAPTA). DAPTA proscribes limits on the gathering, retention, and sharing of data collected by UAS. It would require that certain disclosures be made as part of the flight approval process, including the identity of the UAV operator; the flight path, the type of data to be collected, and

how the data will be used. Law enforcement agencies would be required to file a "data minimization statement," which would explain how the agency will minimize the collection and retention of data unrelated to the criminal investigation. All this information would be available in a publicly searchable database, including the times and location of all UAV flights, along with disclosures of any data security breaches suffered by a licensee. Moreover, DAPTA would place restrictions on how long the data will be in the possession of the agency that collected it and whether the information can be sold, leased, or otherwise provided to third parties. These measures would add a layer of transparency and accountability to the deployment of unmanned aircraft.

States have responded more quickly than the federal government, all inclined toward restricting the scope and use of unmanned aircraft. At this writing, 18 states have enacted laws ranging from moratoriums on UAS to prohibiting any government official from using an unmanned aerial vehicle without first obtaining a warrant.[8] To date, all but two states have initiated bills and resolutions to regulate the use of unmanned aircraft systems. Efforts to create an enforceable privacy interest are evinced in the titles of the proposed bills: "Freedom From Unwanted Surveillance Act" (Florida),[9] "An Act Relating to Privacy Protection" (Vermont),[10] and "Freedom from Drone Surveillance Act" (Illinois).[11] Almost all of these proposed state laws would require a warrant for government surveillance, with some states allowing for exceptions, such as a high risk of a terrorist attack, search-and-rescue missions, preventing the escape of a suspect, imminent danger to life, or serious damage to property. Other provisions in the proposed laws would include barring the use of unlawfully obtained evidence from criminal prosecution, enforcing civil penalties for noncompliance, and limiting the time that data can be retained by law enforcement agencies.

*Hillary B. Farber is an associate professor of law at the University of Massachusetts School of Law in Dartmouth. She can be reached at hfarber@umassd.edu.*

More recently, lawmakers have sought to restrict use of unmanned aircraft by private users. Among the 18 states that have passed laws regulating unmanned aircraft, 10 states include restrictions on private deployment of unmanned aircraft.[12] More than half the UAS legislation introduced in 2014 proposed restrictions on private use of UAVs.

When federal regulation on unmanned aircraft systems is enacted, some of the state laws may be preempted by the federal government's intent to "occupy the field."[13] Because use of unmanned aircraft will exist largely in federal airspace, Congress has the authority to set policy over how UASs are operated. This will undoubtedly cause disruption in terms of the enforceability of particular state statutes.

## Use of Aerial Surveillance by Law Enforcement and Current Fourth Amendment Jurisprudence

In addition to regulatory and statutory responses, there is also the Fourth Amendment and its application to unmanned aerial surveillance. The Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[14] If the police unreasonably intrude upon an individual's reasonable expectation of privacy without a warrant or probable cause, the evidence derived from the illegal search will be inadmissible. Conversely, if there has been no "search," then the Fourth Amendment is not implicated. In 1967 the Supreme Court in *Katz v. United States* declared that the Fourth Amendment protects "people not places," a major departure from the pre-existing property rights-based analysis.[15] The Court's decision transformed the way courts assess whether police conduct constitutes a search under Fourth Amendment principles. Justice Harlan's famous concurrence set forth the two-pronged "reasonable expectation of privacy" test. This doctrinal formulation makes investigatory searches by police constitutionally significant if (1) there is an actual expectation of privacy and (2) the expectation is deemed one that society is willing to recognize as reasonable.[16]

Some years following *Katz*, the Court applied its reasonable expectation analysis to observation from the sky. The Supreme Court decided three important aerial surveillance cases involving police-manned aircraft flying at altitudes of 400 and 1,000 feet, taking pictures of private property concealed from ground observation.[17] In all three cases, the Supreme Court found no reasonable expectation of privacy because the observations were made from public, navigable airspace. The Court reasoned that navigable airspace is the equivalent of a public thoroughfare, open to anyone who abides by the regulations governing air travel.[18]

In 2001, the Supreme Court addressed the constitutional relevance of sense-enhancing technology in *Kyllo v. United States*.[19] The case involved police use of a thermal imaging device. Federal agents suspecting the defendant of using high-intensity heat lamps to grow marijuana plants inside his home used a thermal imaging device to detect the heat levels from discrete areas inside his home. Coupled with other information, the police obtained a search warrant for the house and found marijuana plants growing inside. In this very close case the Court determined that the technology used to obtain information regarding the interior of the home was not in "general public use" and therefore constituted a search.

Unmanned aircraft systems and many of the technologies with which they can be equipped, by contrast, are in general public use. Although the regulations for UAS are still being developed, many people own and operate them.[20] One of the more basic platforms is the AR Parrot drone, which retails for under $300 and is available at many commercial outlets. As the price increases, the onboard instruments get more sophisticated, but the Parrot drone itself is equipped with live-streaming video capability and a 720-megapixel camera. The global proliferation of UASs may well dilute the protections enunciated in *Kyllo*, leaving Americans vulnerable to intrusions in and around their homes by government and neighbors alike.

It is plausible that the increased power that technology affords police could prove to be a significant factor in the Court's willingness to extend the reach

of the Fourth Amendment.[21] In *United States v. Jones*, the Supreme Court considered whether the use of a GPS device to monitor Jones' movements constituted a search within the framework of the Fourth Amendment.[22] Five justices expressed a willingness to reassess the legal framework for evaluating long-term electronic monitoring of a person in public.[23] In two notable concurrences, the justices recognized the "quantum of intimate information about a person" that can be obtained from a GPS device with relative ease and little expense.[24]

Moreover, the qualitative and quantitative differences between digital data and physical objects may influence where the Court draws the line between personal privacy and the public domain. In an even more recent case, *Riley v. California*,[25] Chief Justice Roberts emphasized the pervasiveness of cell phones and their capacity to retain and transport the privacies of life. With such significant privacy interests at stake, the Court unanimously voted to require the police to obtain a warrant before searching a cell phone incident to arrest.

It will likely be some time before courts take on the novel legal issues posed by unmanned aircraft. In the meantime, unmanned aircraft systems are becoming a ubiquitous presence in our airspace. Because of the extraordinary capabilities of UAS, they may need their own set of specific legal controls to ensure privacy, avoid infringing upon First Amendment activities, and prevent discriminatory targeting. Striking the right balance is crucial so that society can enjoy the benefits of this technology without sacrificing the privacy and liberties Americans have relied upon for centuries. ◆

## Note

This article is excerpted from the full-length article, "Sensing and Surveillance: Issues of Privacy in Unmanned Aircraft," which appears in the forthcoming book *Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law*, Donna A. Dulo, editor.

## Endnotes

1. Federal Aviation Administration Modernization and Reform Act, Pub. L. No. 112-095 (2012).

2. *The Future of Drones in America: Law Enforcement and Privacy Considerations, Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 2 (2013) (statement of Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary).

3. Darryl Jenkins & Bijan Vasigh, Ass'n for Unmanned Vehicle Sys. Int'l, The Economic Impact of Unmanned Aircraft Systems Integration in the United States (Mar. 2013), *available at* http://qzprod.files.wordpress.com/2013/03/econ_report_full2.pdf.

4. Jack Nicas, *FAA Gives Approval to BP to Use Commercial Drones*, Wall St. J., June 10, 2014, http://online.wsj.com/news/article_email/bp-launches-landmark-drone-program-in-alaska-1402404549-lMyQjAxMTA0MDEwMDExNDAyWj.

5. Press Release, Federal Aviation Administration, *U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production* (Sept. 25, 2014), *available at* http://www.faa.gov/news/press_releases/news_story.cfm?newsId=17194.

6. *Overview of Small UAS Notice of Proposed Rulemaking*, http://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

7. Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, *available at* https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

8. *See* H.B. 255, 28th Leg., (Alaska 2014); H.B. 1349, 90th Gen. Assemb. (Ark. 2015); S.B. 92, 2013 Leg., 115th Reg. Sess. (Fla. 2013); S.B. 1134, 62nd Leg., 1st Reg. Sess. (Idaho 2013); Freedom from Drone Surveillance Act, S.B. 1587, 98th Gen. Assemb., 1st Reg. Sess. (Ill. 2013); H.B. 1009, 118th Gen. Assemb. (Ind. 2014); H.B. 2289, 85th Gen. Assemb. (Iowa 2014); H.B. 1029, 2014 Reg. Sess. (La. 2014); S.B. 196, 63rd Leg. (Mont. 2013); S.B. 744, 2013 Gen. Assemb. (N.C. 2014); H.B. 1328, 64th Leg. Assemb. (N.D. 2015); H.B. 2710, 77th Leg. Assemb. (Or. 2013); Freedom from Unwarranted Surveillance Act, S.B. 796, 108th Gen. Assemb., 1st Reg. Sess. (Tenn. 2013); Texas Privacy Act, H.B. 912, 83rd Leg. (Tex. 2013); S.B. 167, 2014 Gen. Sess. (Utah 2014); S.B. 1331, 2013 Gen. Assemb., Reg. Sess. (Va. 2013); S.B. 18, 2015–16 Reg. Sess. (Vt. 2015); S.B. 196, 2013-2014 Reg. Sess. (Wis. 2014).

9. S.B. 92, 2013 Leg., 115th Reg. Sess. (Fla. 2013).

10. S.B. 18, Gen. Assemb. 2015-2016 Sess. (Vt. 2015).

11. S.B. 1587, 98th Gen. Assemb., 1st Reg. Sess. (Ill. 2013).

12. H.B. 1349, 90th Gen. Assemb. (Ark. 2015); S.B. 768, 2015 Leg. Sess. (Fla. 2015); S.B. 1134, 62d Leg., 1st Reg. Sess. (Idaho 2013); S.B. 1587, 98th Gen. Assemb., 1st Reg. Sess. (Ill. 2013); H.B. 1009, 118th Gen. Assemb. (Ind. 2014); H.B. 1029, 2014 Reg. Sess. (La. 2014); H.B. 2710, 2013–14 Reg. Sess. (Or. 2013); S.B. 796, 108th Gen. Assemb., 1st Reg. Sess. (Tenn. 2013); H.B. 912, 83d Leg. (Tex. 2013); S.B. 196, 2013-2014 Reg. Sess. (Wis. 2014).

13. See Federal Aviation Administration Modernization and Reform Act, Pub. L. No. 112-095 (2012).

14. U.S. Const. Amend. IV.

15. Katz v. United States, 389 U.S. 347 (1967).

16. *Katz*, 389 U.S. at 361.

17. *See* Dow Chem. Co. v. United States, 476 U.S. 227 (1986); California v. Ciraolo, 476 U.S. 207 (1986); Florida v. Riley, 488 U.S. 445 (1989).

18. *Ciraolo*, 476 U.S. at 213. ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.")

19. Kyllo v. United States, 533 U.S. 27 (2001).

20. Scott Shane, *F.A.A. Rules Would Limit Commercial Drone Use*, N.Y. Times, Feb. 15, 2015, available at http://www.nytimes.com/2015/02/16/us/faa-rules-would-limit-commercial-drone-use.html?emc=eta1&_r=0.

21. *See* Hillary B. Farber, *Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment*, 64 Syr. L. Rev. 1 (2014).

22. United States v. Jones, 132 S. Ct. 945, 948-49 (2012).

23. *See Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

24. *Id.* at 955 (Sotomayor, J., concurring) ("With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.").

25. Riley v. California, 134 S. Ct. 2473 (2014).

# DRONES TO SATELLITES

## SHOULD COMMERCIAL AERIAL DATA COLLECTION REGULATIONS DIFFER BY ALTITUDE?

**BY JANNA J. LEWIS & LAUREN R. CAPLAN**

The news and social media commentary of late reveals considerable discomfort with the idea that "drones," or unmanned aircraft systems (UASs), could be used to collect images and data for commercial purposes. The idea that a flying machine—say, a six-inch quadcopter equipped with tiny cameras—might track people or record images and data about their movements and habits strikes many as invasive.[1]

Yet, for all the recent attention on commercial drones, commercial aerial data collection is hardly a new concept. Private companies have been capturing and commercializing images of the Earth and its inhabitants for decades[2]—never mind that hobbyists have been flying cameras on model airplanes long before the term "drone" entered the public lexicon, or that governments have been peering at the planet from space since Sputnik first beeped across the skies.[3]

Indeed, a growing number of commercial operators are using satellites orbiting hundreds of miles above the Earth to gather data and images,[4] a feat generally referred to as "remote sensing." These operators process and sell the information to companies, research institutes, and even government agencies for various commercial and noncommercial uses.[5] Many of the uses are undeniably beneficial, such as weather forecasting and monitoring disaster zones. Other uses, such as monitoring farmland, livestock movements, and energy and mining resources, give businesses an operational edge, while still other uses of satellite data, such as location-based services and detection of traffic patterns for smartphone apps, are now a daily part of life for countless people.

Few would argue that satellites are as easily accessible or potentially intrusive as drones—satellites are much more expensive to develop, operate, and launch, and not nearly as agile as drones. However, with their increasingly sophisticated optics, sensors, and processing technologies, satellites can record places, events, and people with a degree of precision and pervasiveness that is worrisome for data privacy advocates. From the perspective of commercial satellite and drone operators, issues of data privacy and consumer consent to collection of personal data present significant business challenges.

Existing regulations and proposed rules do little to quell these concerns. Different government agencies

promulgate a patchwork of regulatory schemes and guidelines for operation of commercial drones and satellites, which do not consistently address personal data privacy protections.[6] This makes it difficult for private citizens and commercial operators, alike, to know their rights and duties with respect to collection, storage, and dissemination of personal data and images via commercial aerial platforms.

Yet, even as some federal agencies are considering privacy issues in relation to commercial drone use, questions arise as to whether enactment of privacy regulations for aerial data collection should even be a federal initiative.[16] Still, consistent and interoperable privacy protections cannot be achieved at any level if current initiatives do not contemplate all aerial data collection platforms.

To briefly explain, different regulations apply according to the type of aerial platform (such as satellite, aircraft, balloon, or UAS); the altitude at which it flies; the way it got there (such as self-propelled take-off or rocket launch); whether the platform is operated by a private individual, a commercial entity, or a public sector agency (such as the US military or local law enforcement); and the manner of use and distribution of the imagery and data collected. The Federal Aviation Administration (FAA) regulates commercial drones,[7] and an increasing number of states have proposed legislation to govern commercial drone use within state borders.[8] The federal agencies that regulate aspects of commercial satellite use include the National Oceanic and Atmospheric Administration (NOAA)[9] and Federal Communications Commission (FCC).[10]

Existing commercial satellite and drone regulations approach the issue of aerial data collection in various ways, emphasizing different security issues and priorities. However, none expressly contemplates the growing overlap of aerial data collection capabilities by different commercial aerial platforms. This overlap raises questions about whether privacy and data protections should differ according to the altitude at which a data collection platform flies.

Arguably, increased altitude does not mitigate privacy concerns. The 500-foot ceiling recently proposed by the FAA in its Notice of Proposed Rulemaking[11] (NOPR) for commercial operation of small UASs is not the upper limit of aerial data-capture capabilities.[12] Indeed, many commercial drones are capable of operating at altitudes above 500 feet, or even at suborbital altitudes,[13] well above the reach of data privacy regulations that might stem from the FAA's small UAS rules. At the same time, the resolution and quality of imagery and data captured by commercial satellites is steadily improving and increasingly in demand,[14] yet existing data security regulations do not expressly account for technological improvements that implicate personal privacy. It is not far-fetched to imagine that, soon, a single company could operate both satellites and drones for aerial data collection. Under the current regulatory trajectory, that company could be subject to different degrees of data privacy requirements, despite the feasible similarity in images and other data collected by its satellites and drones.[15]

Of course, it's a complicated issue, and there are no easy answers, but there are opportunities to start the discussion now. Privacy initiatives for protecting data collected by commercial drones are in formative stages and are receptive to input from all stakeholders, and there appear to be options for implementing privacy protections for data and imagery collected via commercial satellite without a complete overhaul of the regulations that currently govern commercial satellite systems.

At the request of President Obama,[17] the US Commerce Department's National Telecommunications and Information Administration (NTIA) recently issued a Request for Public Comment (RPC) on formulation of best practices for privacy, transparency, and accountability in the handling and collection of data by commercial and private drones.[18] Managing this effort will be no small task, and it may take years for a final policy to materialize. However, although the RPC is directed to commercial UAS data collection, NTIA provided a framework that could be used to prompt thoughtful discourse on implementing alighned safeguards for aerial data collection, retention, and dissemination, regardless of platform or altitude.

Likewise, although the existing regulations for commercial satellites heavily emphasize national security protections,[19] there might be ways to address privacy concerns about commercial satellite data collection and implement balanced protections through the existing regulatory process.

For example, NOAA, the agency charged with licensing and regulating US private remote sensing space systems,[20] can require specific and enforceable limitations on operational performance of commercial satellites, which can include limitations on data collection and dissemination.[21] Private satellite operators must submit a Data Protection Plan (DPP) as part of their license application to NOAA.[22] In a DPP, a commercial satellite operator must describe its process for protecting data and information through all stages of collection, storage, and dissemination. The DPP must meet certain minimum requirements, but the DPP can be adjusted to accommodate agency needs

*Janna J. Lewis is a registered US patent attorney and a member of Holland & Hart's Intellectual Property Group and Government Contracts Group. She focuses her practice on licensing and technology transactions and government contracts, with particular emphasis on technologies in the Aerospace & Defense industry, including UAS, satellite, launch, and space transport technologies, and can be reached at jjlewis@hollandhart.com. Lauren R. Caplan is a member of Holland & Hart's Government Contracts Group. She advises commercial and defense contractors on rights and obligations under government contracts and subcontracts, and can be reached at lrcaplan@hollandhart.com.*

and advancements in technology.[23] Just as NOAA requires private satellite operators to describe and adhere to their data security plans, NOAA could require operators to include privacy protections in their DPPs, or similar plans, for imagery and data collected by commercial satellites.[24]

The looming question, then, is what should overarching privacy principles for aerial data collection look like? Who should structure them, and under what mandate? Should commercial drone and satellite operators be required to obtain consent from every person detected by an aerial lens or sensor? If so, when and by what means that will minimize the burden on commercial operators? To avoid regulatory inconsistencies, they would need to be flexible enough to apply to data collected by drones, satellites, aircraft, and even gliders and balloons, and take into account the diverse views, roles, and interests of all stakeholders, public and private alike. They would need to be interoperable with, and deferential to, federal, state, and local regulations and constitutional principles, and should not restrict innovation or inappropriately restrain companies from pursuing commercial opportunities.[25]

There are numerous other important considerations that need attention and analysis, such as whether and under what circumstances compliance should be voluntary, the costs of implementation and management, issues of accountability and enforcement, as well as alignment with international treaties. Components of the existing regulatory framework can be used to address some of these issues, but the discussions need to go beyond commercial UAS operations to include other commercial aerial data collection capabilities.

To be sure, commercial drones and satellites hold tremendous economic potential, and already are spurring growth of vibrant and exciting industries. But the privacy concerns are real. All stakeholders will need to participate in proactive development of balanced rules and policies to address those concerns—ideally, ones that can be implemented consistently across all aerial data collection platforms, current and future, and regardless of altitude.

## Endnotes

1. *See, e.g.*, UAS Privacy Considerations, The Aerospace States Association, *available at* http://aerostates.org/wp-content/uploads/2013/08/UAS-State-Privacy-Considerations-Final2.pdf.

2. Launched in 1999, the IKONOS satellite is the first commercial satellite to collect images from space. *See* Dr. Christopher Lavers, The Origins of High Resolution Civilian Satellite Imaging-Part 2: Civilian Imagery Programs and Providers, Directionsmag.com, 2013, http://www.directionsmag.com/entry/the-origins-of-high-resolution-civilian-satellite-imaging-part-2-civil/307714.

3. NASA, Sputnik and the Dawn of the Space Age, http://history.nasa.gov/sputnik/.

4. Catalog of Earth Satellite Orbits, *available at* http://earthobservatory.nasa.gov/Features/OrbitsCatalog/.

5. *See, e.g.*, DigitalGlobe Industry Solutions, https://www.digitalglobe.com/industries.

6. For example, the Federal Trade Commission has established a privacy protection regime that includes regulation and enforcement of privacy and data security laws; *see* Statutes Enforced or Administered by the Commission, *available at* https://www.ftc.gov/enforcement/statutes; *see also* Susan Landau, *Control Use of Data to Protect Privacy*, 347 Science 504–06 (2015). In principle, people have the right to control the collection, use, and disclosure of their personal data. In the context of online data collection, for example, notice and consent are considered integral elements of personal data protections. But it is not clear that notice and consent would be workable for aerial collection of personal data and imagery. For example, at what stage, and in what manner, should a commercial drone or satellite operator notify consumers that they will collect data, and how would those consumers manifest consent? What, realistically, should a commercial operator do if a consumer declines consent?

7. *See*, FAA Unmanned Aircraft System (UAS) Regulations and Policies, *available at* https://www.faa.gov/uas/regulations_policies/. The FAA also regulates the commercial space transport industry, including commercial satellite launches and reentry, *see, e.g.*, Commercial Space Launch Act, 51 U.S.C. Ch. 509, §§ 50901-23 (2011) and FAA Office of Commercial Space Transportation, Licenses, Permits & Approvals, *available at* http://www.faa.gov/about/office_org/headquarters_offices/ast/licenses_permits/. However, the FAA does not monitor payloads (such as commercial satellites) that are subject to regulation by the FCC or NOAA. Generally speaking, the FAA's jurisdiction ends where space begins.

8. Proposed rules and regulations at the state and local levels are popping up around the country. *See, e.g.* Idaho Code Ann. § 21-213 (Idaho); N.C. Gen. Stat. Ann. § 15A-300.1 (North Carolina); Or. Rev. Stat. Ann. § 837.380 (Oregon); Tenn. Code Ann. § 39-13-903 (Tennessee); Tex. Gov't Code Ann. § 423.003 (Texas); Wis. Stat. Ann. § 942.10 (Wisconsin); *see also* Resolution Supporting Usage of Unmanned Aircraft Systems, the Council of State Governments, *available at* http://knowledgecenter.csg.org/kc/system/files/csg_resolution_supporting_audited_usage_of_unmanned_aircraft_systems_-_approved_9-22-2013.pdf, and the ACLU's Status of 2014 Domestic Drone Legislation in the State, *available at* https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states.

9. Most of the US and international codes, policies, and rules applicable to commercial satellites focus on licensing, data storage, processing, access, and preservation of national security and compliance with foreign policy and international obligations of the United States—and not necessarily on individual privacy. *See, e.g.*, General Conditions for Private Remote Sensing Space System Licenses, *available at* http://www.nesdis.noaa.gov/CRSRA/files/General%20Conditions.pdf; *see also* NOAA Commercial Remote Sensing Regulatory Affairs Office, Overview of NOAA's Commercial Remote Sensing Regulatory Affairs Office (Mar. 31, 2009), *available at* http://calval.cr.usgs.gov/JACIE_files/JACIE09/TuesdayAM/D'AguannoNOAAGovt.pdf).

10. *See, e.g.*, 47 C.F.R. Chapter I (Federal Communications Commission regulations); 15 C.F.R. § 960.11 (Department of Commerce Regulations).

11. Operation and Certification of Small

Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (Feb. 23, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-23/pdf/2015-03544.pdf.

12. *Id.* at 9552 (The NOPR acknowledges potential implications of commercial small UAS operations on privacy, civil rights, and civil liberties, but notes that privacy issues are beyond the scope of the NOPR).

13. As drones gain altitude and the ability to operate at suborbital heights, the line between drone and satellite fades. *See, e.g.*, *Almost Orbital, Solar-Powered Drone Offered As "Atmospheric Satellite," available at* http://arstechnica.com/information-technology/2013/08/almost-orbital-solar-powered-drone-offered-as-atmospheric-satellite/; *see also*, *Tiny NASA Helicopter Drone Could Explore Mars One Day, available at* http://www.space.com/28360-nasa-mars-helicopter-drone.html.

14. Resolution of satellite imagery has evolved from the grainy, 40-foot resolution of photos taken by the first CORONA satellite, to 15- to 60-meter resolution of images taken by, for example, the Landsat 7 satellite, to the high-resolution, digital images now available via satellite constellations circling the globe today. The clarity of the image processed for dissemination is set by the US Department of Commerce, which limits the resolution of commercial satellite images to 25 cm or about 10 inches). This means that objects smaller than 25 cm should not be easy to discern in the image. *See, e.g.*, Andrea Shalal, *DigitalGlobe Gains U.S. Govt License to Sell Sharper Satellite Imagery*, REUTERS, June 11, 2014, http://www.reuters.com/article/2014/06/11/digitalglobe-imagery-idUSL2N0OR2UX20140611.

15. See, e.g., Martyn Williams, *Google's Solar-Drone Internet Tests About to Go Airborne*, Computerworld.com (May 13, 2015), http://www.computerworld.com/article/2896581/googles-solar-drone-internet-tests-about-to-go-airborne.html; Ellen Huet, *Google Buys Skybox Imaging – Not Just For Its Satellites*, Forbes.com (June 10, 2014), http://www.forbes.com/sites/ellenhuet/2014/06/10/google-buys-skybox-imaging-not-just-for-its-satellites.

16. See, e.g., Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, Brookings.edu (September 2014), http://www.brookings.edu/research/reports2/2014/09/civilian-drones-and-privacy.

17. Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

18. Request for Comments on Privacy Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, 80 Fed. Reg. 11978 (Mar. 5, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-03-05/pdf/2015-05020.pdf.

19. *See, e.g.*, the National and Commercial Space Programs Act of 2010, 51 U.S.C. §60101, et seq., formerly the 1992 Land Remote Sensing Policy Act of 1992, 15 U.S.C. 5601 et seq.; Licensing of Private Remote-Sensing Systems, 15 C.F.R. Part 960; National Space Policy of the United States of America (June 28, 2010), *available at* http://www.nesdis.noaa.gov/CRSRA/files/national_space_policy_6-28-10.pdf; U.S. Commercial Remote Sensing Policy (Apr. 25, 2003), *available at* http://www.nesdis.noaa.gov/CRSRA/files/Commercial%20Remote%20Sensing%20Policy%202003.pdf; United Nations General Assembly, Principles on Remote Sensing (Dec. 3, 1986), *available at* http://www.un.org/documents/ga/res/41/a41r065.htm; General Conditions for Private Remote Sensing Space System Licenses, *available at* http://www.nesdis.noaa.gov/CRSRA/files/General%20Conditions.pdf.

20. NOAA, About Commercial Remote Sensing Regulatory Affairs, http://www.nesdis.noaa.gov/CRSRA/.

21. 15 CFR Part 960(b)(1) ("Specific limitations on operational performance, including, but not limited to, limitations on data collection and dissemination, as appropriate, will be specified in each license.").

22. 15 C.F.R. § 960.11(b)(13); 79 Fed. Reg. 24474 (Apr. 25, 2006).

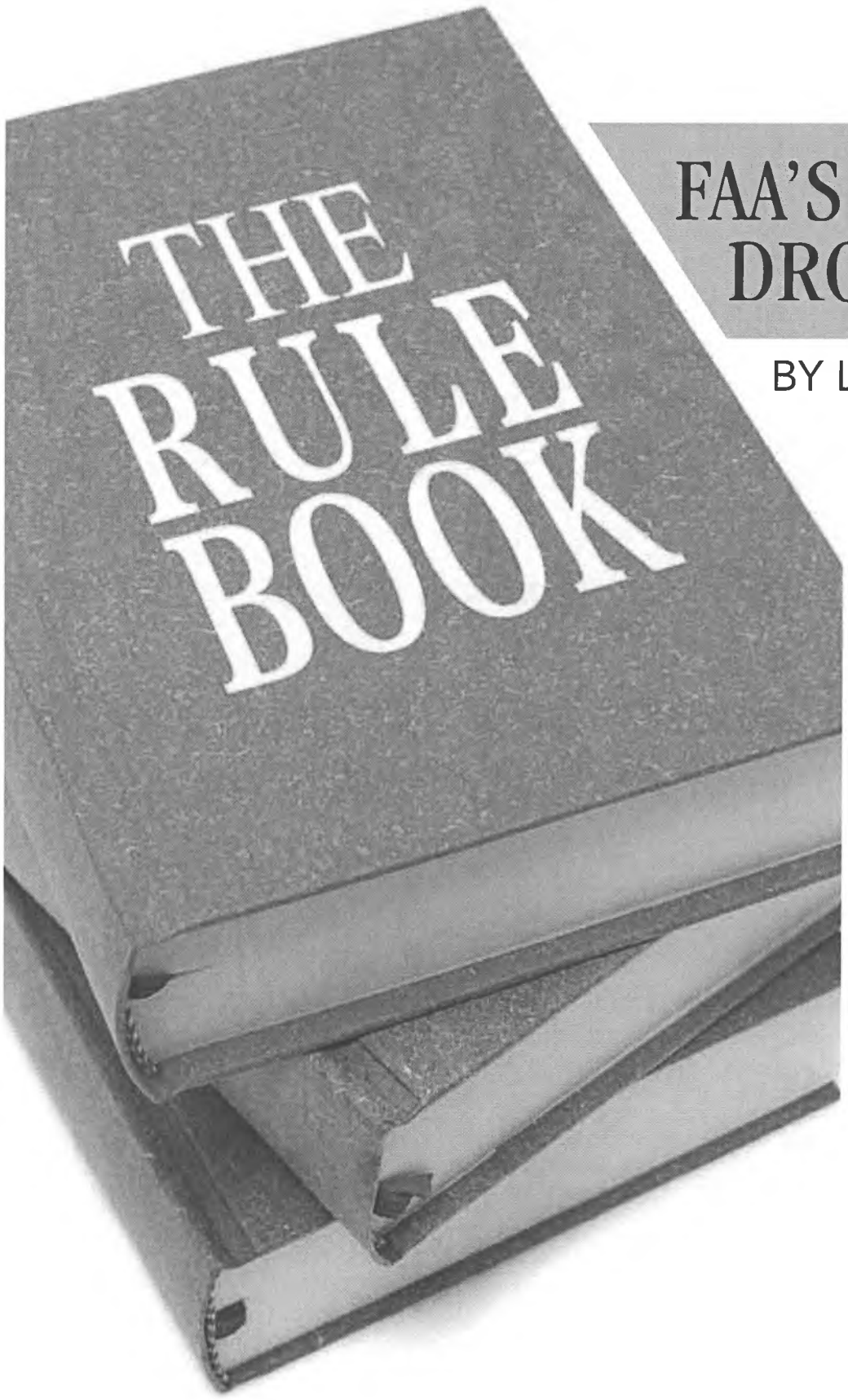
23. *Id.* ("As NOAA licenses more advanced systems, greater emphasis has been placed on protection of the data.")

24. Some commentary has suggested a need to revise commercial satellite regulations to address the CubeSat phenomenon (i.e., the upswing in launch and operation of tiny satellites by people, educational organizations, and other entities who don't realize that, technically, they need a license from NOAA for those activities). If changes are made to address CubeSats, NOAA could also use that opportunity to address privacy concerns relating to data collection by commercial satellites.

25. *See, e.g.*, 80 Fed. Reg. at 11980. NTIA addressed the issue succinctly by asking, "What specific best practices would promote accountable commercial and private UAS operation while supporting innovation?"



Published in The SciTech Lawyer, Volume 11, Number 4, Summer 2015. 




# FAA'S NEW DRAFT DRONE RULES

## BY LOIS MERMELSTEIN

In February 2015, the Federal Aviation Administration (FAA) released its long-awaited draft rules for the operation of small unmanned aircraft systems (UASs), popularly known as "drones." Although it seems these systems are already being used everywhere, commercial uses are currently allowed only with individually granted waivers and other exemptions. Commercial uses, in FAA regulations, are generally those involving aircraft operations for compensation or hire (14 CFR 1.1). For drones, these commercial uses could include newsgathering; crop and wildlife monitoring; inspections of power lines, pipelines, bridges, and antennas; aerial photography; and other research and educational activities. The new proposed rules would apply to all of these activities.

The FAA already regulates manned aircraft through Code of Federal Regulations Title 14. Airplanes, helicopters, balloons, and other aircraft are all covered, as well as the pilots, mechanics, airlines, and others who interact with those aircraft. The FAA had also previously (in 1981) issued an Advisory Circular (AC 91-57) that covered recreational model aircraft. But neither type of regulation was appropriate for unmanned aircraft being used commercially. These new requirements would be added as a new part 107 to the existing rules.

For starters, the new rules set a weight limit—under 55 pounds or

25 kilograms, for the aircraft itself and everything on board. Just as for larger aircraft, the responsibility for and ability to see and avoid other traffic is critical. For drones, this means the operator would be required to always keep the drone "in sight." And this means unaided sight—cameras on the drone, binoculars, and other aids (except glasses or contact lenses for the operator) do not count. The FAA clearly has concerns about drones getting too far from the operator and losing the control signal, does not yet trust cameras on the drone to be sufficient for see-and-avoid, and considers current electronic collision avoidance systems to be too heavy for drone applications. Drones would operate only in daylight and would have to avoid any other aircraft.

Conventional airplanes in uncontrolled airspace—away from airports and close to the ground—need only operate with one mile of visibility and clear of any clouds. But drones in the same airspace would have the stricter requirements—three miles visibility, at least 500 feet under and 2,000 feet horizontally from clouds—that are required of other aircraft only in controlled airspace. This is intended to give the drone operator more time to avoid a manned aircraft. For the same reasons, an operator would only be allowed to handle one drone at a time, and not from a moving vehicle or aircraft (although moving boats would be acceptable, because there are far fewer people, and there is less property, over water).

It's also important that drones not interfere with other aircraft operations. To that end, the rules propose they currently be limited to a maximum altitude of 500 feet, staying below where other (manned) aircraft are allowed to be. Drones could operate in controlled airspace (near most airports) only with air traffic controllers' permission, and no faster than 100 mph (or 87 knots). Drones would also have to stay out of restricted or prohibited airspace without permission, just as for larger aircraft.

All aircraft operators have a duty not to endanger the life or property of others by their operations. So, as is required for larger aircraft, no careless or reckless operations would be allowed; operators would have to do a preflight inspection before flight; and drones could not fly if the operator, aircraft, or environment was in a condition that would interfere with safe operation. One difference from larger aircraft is that drones could not operate over people uninvolved in their operation unless the people below were sufficiently protected from potentially falling drones. And while the prohibition against careless or reckless operations for larger aircraft has been in place long enough to accumulate a substantial body of regulatory and court precedent, what it will mean for drones has yet to be tested.

Drone pilots would now be called *operators*, and would be subject to their own rules. Like pilots of larger aircraft, they would have to pass an initial written test, be vetted by the Transportation Security Administration, and obtain an operator certificate. The test would cover regulations, airspace, obstacle clearance, weather, performance calculations for safe flight, aeronautical decision-making, airport operations, and drugs and alcohol—similar to other pilots' requirements, but adapted for drone operations. Just as other pilots are required to undergo periodic flight reviews, drone operators would have to take a written test every two years. Operators would have to be at least 17, like most other pilots, and have to comply with the same alcohol and drug rules as other pilots. All of this is intended to ensure that drone operators remain under the FAA's authority and operrate as other pilots, hopefully ensuring that everyone using the same airspace stays on the same page.

Drones would not need the types of airworthiness certification and maintenance that larger aircraft have. They would require registration and marking like their bigger cousins, though.

Some types of proposed drone operations would specifically not be allowed under the proposed rules. For example, package delivery via drone, such as Amazon has proposed, would be considered an "air carrier" operation that would not be allowed (even if otherwise under the 55-pound limit). However, the FAA is seeking comment on whether such operations could work within its other proposed constraints, such as line-of-sight operation and the ban on flights over uninvolved persons. External-load and towing operations would not be allowed either, but might be in the future. And any operation might still be possible if the FAA grants an individual waiver for it—as it already has in several instances.

Now that the rules are drafted, and more than 3,000 comments have been received, domestic drone operations are poised to expand rapidly. Even non-aviation lawyers should keep up with developments.

The complete proposed rules with FAA explanatory notes are available at https://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf. ◆

*Lois Mermelstein (lmermelstein@farneydaniels.com) is an associate at Farney Daniels, PC, where she focuses her practice on intellectual property litigation. She is also a licensed fixed-wing pilot and flight instructor.*

# UNMANNED AIRCRAFT CLASSIFICATIONS

## The Foundation for UAS Regulations in the National Airspace

**BY DONNA A. DULO**

The unmanned aerial system (UAS) encompasses a wide range of technologies and aeronautical platforms from the highly sophisticated to the most basic models. The functions, cost, and ability for operators to acquire a UAS vary based on the level of sophistication for each system.

The potential use of UAS technology has grown exponentially over the past few years in the civilian sector. Incorporating lighter composites, advanced embedded electronics, and efficient computational algorithms, the UAS is becoming the platform of choice for increased aerial mobility and functionality for a wide range of operators including police departments monitoring crime to science departments mapping archaeological sites.

The key to UAS use is expanded operations in three-dimensional space. Current UAS technology allows operators to transverse three-dimensional space in a more rapid and customized manner that transcends the current military-based use of the UAS for operations that are too "dull, dirty, or dangerous" for a manned aircraft. Rather, new and innovative uses of unmanned aircraft technologies are facilitated due to the compact and relatively inexpensive nature of unmanned aircraft compared to their manned counterparts. This new-found aeronautical ability for operators enhances real-time situational awareness allowing information to be gathered and disseminated in an exponentially greater manner compared to the past.

The increased information intake allows for significant reductions in decision cycles that results in faster situational resolutions and reduced information product turnarounds. In

essence, new civilian UAS technology has the potential to transform the manner in which agencies and operators do business through enhanced information gathering from a three-dimensional vantage point.

The FAA Modernization and Reform Act of 2012[1] mandates that a plan to integrate UAS technology into US national airspace be developed by the Secretary of Transportation in consultation with the aviation industry and applicable federal agencies. The types of UAS technology are not specified, but rather, the legislation states that agencies will be allowed access to the national airspace as "standards are completed and technology issues are resolved." This plan leaves the technological door open for a wide range of UAS platforms, payloads, and airframe uses in the national airspace. This plan allows for a wide range of flexibility for the FAA to implement the mandates.

FIGURE 1 A Fixed-Wing Unmanned Aircraft[2]

The most basic principle to understand is that a UAS is an aircraft that obeys the same aerodynamic principles as a manned aircraft. In fact, all aircraft theoretically can be remotely operated, ranging from large aircraft such as airliners to high-speed jets. However, unmanned aircraft are distinguished due to their technological design that does not center on a cockpit but rather on their potential mission functionality. Indeed, essentially all unmanned aircraft are designed around their payloads.

Without their payloads, unmanned aircraft would be classified as model aircraft or experimental units. Thus, unmanned aircraft tend to be crafted for specific missions that are evident from the design to implementation, yet their basic technological foundations mirror those of their manned counterparts. The following definitions demonstrate this principle.

The Federal Aviation Administration (FAA) defines an aircraft in the Federal Aviation Regulations (FAR) section 1.1 as, "A device that is used or intended to be used for flight in the air." This definition, which derives its authority from 49 U.S.C. 106(g), 40113, 44701, applies to both manned and unmanned aircraft. The definition of airplane, which emerges from the same authority, is "An engine-driven fixed-wing aircraft heavier than air, that is supported in flight by the dynamic reaction of the air against its wings." This definition rightly applies to both manned and unmanned systems. Exploring this concept a step further under the same authority, the definition of a rotorcraft is "A heavier-than-air aircraft that depends principally for its support in flight on the lift generated by one or more rotors."

Because a UAS can be composed of either fixed-wing or rotorcraft form, all of the above definitions apply perfectly to an unmanned aircraft, because the unmanned aircraft obeys the same three-dimensional aerodynamic principles as its manned counterpart and requires the same basic components to operate in the air. So where is the definitional variance? The definition of unmanned aircraft can be found in The FAA Modernization and Reform Act of 2012, Subtitle B §331:

> An aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

Thus, it is clear that the sole distinguishing factor of manned and unmanned aircraft from a legal definitional standpoint is the absence of a human pilot onboard the physical aircraft. This is a major legal point as well as a technological reality. Without the human on or inside of the aircraft, its legal role in the national airspace is vastly different than its manned counterpart although they both are aerodynamically and technologically similar.

## Types of Unmanned Aerial Systems

There are several ways to classify an unmanned aircraft. Methods of classification vary between the military services, between the military and civilian sectors, and between different countries. In general, it is useful to classify an unmanned aircraft according to three specific criteria:

1. FAA Operational Categories
2. General Airframe Technologies
3. Functional Size Categories.

Each UAS will have a specification within each of the three criteria, allowing for a specific type of identification of the aircraft. This facilitates a general understanding of the performance, range, and maneuverability of the aircraft at an initial glance.

### UAS Operational Categories

To begin the discussion of UAS technologies, the three types of civilian operational categories of the UAS as defined by the FAA are as follows:

- Experimental Unmanned Aircraft
- Model Unmanned Aircraft
- Public Unmanned Aircraft

These are the general categories of UAS that currently exist in the rapidly evolving realm of regulatory definitions. While each are considered unmanned aircraft, they have unique characteristics that warrant their own special category.

*Experimental Aircraft*

Experimental aircraft are unmanned aircraft that serve various experimental purposes such as airframe testing, payload testing, research and development, pilot and aircrew training, academic and educational training,

and systems demonstration aside from air shows and air racing events. Their technologies range from fixed-wing to rotorcraft, to a combination of the two with a plethora of propulsion and payload technologies. The FAA issues special UAS experimental category airworthiness certificates under FAR section 21.191 for operations of experimental aircraft. These aircraft must be operated with full FAA approval. In many cases these aircraft encompass the cutting-edge elements of aeronautical design and development.

*Model Aircraft*
Model aircraft are recreational unmanned aircraft, with technologies ranging from fixed-wing, to rotorcraft to lighter-than-air models, that are regulated by Advisory Circular AC 91-57 and more currently by the FAA Modernization and Reform Act of 2012 section 336 (Special Rule for Model Aircraft). Section 336 defines a model unmanned aircraft as:

1. capable of sustained flight in the atmosphere
2. flown within visual sight of the person operating the aircraft; and
3. flown for hobby or recreational purposes.

The guidelines for model aircraft in section 336 state that model aircraft are flown strictly for hobby or recreational use, are not more than 55 pounds unless otherwise certified, are operated in a manner that does not interfere with and gives way to manned aircraft, and, when flown within five miles of an airport, the airport operator and air traffic control tower are notified, and mutual arrangements are made. Model aircraft are flown within community-based sets of safety regulations that are based upon national community-based model aircraft organizations. These organizations design, develop, and implement their own safety programs for use in the model aircraft community.

*Public Aircraft*
Public unmanned aircraft are discussed in section 334 (Public Unmanned Aircraft Systems.) This section provides the provisions for the establishment of unmanned aircraft in the national airspace. While the ultimate size and limits of the aeronautical technologies of public unmanned aircraft are not defined in section 334, the section does permit government public safety agencies to operate small unmanned systems while the issues of the national airspace are being worked out legislatively. Section 334 allows for an agency to operate an unmanned aircraft weighing 4.4 pounds or less if operated:

1. within sight of the operator
2. less than 400 feet above the ground
3. during daylight hours
4. within class G airspace; and
5. outside of five statute miles from any airport, heliport, seaplane base, spaceport, or other location with aviation activities

The above operational categories are general classifications of UAS. These categories can encompass a wide variety of aeronautical designs and capabilities. These designs and capabilities revolve around the choice of airframe as well as the size the of aircraft being used for a particular mission.

## UAS Airframe Technologies

When looking at an unmanned system, the airframe is the key determinant to the degree of maneuverability that the aircraft will have in three-dimensional airspace. The speed, range, and maneuverability requirements of a UAS will be key factors in determining the choice of technology used to achieve the required mobility for fulfilling the mission of the aircraft. The size and weight of the payload, too, will determine the choice of a UAS airframe technology, as well as time in air or "persistence" requirements. There are four basic types of UAS airframe technologies, as well as hybrid models, that agencies and organizations will be choosing from to achieve their maneuverability, speed, range, and payload requirements:

1. **Fixed-Wing UAS:** a rigid body aircraft with fixed wings, a fuselage, and empennage that uses forward motion to generate lift and move the UAS through the air.
2. **Rotorcraft UAS:** an aircraft that generates lift through rotating rotor blades that revolve around a mast. A rotorcraft can be in the standard single rotor "helicopter" frame, or the popular quad rotor (or more) airframe, where four or more masts and blade systems propel the aircraft.
3. **Tilt-Rotor UAS:** an airframe that uses a pair of powered rotors mounted on rotating shafts that are located at the end of a fixed aircraft wing. The wing of this aircraft is fixed, but the rotors and pylons on which they are mounted tilt in the order of a 90 degree or better range, allowing for various combinations of horizontal or vertical flight.
4. **Lighter-Than-Air UAS:** an aircraft that uses buoyancy to float through the use of one or more large gas bags or canopies.

The choice of UAS airframes, in addition to the payload requirements, will depend on a careful analysis of long-term mission requirements, cost, and pilot capabilities as well as ground station availability and location.

*continued on page 23*

---

*Donna A. Dulo has been with the Department of Defense for more than 27 years and is the president and founder of the Unmanned Aircraft Safety and Security Society, Inc. She is the editor and lead author of the American Bar Association's book* Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law *due out in early summer of 2015.*

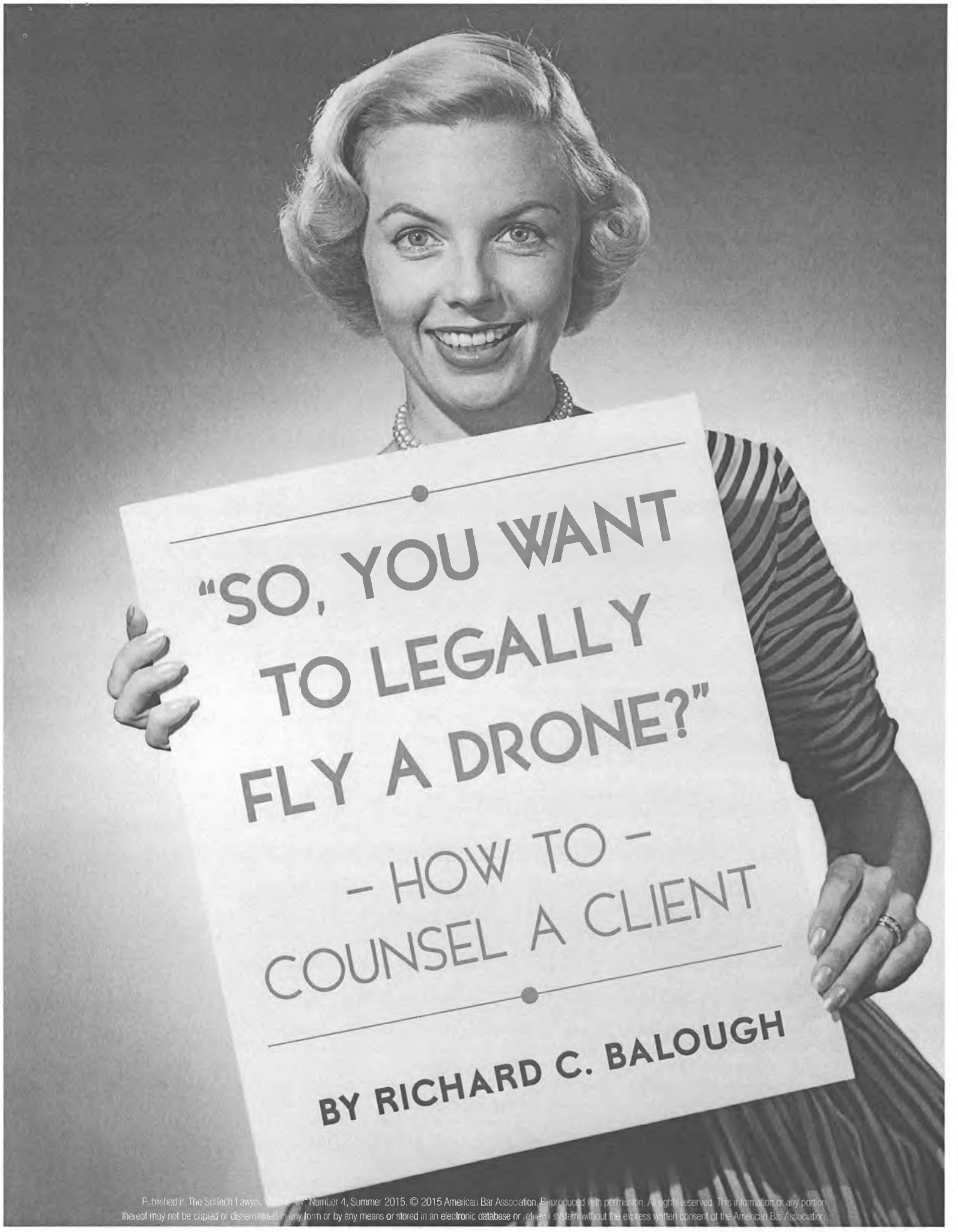

# 2015 ABA SECTION OF SCIENCE & TECHNOLOGY LAW

# ANNUAL MEETING

## JULY 30–AUGUST 1
## CHICAGO / OMNI HOTEL

ABA SECTION OF
SCIENCE & TECHNOLOGY LAW

THANKS TO OUR SILVER SPONSOR BAKER BOTTS



A good client calls you to ask if they should worry about the legal aspects of using a drone for photography. What do you say?

First, appreciate your client's perspective. Drones can take dramatic videos and digital images that could be used for selling real estate, inspecting construction sites, filmmaking, and finding missing persons.

However, unless the business has obtained special permission from the Federal Aviation Administration (FAA), all of these commercial uses currently are illegal in the United States.

The FAA currently prohibits using drones for any commercial purpose without a special permit, and only a few purposes have been approved. As described in more detail in the article by Lois Mermelstein on page 14 in this issue, the restrictions will continue for the remainder of 2015 as the FAA reviews comments on proposed rules to permit limited commercial use of drones. These proposed rules apply only to drones weighing less than 55 pounds. FAA rules for larger drones still are being developed.

Despite the legal obstacles, the desire to use drones will only increase. The cost of drones, technically unmanned aircraft systems (UASs), has decreased dramatically, and the quality of the onboard cameras continues to increase. Drones range from the very small (less than several ounces) to the size of a small airplane. Most personal drones weigh well under 55 pounds. They can fly several thousand feet in the air and out-of-sight of the operator.

*Business Insider* reports that over the next decade 12 percent of an estimated $98 billion in global spending on drones will be for commercial purposes.[1] Another report, from the Association for Unmanned Vehicle Systems International, claims that the industry will create more than 100,000 jobs in the United States in the next 10 years.[2]

With a camera attached, a small drone costing $1,000 or less provides a wide range of commercial functions. As functionality increases (such as more sophisticated cameras, infrared devices and the like), the price increases as well. Actual and announced uses for drones include:

- Photographing bridges to detect faults or areas where maintenance is required. Drones can do a more thorough job than an on-the-ground crew.
- Surveying and assessing damage caused by tornados or hurricanes by insurance carriers. Drones give the insurance adjusters access to the damage almost immediately without interfering with search, recovery, and clean-up operations.
- Inspecting oil and gas pipelines, electric transmission lines, and solar panels by flying closer to the pipelines, transmission lines, and solar panels at lower speeds.
- Providing journalists with overhead images of fires, disasters, and other news events.
- Managing crops. Not only can drones take photographs of crops to monitor crop health and development, but drones also may apply fertilizers, insecticides, and other treatments, reducing the need for large, manned crop duster planes.
- Searching for missing persons, especially where the terrain makes it difficult to cover on foot. A drone can cover far more territory in a shorter time.
- Mapping archaeological sites that are not easily surveyed by airplane.
- Photographing homes for real estate agents.
- Delivering packages, as has been announced by Amazon.com.

However, the increased amount and variety of uses raise both safety and legal issues. Although drones are small and lightweight, a collision with an aircraft might cause extensive damage to the aircraft. If a drone is sucked into a jet engine, it could cause engine failure. A drone flying into a helicopter tail rotor could cause the helicopter to go out of control and crash. As one pilot told the FAA, "If one of those things hits us, we're coming down."[3]

Incidents involving drones are increasing. Early this year, a wayward drone made headlines when it crashed on the White House lawn. In a response to a Freedom of Information Act request by the *Washington Post*, the FAA reported that in a five-month period, pilots and air traffic controllers reported 25 instances where drones came within a few seconds or feet of crashing into much larger aircraft, with many of the near misses occurring near large airports.[4]

Recently, the FAA sent cease-and-desist letters to:

- a commercial photographer who used a drone to take aerial photographs of a house for a real estate company.[5]
- a photographer who posted and offered to sell aerial shots taken with a drone of a concert in Chicago's Grant Park.[6]
- a search and rescue organization that used drones to help find missing persons when ground and horseback searches were not successful or the terrain was too difficult for other methods.[7] The FAA argued that, because the organization took donations, it was involved in a commercial operation.
- two journalism schools that were using drones to take pictures for class stories.

According to the FAA, each of the above uses is a *commercial* use subject to FAA regulation. However, if the commercial aspect of the transaction could be eliminated, these actions would be unregulated by the FAA,

*Richard C. Balough is the Co-Chair of the Global and Connected Devices Subcommittee of the ABA Cyberspace Law Committee. He is a founding member of Balough Law Offices, LLC, in Chicago, Illinois. He has written extensively on technology and privacy issues, and can be reached at rbalough@balough.com.*

although the potential hazard might remain the same. The regulatory category of *commercial* may no longer work.

The ban against commercial drones dates back to a 2007 FAA order, which allows the commercial use of drones only if the operator obtains special FAA permission. In 2012 Congress passed the FAA Modernization and Reform Act, requiring the FAA to integrate drones into the National Airspace System (NAS). The Act directed the FAA to develop a five-year road map for introducing drones into the NAS, to initiate a rulemaking on small unmanned aircraft, and to establish pilot projects.

Some proponents of commercial drones argue that the small craft should be given the same treatment as model aircraft, which are covered by FAA Advisory Circular 91-57, issued in 1981. This circular generally limits operations for hobby and recreational use to below 400 feet, away from airports and air traffic, and within sight of the operator. Some argue that the 2012 Modernization Act confirms drones are model aircraft exempt from regulation if they are flown strictly for hobby or recreational use, weigh less than 55 pounds, are operated in a manner that does not interfere with any manned aircraft, and are flown within visual line of sight of the person operating the aircraft.[8] The distinction between hobby and commercial drones was recognized by the FAA in its initial proposed rules for drones published in February 2015. However, the FAA maintains the right to take enforcement action against model aircraft to protect people and property on the ground. The FAA argues that the model aircraft rules do not apply to commercial uses of drones, regardless of how low they are flying. In other words, *hobby/recreational* and *commercial* may now be overlapping regulatory categories, creating confusion.

In the proposed rules,[9] the FAA attempts to allow the commercial use of drones under 55 pounds while protecting the public and aircraft. The proposed rules limit small UAS to daytime flights, require visual-line-of-sight operations, and restrict altitude to lower than 500 feet.

Because on one hand the FAA does not assert any jurisdiction over the noncommercial use of drones, but on the other hand asserts total jurisdiction over commercial drones, it raises the interesting dichotomy where, if an individual flies a drone to take pictures of her house, her action is not regulated. At the same time, if the same photographs were taken by a commercial photographer for use by a real estate agent selling the house, the activity would be regulated, and—under today's FAA regulations—it would be illegal unless an FAA permit had been obtained. Yet the hazards would be the same.

Until the formal rules on commercial use are finally adopted, businesses may apply to the FAA for special use exemptions, which are subject to public notice and public comment. The FAA has granted authority to several aerial photo and video production companies in the film and television industry to use drones, which weigh about 50 pounds, for their filming. The certificates require that the operators hold private pilot certificates, keep the drones within line of sight at all times, restrict the flights to the "sterile area" on the set, conduct an inspection of the aircraft before each flight, and prohibit operations at night. There are scores of other requests pending.

The ban on commercial drones also grounds drones for news gathering. This has drawn the ire of the media, which argue that the ban violates the First Amendment because news gathering is not a "commercial" use. Rather, the media argue, use of drones benefits the public because the lower-cost aerial photography would help newsrooms bring more accurate and useful information to the public.

Journalists also are concerned about some state laws on drones. For example, Utah criminalizes interference with agriculture operations, which includes "knowingly or intentionally" recording an image of an agriculture operation.[10] This could prevent investigative journalists from photographing a farm as part of an investigative story on agribusiness. Texas prohibits taking photographs of private property "with the intent to conduct surveillance," which might prohibit investigative journalists from using drones over private property.[11]

Several states have enacted legislation regarding the private use of drones. In an interesting twist, Illinois has made it a crime to use a drone "that interferes with another person's lawful taking of wildlife or aquatic life."[12] (For other examples of state regulation of UAVs, see Hillary Farber's article on page 6.) When the FAA does allow commercial use for drones, the use will be subject to laws governing right of privacy, intrusion upon seclusion, and right of publicity for images captured by the drones.

What, then, should a lawyer tell a client who wants to use drones for a commercial use?

The client should be told that the FAA currently bans commercial use of drones in the United States. The client may apply to the FAA for an exception by obtaining a special airworthiness certificate or for a certificate of waiver and authorization. Either process requires a detailed filing, public input, and time. If client does not want to file for a waiver, it could develop the commercial use outside the United States in countries that allow commercial use of drones. Or the client could wait until the FAA's rules on commercial drones are adopted and hope that no one develops and pre-empts the client's use in the interim. ◆

## Endnotes

1. Marcelo Ballve, *Drones: Commercial Drones Are Becoming a Reality, With Huge Impacts for Many Industries*, Bus. Insider, http://www.businessinsider.com/drones-navigating-toward-commercial-applications-2-2014-1.

2. *The Economic Impact of Unmanned Aircraft Systems Integration in the United States*, Mar. 2013, https://higherlogicdownload.

s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf.

3. Craig Whitlock, *Near Mid-Air Collisions with Drones*, Wash. Post, Nov. 26, 2014, http://www.washingtonpost.com/wp-srv/special/national/faa-drones.

4. Craig Whitlock, *Near-Collisions Between Drones, Airlines Surge, New FAA Reports Show*, Wash. Post, Nov. 26, 2014, http://www.washingtonpost.com/world/national-security/near-collisions-between-drones-airliners-surge-new-faa-reports-show/2014/11/26/9a8c1716-758c-11e4-bd1b-03009bd3e984_story.html.

5. Dennis Rodkin, *FAA to Drone Photographer: Cease and Perhaps Desist*, Crain's Chicago Bus., May 29, 2014, http://www.chicagobusiness.com/article/20140529/NEWS07/140529748/faa-to-drone-photographer-cease-and-perhaps-desist.

6. *FAA Reviewing Drone Flying Over Lollapalooza*, Chicago Trib., Aug. 8, 2014, http://www.chicagotribune.com/news/local/breaking/chi-faa-reviewing-drone-flying-over-lollapalozza-20140807-htmlstory.html.

7. *Gene Robinson Drone*, https://www.youtube.com/watch?v=UTcWo4OAwtA.

8. FAA Modernization and Reform Act of 2012, §§ 336 and 337.

9. 80 Fed Reg. 9544 (Feb. 23, 2015).

10. Utah Code Tit. 76, Ch. 6 § 112(2)(a).

11. Tex. Rev. Civ. Stat. 423.001. Titled the Texas Privacy Act, the act deals with use of unmanned aircraft. It allows many uses for drones including research, agriculture, gas and electric inspections, which currently are not allowed by the FCC.

12. 720 ILCS 5/48-3(b)(10).

# Unmanned Aircraft Classifications

*continued from page 18*

### UAS Size Categorizations

A final category of UAS is the functional-size categorization. This category is particularly important in the legal arena as future airspace operations regulations are likely to revolve around UAS size as well as operational category and airframe. The functional size of a UAS not only determines its robustness in terms of aeronautical capabilities and payload abilities, but also its visibility in the air and its maneuverability. Both of these factors contribute to the safe operation of the aircraft.

**FIGURE 2** A Medium-Sized Fixed-Wing UAS[3]

The functional-size categories in the civilian world are arbitrary, except for the small category, which is specifically defined in the FAA Modernization and Reform Act of 2012. The categories are as follows:

- Large UAS
- Medium UAS
- Small UAS
- Micro/Mini UAS
- Nano UAS

These categories cover all airframe types. Additionally, lighter-than-air unmanned aircraft tend to be larger by nature and as such are usually categorized by their specific volume as well as size.

### Conclusion

The classification and categorization of the UAS are vital in understanding the operational capabilities of the aircraft. They are also important for understanding the capability, maneuverability, range, and endurance specifications of unmanned aircraft models and airframes. By understanding the operational and size categories, as well as the airframe technologies of UASs, a defined picture of system capabilities can be drawn in order to understand specific applications of unmanned aircraft.

Understanding the technical capabilities of a UAS also aids the legal practitioner in understanding the legal ramifications of the use and implementation of the specific UAS technology. Each airframe as well as airframe-size classification poses specific legal challenges and issues. By understanding these technological specifications, a clearer picture of emerging legal challenges can be gained. ◆

### Note

This article is excerpted from the forthcoming book, *Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law*, Donna A. Dulo, editor.

### Endnotes

1. The FAA proposed a framework of regulations in February 2015 that is discussed more fully in the article in this issue by Lois Mermelstein on page 14. *See* http://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

2. Photograph by Donna A. Dulo, 2014.

3. Photograph by Donna A. Dulo, 2014.

# Privacy, Security, and the Internet of Things: The Looming Crisis

## — WEBINAR SUMMARY —

REPORTED BY JARED CHANEY

*Trying to determine the market size of the Internet of Things is like trying to calculate the market for plastics, circa 1940.*
*—Michael Nelson, Bloomberg Government & Georgetown University*

To address this hot area, the ABA Section of Science & Technology Law presented a webinar, "Privacy, Security, and the Internet of Things: The Looming Crisis," on Tuesday, March 10, 2015.

Jeff Greene moderated the panel. He is senior policy counsel and covers issues including cybersecurity, identity management, and privacy, and works extensively with industry and the government. Jeff currently serves as Vice-Chair of the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law and Co-Chair of the Supply Chain Working Group on the Information Technology Sector Coordinating Council. The panel included the following faculty members.

- Martha Chemas is an attorney, Internet presenter, and blogger. She has worked with Sullivan & Cromwell LLP, Shearman & Sterling LLP, and Covington & Burling LLP in New York and has taught law with Lawline. She is the Co-Chair of the Information Security Committee of the American Bar Association.
- Cheryl A. Falvey is a Washington, DC-based partner and Co-Chair of Crowell & Moring's Advertising & Product Risk Management Group. An experienced trial lawyer, she provides litigation and counseling services, with a focus on brand and consumer protection matters, including product safety, privacy, anticounterfeiting, sweepstakes, promotions, and advertising.
- Kristen Anderson is a staff attorney at the Federal Trade Commission, in the Bureau of Consumer Protection's Division of Privacy and Identity Protection. Her practice focuses on consumer privacy and data security. She has investigated and pursued cases against advertising companies, financial services companies, and others for violations of the FTC Act, Fair Credit Reporting Act, and Gramm-Leach-Bliley Act.

The panel addressed how so many systems on the Internet of Things (IOT) are venerable to infiltration—not only when there are defects that make them susceptible to hacking, but also when the security features are not utilized. Often infiltrations occur when default credentials are used after the initial setup, or when simple passwords, such as 1234, are used. It is often very hard to get people to change or even set up passwords. The number of essential systems that are vulnerable is staggering, from water treatment plants to a range of medical devices. There are very basic things that are not being done to secure the infrastructure of essential systems.

As new devices and systems are being built, they need to be designed with integral security systems. There are several groups and agencies that are looking into how to encourage data security in the next generation of systems. The potential areas of law that will depend on this type of security range from products liability to patents.

In order to prevent, or at least limit, catastrophe, the next generation will need to bring a new understanding to product design. Companies should not only design precautionary safety measures into products, but also include features to detect security breaches. Furthermore, when a manufacturer designs a new product, it must also determine the effective life of the product and exactly how long it is willing to provide support and upgrades. The risk profile for these issue and concerns does not only affect litigation for product issues and regulation enforcement, but also can cause damage to a client's brand.

When examining these issues, it will be important to understand how the government will control its oversight. The FTC is looking at security vulnerabilities for the IOT. The FTC is focused on the rights and security of the consumers' data. They are trying to make sure that no company is violating or failing to safeguard consumers' data security. Because the FTC's goal is not punishment but compliance, after they settle a case they also monitor the company's compliance with the orders.

Overall, security developments in the Internet of Things will have far-reaching ramifications. As new products are developed, privacy and security will have to be built into those products and services at the outset. Transparency and duty to consumers will have to be considered as data security for the IOT with every new development. With more than 100 billion devices expected to be connected to the Internet in the near future, the benefit to consumers will be immense, but data security and privacy legislation will have to develop along with it.

A full recording of the presentation, along with the CLE materials, can be purchased from the ABA at www.americanbar.org/groups/science_technology/events_cle.html. ◆

*Jared Chaney is a Material Science Engineer, a law student at St. Thomas School of Law, and a law clerk with Kinney & Lange P.A. He also serves the SciTech Section as Student Liaison. He can be reached at chan7393@stthomas.edu.*

# ABA SECTION OF SCIENCE & TECHNOLOGY LAW NOMINEES FOR 2015–2016 SECTION OFFICER AND COUNCIL POSITIONS

The Nominating Committee, chaired by Cynthia Cwik, is pleased to announce the following slate of nominees for 2015–2016 Officer and Council positions in the Section of Science & Technology Law.

The Section membership will vote on the slate of candidates during the Section's Annual Business Meeting, which immediately follows the Council Meeting on Friday, July 31, 2015, during the ABA Annual Meeting in Chicago, IL.

Cynthia Cwik will automatically succeed to the position of Section Chair at the completion of the ABA Annual Meeting in Chicago.

| CHAIR-ELECT | VICE-CHAIR | SECRETARY | BUDGET OFFICER | DELEGATE | COUNCIL | COUNCIL | COUNCIL |
|---|---|---|---|---|---|---|---|
| Eileen Smith Ewing | David Z. Bodenheimer | William B. Baker | Garth B. Jacobson | Bonnie Fought | Katherine E. Lewis | Lisa R. Lifshiftz | Joe Pennell |

## Incoming Section Chair

**Cynthia Cwik** is a partner with the San Diego office of Jones Day. She has extensive experience in complex litigation and class actions, including mass tort and product liability cases, consumer class actions, and environmental cases. She has particular expertise with cases involving health and science issues, and she has had significant victories in high-profile matters. In one case, Cynthia won motions to exclude the testimony of five of the plaintiffs' experts and had the claims of all of the trial plaintiffs dismissed. A journalist described Cynthia as "formidable" and "the mastermind behind the team's savvy attack." She has been selected seven times as a California "Top Female Litigator" by *The Los Angeles/San Francisco Daily Journal*, and she has been included in *Best Lawyers of America*.

Cynthia is currently Chair-Elect of the ABA Section of Science & Technology Law, Vice-Chair of the Long Range Planning Committee and a member of the Section Council. She has served the Section in various leadership roles, including as Life & Physical Sciences Division Co-Chair and coeditor of the ABA SciTech Section book *Scientific Evidence Review: Monograph No. 9*, published in 2013.

She has been active in other bar and community organizations, including serving as Chair of the Executive Committee of the Yale Law School Association and President of the San Diego Chapter of the Federal Bar Association. Cynthia has made presentations to many organizations, including the Association of General Counsel and the National Judicial College.

Cynthia graduated from Yale College in 1983 (summa cum laude) and from Yale Law School in 1987. She served as a judicial clerk to the Honorable Thomas Meskill on the Court of Appeals for the Second Circuit.

## Section Chair-Elect

**Eileen Smith Ewing** practices law in Boston, where she counsels her life sciences clients on a variety of business transactions, ranging from traditional mergers, acquisitions, and capital financing to complex, cutting-edge product development collaborations and other strategic alliances.

Eileen publishes and lectures frequently on legal issues of interest to the biopharmaceutical and medical device sectors. She is the author of more than 50 publications. Eileen served as coeditor-in-chief and a chapter author of the ABA SciTech Section book *Biotechnology and the Law: A Primer*. She also contributed chapters to two books in the Aspatore Press *Inside the Minds* series: *Life Sciences Mergers and Acquisitions* and *Winning Legal Strategies for Life Sciences Settlements and Negotiations*. Legal Media Group/Euromoney has named Eileen a 2012 and 2013 "Life Sciences Star" in the Financial & Transactional category.

Eileen currently serves as Vice-Chair of the ABA Section of Science & Technology Law, Chair of the Administration Division, Vice-Chair of the Long Range Planning Committee, a member of the Section Council, and a member of the Finance Committee. Past ABA positions include Chair and Co-Chair of the Section's Life and Physical Sciences Division, Chair of the Section's Biotechnology Committee, and member of the ABA Special Committee on Bioethics and the Law. Eileen is an American Bar Foundation Fellow and serves as Co-Chair of the Board of the National Conference of Lawyers and Scientists (American Academy for the Advancement of Sciences).

Eileen received her A.B. in East Asian Studies, summa cum laude, from Harvard University and her J.D. from Columbia University School of Law.

## Section Vice-Chair

**David Z. Bodenheimer** is a Government Contracts partner and litigator in Crowell & Moring LLP's Washington, DC, office, where he heads the Homeland Security practice.

Representing all sizes of technology clients for 32 years, David litigates, counsels, and resolves the full range of issues confronting clients selling to the government. *See, e.g., US v. UTC* (6th Cir. 2015) ($657 million False Claims Act litigation); *BAE Systems*, 2013 CPD § 278 (NextGen airborne jammer protest litigation); *Supreme Foodservice GmbH v. United States*, 109 Fed. Cl. 369 (2013) (injunctive action on $8 billion acquisition); *Health Net Federal Services*, 2009 CPD § 220 ($16 billion protest litigation); *Wynne v. UTC*, 463 F.3d 1261 (Fed. Cir. 2006) ($299 million defective pricing trial/appeal). He authored the *Defective Pricing Handbook* (Thomson West, 2014–15 ed.) and regularly lectures on government contracting, pricing, and fraud matters.

Nationally recognized by Chambers USA in Government Contracts as "a leading lawyer within the cybersecurity space," he advises and trains Fortune 500 companies on cyberlaw and security (NIST standards, cloud, FedRAMP, APT breaches, network audits, and cyber disputes), handles protest litigation on cyber issues, testifies before Congress on cybersecurity, teaches cybercontracting for Federal Publications, and publishes extensively. He currently serves as ABA SciTech Section Secretary; Co-Chair of the Security, Privacy, and Information Law Division; Co-Chair of the Homeland Security Committee; and a member of the Section Council. He also serves as a Public Contract Law Section Committee Co-Chair (Cybersecurity, Privacy, and Data Protection) and as a member of the ABA President's Cybersecurity Legal Task Force.

Section Secretary

**William B. Baker** is a partner in the Potomac Law Group, PLLC, a Washington, DC-based law firm. He has practiced for more than 30 years in the areas of communications, technology, and postal law, with particular interest in privacy, information law, and marketing communications. He is a frequent author and lecturer on privacy and postal matters. He previously practiced for more than 30 years in the Washington, DC, law firm Wiley Rein LLP.

Bill has served as Budget Officer of the Section of Science & Technology Law since 2012 and as Assistant Budget Officer prior to that. He has served on the Section's Council since 2008. He has chaired or co-chaired several Section committees, including the committee on Telecommunications and Information Services from 1998–2002, the ePrivacy Law Committee from 2003–2008, and the Data Property Rights Committee since 2013. He is a Fellow of the American Bar Foundation.

He has written numerous articles on privacy and technology issues, contributed to several Section publications, and served as a moderator or panelist on a number of Section programs. Bill chaired the Government Affairs Committee of the Northern Virginia Technology Council from 2001–2005 and served on Advisory Committees to the Virginia General Assembly's Joint Commission on Technology and Science from 1997–2005.

Bill holds a bachelor of arts degree in economics, and a juris doctor degree, both from the University of Virginia. He lives in Arlington, Virginia.

Section Budget Officer

**Garth B. Jacobson** serves as a Senior Government Relations Attorney for CT Corporation. Previous positions include working as an attorney at Preston Gates and Ellis LLP and chief legal counsel to the Montana Secretary of State. As chief legal counsel, he successfully litigated election law cases before the state trial and appellant courts and federal courts. During that tenure, he also served on the state bar committees that drafted business entity legislation including profit and nonprofit corporate acts, revisions to the partnership laws, and the limited liability company act. Additionally, he developed and administered alternative dispute resolution of business name infringements. He served on the Montana Ethics Advisory Commission, on the Board of Trustees of the State Bar of Montana, and as president of the First Judicial District Bar Association.

Garth served as an observer/advisor to various Uniform Laws Commission business entity drafting committees. Currently he participates as an "observer" on the Series LLC drafting committee and the ABA advisor on the Wage Garnishment Committee. He is a member of the ABA Business Law and the Science & Technology Law sections where he serves as co-chair on both ULC Committee and E-filing Committee and LLC Committee subcommittee chair. Garth also serves as SciTech's Assistant Budget Officer. He coauthored an article, "Electronic Service of Process," published in the Spring 2008 *SciTech Lawyer*.

Garth has many years' experience with legal education as a presenter, organizer, or moderator of numerous continuing legal education (CLE) programs. He conducted programs on a variety of topics, including tax law, corporations, LLCs, UCC, service of process, and legal ethics. He also taught business law classes at Carroll College as an adjunct professor, in Helena, Montana.

Garth received a bachelor of arts degree in economics and philosophy, a juris doctorate and a master's degree in public administration from the University of Montana. Additionally, he holds an LLM in Taxation from the University of Washington. He is a member the bar in Washington and Montana. The Counsel of State Governments named him a Toll Fellow. This prestigious national award recognizes outstanding leadership and service in state government.

Garth enjoys rock, alpine, and ice climbing. His climbing resume includes summits of Mt. Rainier, Mt. Hood, Mt. Adams, Mt. Baker, Castleton Tower, and the Snake Dike route on Half Dome, Yosemite. He is a member of the Seattle Mountaineers' climbing program. Additionally, he often creates pottery at Pottery Northwest, where he completed a 10-year term on its board of directors.

### Section Delegate to the ABA House of Delegates

**Bonnie Fought** was a founder and member of the executive team of Connectix Corporation for more than 15 years and served as its chief financial officer, general counsel, and later chief operating officer. Connectix designed, manufactured, and marketed an array of computer software and hardware products. After licensing and selling various technologies, Connectix's primary technology was sold to Microsoft Corporation in 2003.

For the past six years, Bonnie has served as the Section Delegate in the House of Delegates for the Section of Science & Technology Law. In addition, Bonnie is a Past Chair of the ABA Section of Science & Technology Law. She served as the Chair of its Book Publishing Board for three years and as the Section's Budget Officer for three years. Bonnie also served as a member of the ABA's Standing Committee on Technology and Information Systems from 1999–2002, the Standing Committee on Publishing Oversight from 2011–2014 and currently serves on Standing Committee on Continuing Legal Education. Bonnie also serves as the Co-Chair of the SOC Decennial Governance Review Committee.

Bonnie has a J.D from the University of California at Berkeley (Boalt Hall) and was admitted to the California State Bar in 1990.

### Section Council

**Katherine E. Lewis** has worked as an attorney-advisor at the Smithsonian Institution's Office of Contracting since 2012. Prior to working with the Smithsonian, Katherine had a private practice in New York working with solo practitioners, small firms, and large firms on e-discovery matters in addition to representing clients in a variety of practice areas, including copyright and trademark law. Katherine is an active member of the ABA Section of Science & Technology Law. She has been Chair of the Museums and Arts Committee since 2013 and also serves as Vice-Chair of the Program Committee. Katherine was recently recognized as a Rising Star in the Winter 2015 edition of *The SciTech Lawyer*. She previously served as Vice-Chair of the Museums and the Arts Committee and member of the FY2015 Nominating Committee. She is a frequent speaker and guest lecturer and has published articles and essays on matters related to intellectual property, social media, and information technology. Katherine earned her J.D. and LL.M in intellectual property law from the University of New Hampshire School of Law and is licensed to practice in New York, Massachusetts, New Hampshire, and Washington, DC. She earned a bachelor of arts in art history at the University of Connecticut.

**Lisa R. Lifshitz** is head of Torkin Manes's Technology, Privacy and Data Management Group and a partner in the Business Law Group. She has extensive expertise in preparing and negotiating technology licenses and agreements, including software license, cloud computing, system acquisition and Internet/e-commerce/m-commerce-related contracts. She advises on compliance with Canadian federal and provincial private sector privacy legislation and data management issues. Lisa also provides export control and open source advice on cross-border deals. She has considerable experience helping non-Canadian companies, especially American entities, create appropriate legal agreements for their entry into the Canadian marketplace. Lisa is currently the President of the Canadian IT Association, Canada's national technology law association; Chair of the ABA Business Law Section's Technology Committee; and is a member of the ABA Standing Committee on Technology and Information Systems. Lisa is also on the editorial boards of the ABA's *Business Law Today* and *The SciTech Lawyer*. Lisa is a member of the Section of Science & Technology Law (SciTech) Membership and Diversity Committee and serves as SciTech's Liaison to the Business Law Section. Lisa is a prolific speaker and writer and is the author of the monthly technology column, "IT Girl," for *Canadian Lawyer* magazine. Ranked as a recommended lawyer in Computer & IT Law and Technology Transactions in *The Canadian Legal Lexpert Directory* since 2005, Lisa is also recommended for information technology in *Chambers Global 2015*; recognized by *Best Lawyers in Canada 2015* for Technology Law; as a leading Internet & e-commerce lawyer by *Who's Who Legal: Canada* and *The International Who's Who of Business Lawyers*. In her spare time she sings (badly) in a community choir and loves to travel to remote venues.

**Joe Pennell** is a senior associate in the Business & Technology Sourcing practice in Mayer Brown's Chicago office. Joe focuses his practice on information technology and managed services transactions, including cloud computing, software licensing and development, and the outsourcing of finance and accounting services, IT infrastructure services and support, managed network services, and application development and maintenance. He is a Co-Chair of the ABA Section of Science & Technology Law's Cloud Computing Committee. Joe was recently recognized as a Rising Star in the Winter 2015 edition of *The SciTech Lawyer*. He graduated from Harvard Law School in 2008 and earned his undergraduate degree in electrical engineering (with high honors) from Michigan State University.

BOOK REVIEW

# *PREDATOR: THE SECRET ORIGINS OF THE DRONE REVOLUTION*

BY RICHARD WHITTLE

## Reviewed by Casey Civiello

The date is September 4, 2001, less than a year after the suicide attack on the *USS Cole* in the Yemeni port of Aden. President George W. Bush is holding his first National Security Council Principals Committee meeting since his election. Just prior, the top counterterrorism official at the time, Richard Clarke, directs a note to then-National Security Advisor Condoleezza Rice pleading to extend drone usage beyond mere intelligence gathering by arming the aircraft. Clarke alludes to a feared (and, as we now know, actual) imminent al-Qaeda attack on American lives, warning: "What would those decision makers wish that they had done earlier? That future day could happen at any time" (page 226).

On multiple occasions in the preceding year, Predator unmanned aerial systems, (UASs, or more colloquially, "drones") had silently stalked and captured footage of Osama bin Laden, who was on the verge of becoming an infamous household name. In the months prior the 9/11 attacks, members of "Big Safari," a quasi-secret United States Air Force group of engineers, had scrambled to weaponize the drone with laser-guided Hellfire missiles, and Clarke was determined to cut through bureaucracy and gain authority and guidelines for use of these missiles to kill terrorist threats. The technology remained an afterthought by hardened military officials, viewed as more gimmick than as a functional tool. Pilots directed to Indian Springs, Nevada, to remotely fly the early Predator view the assignment as punishment, sarcastically referring to it as "life at One G." But after 9/11, a new attitude emerged.

In *Predator*, Richard Whittle invites the reader behind the curtain of secrecy surrounding the drone warfare program. He traces the documents and influential players in the struggle to capture funding and implement drone technology, juxtaposed against the rise of al-Qaeda in the Middle East. The account of events humanizes the creation of a silent stalker; balancing a sequential story with technical jargon among a colorful cast of engineers, government officials, and political fixers who together transformed the Predator from a military afterthought to perhaps the world's most valuable intelligence gathering and fear-inducing active weapon, capable of silently stalking and destroying targets anywhere on earth.

As with any good story, the truth lies not only in the composite materials and feats of engineering but in the characters who bring the technology to life. Whittle takes the reader to 1973, the end of the Yom Kippur War between Israel and an Arab coalition led by Egypt and Syria. Abe Karem, an Israeli engineer who had risen to be chief designer with the government-owned Israel Aircraft Industries, was issued a challenge to rapidly create a decoy that could be released from a fighter jet to fool the Arabs' Soviet-built surface-to-air missile radar systems, which had served as a formidable counter to the powerful Israeli Air Force.

Though undistinguished in its military application, the decoy created was functional within two weeks and inspired Karem to recognize the future of unmanned flight. This occurrence pushed him to start Leading Systems, Inc. in his garage some years later, after relocating to California. The lightweight, broad-wing aircraft dubbed the "Amber" would later evolve to become the physical platform for General Atomics to create the present-day Predator.

Whittle observes that "Necessity is the mother of invention, and war [is] the mother of necessity" (page 293). Demand for development of the Predator increased during the conflict in the former Yugoslavia, where frustration reigned over lack of intelligence about movement of Serbian artillery targeting civilians in Bosnia. Early versions of the Predator flew over the region in 1995 with mixed success. One Predator was shot down by the Serbian military, while another crashed as a result of engine failure. The real-time information gathered amazed military commanders. But, due to lack of clearly defined leadership and disputes between the Navy, Army, Air Force, and CIA, targeted development of the Predator project was effectively handcuffed until the Air Force assumed full control of the program in October 1997.

Thereafter, advancements sped along, largely due to Big Safari, headquartered at Wright-Patterson Air Force Base in Dayton, Ohio. Development was guided by philosophies such as "modify, don't develop" and "provide the necessary, not the nice

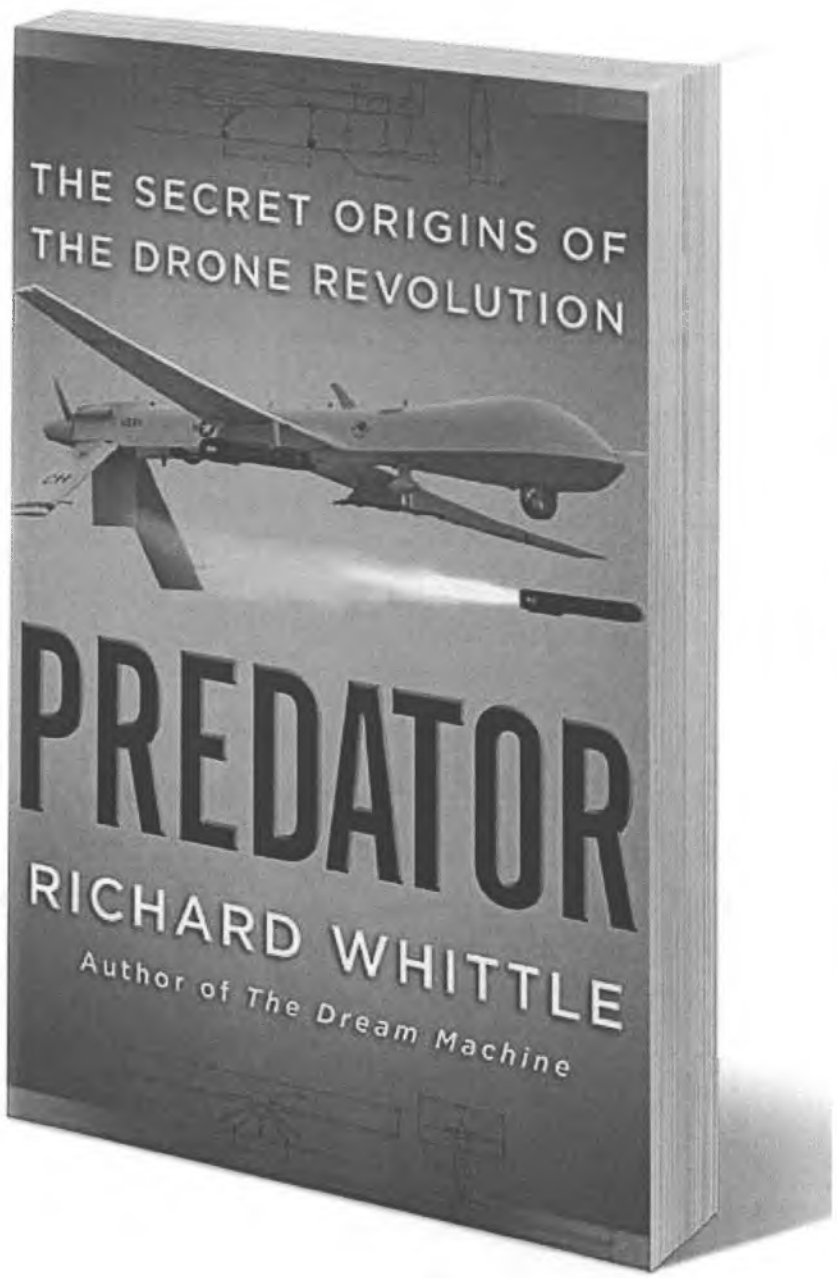
*Casey Civiello is an associate in the Boston, MA, law firm of Henshon Klein LLP. His practice covers a broad range of business and real estate transactions, with a particular focus on assisting early stage start-ups. He can be reached at cciviello@henshon.com.*

to have." The Big Safari team and their supporting advocates inside the government are painted by Whittle as a group of gunslingers who efficiently carry the Predator project from successful experiment into modern-day prevalence, applying innovative ideas (streaming video, multiple-point flight control) to existing military hardware. The culmination of Big Safari innovation efforts resulted in a joint CIA-Air Force team tracking down and killing al-Qaeda military chief Muhammed Atef near Kabul, Afghanistan, in the weeks following 9/11.

Although it is possible to get lost at times in the alphabet soup of government programs, call-names, and plane designations, Whittle gives the reader confident insight into how the innovators were able to cut through red tape, draw resources, and complete a secret project under intense pressure and timelines. In truth, the sometimes confusing roster of players tied to the creation of the Predator may play as a parallel to the complexity of government contracting and development itself. Perhaps the hesitance displayed through bureaucracy is a necessary check on technological development that seems to be outpacing the balancing moral review.

*Predator* successfully lifts the veil of secrecy shrouding perhaps the most influential military innovation of a generation, but Whittle passes on the opportunity to analyze the ethical questions surrounding the Predator. References in the book to collateral damage are sterile, though likely an accurate representation of the feelings of those individuals affiliated with creating and operating the Predator. The book's excitement-inducing narrative tempts the reader to accept impolitic portrayals of casualties of war, such as referring to human bodies blown from a Hellfire blast as "flippers," or to those crawling from the scene as "squirters." Instead, the invitation (to the reader) could be for a more thorough reflection on the long-term impacts of remote-controlled warfare. What are the moral hazards of dehumanizing casualties? What role do anonymous strikes and collateral damage play in advancing the radicalization of Islam? What are the legal and foreign policy implications of this "video game" warfare?

Whittle perhaps recognizes the limitations of his book when near the end he posits, "When automobiles replaced horses, traffic laws and stoplights were needed" (page 305). The military development of unmanned aerial vehicles has quickly skipped to the consumer market and sparked huge popularity of drones for personal and commercial applications. This expansion further stretches the need for timely thought and action with respect to the role that innovators and lawmakers alike will have in shaping the future of drone usage. ◆



# Make Connections That Matter at the ABA Annual Meeting: Sweet Home Chicago

By Ruth Hill Bro

In a 24/7 world humming on mobile technology, it's easy to forget that coming together face-to-face, in person, is the best way to make the connections that matter most. Although *distance* learning, *remote* connections, and *virtual* meetings are essential, they seem so far away and never quite as good as the real thing. In fact, one definition of "virtual" is that it is "*almost* or *nearly* as described, *but not completely*."

That's why most leading businesses recognize a key concept backed up by mounting data from biologists, computer scientists, and psychologists: no matter how well we communicate electronically, it's vital to come together in person. Two *Forbes* articles by Susan Adams, called "Being There" and "Why We Need to Meet in Person," discussed such data and noted, "Meeting face to face does three things better than virtual meetings. It captures trust, it inspires positive emotions, and it builds relationships."

If you doubt it, consider the many things you do more effectively in person: (1) going home for the holidays, relaxing with friends, and celebrating milestones; and (2) building relationships with clients and prospects, conducting job interviews, meeting potential employers and future colleagues, and expanding your network of peers and mentors. The list is endless. No matter what our personal life is like or our job setting is, *we're all in the people business.*

However much you get from your SciTech membership, you could be getting even more of that *SciTech Edge* if you visit your home Section at the ABA Annual Meeting. From July 30th through August 4, 2015, the American Bar Association will meet in Chicago, home to ABA headquarters, renowned architecture, high-profile professional sports teams, Lollapalooza and other top music venues, beautiful Lake Michigan, the Cloud Gate sculpture and Millennium Park, and the Art Institute (site of the 2015 ABA President's Reception) and other internationally acclaimed museums.

Join SciTech at the Annual Meeting to make the connections that matter most: at the SciTech Luncheon (with a top-notch speaker), the SciTech Reception (this year focused on diversity and inclusion and cohosted by the ABA Intellectual Property Law Section), SciTech and ABA CLE programs (meet the speakers), SciTech committee meetings on hot topics (explore ways to contribute and raise your profile), the ABA General Assembly (featuring a keynote address from a US Supreme Court Justice or other prominent legal figure), the ABA Expo (with a Grisham-esque authors panel on "The Law as a Platform for Writing"), etc. You'll also find:

- Meaningful ways to interact with other forward-thinking practitioners (find the answers you need now and colleagues and mentors for years to come).
- Indispensable resources and perspectives that make your work life easier.
- Opportunities to get involved, share insights, and shape law and policy on issues that are not only important, but also important to get right.
- So much more. Register and explore your options at ambar.org/scitech and ambar.org/annual. (Law students: for only $50, you can access 150+ CLE programs, dozens of committee/governance meetings, the General Assembly, and Expo.)

We hope you'll join us every year for the Annual Meeting, but especially this year in Chicago, whether you know it as Sweet Home Chicago (a la the Blues Brothers), my kind of town (a la Frank Sinatra), the Windy City (politics, and literally the wind), or the City of the Big Shoulders (a la poet Carl Sandburg). By standing on those shoulders, you'll see farther and make more of the connections that matter to you. ◆

*Ruth Hill Bro, privacy attorney, speaker, and author (Chicago), chairs the Membership and Diversity (MAD) Committee of the ABA Section of Science & Technology Law and served as the 2008–09 Section Chair. She can be reached at ruth.hill.bro@gmail.com.*
*"It's a MAD World: Membership and Diversity, with a SciTech Edge," is a column designed to spotlight membership and diversity-related topics, resources, and opportunities for SciTech members.*

ABOVE: Pepper has the SciTech Edge. Wouldn't you like to be a Pepper, too?

ABOVE: 2015 ABA Midyear Meeting (Houston); All of these SciTech leaders want to see you in Chicago.



ABOVE: Ruth Hill Bro introducing SciTech Luncheon speaker Chris Kelly, then Facebook Chief Privacy Officer, General Counsel, and Head of Global Public Policy, 2007 ABA Annual Meeting (San Francisco).


LEFT: SciTech CLE panel, "Need-to-Know Information from the Women of Cybersecurity," selected to be part of the Commission on Women in the Legal Profession's Day of the Woman, 2013 ABA Annual Meeting (San Francisco).

LEFT: Speakers with SciTech mobile devices after their panel on "The Mobile Transformation: The Extraordinary Legal Implications of Billions of Mobile Devices," SciTech CLE program, 2013 ABA Annual Meeting (San Francisco).

ABOVE: Section Chairs celebrating SciTech's 35th anniversary, 2009 ABA Annual Meeting (Chicago), SciTech Reception.

Section of Science & Technology Law
American Bar Association
321 North Clark Street
Chicago, Illinois 60654-7598
PC54580001104

Nonprofit
Organization
U.S. Postage
PAID
American Bar
Association

WINNER
2014
APEX®
AWARDS FOR
PUBLICATION EXCELLENCE

CONNECTWITHSCITECH

#SCITECH

## Each year, thousands of members count on SciTech to put the tools they need at their fingertips to navigate rapidly changing science and technology law issues:

**THREE INFORMATION-PACKED PERIODICALS:**

- *The SciTech Lawyer*, our glossy quarterly magazine with cutting-edge coverage
- *SciTech e-Merging News*, our quarterly electronic newsletter with timely practice perspectives and Section activities/opportunities
- *Jurimetrics*, our quarterly electronic law review published by the Section and the Center for Law, Science & Innovation of the Sandra Day O'Connor College of Law at Arizona State University

---

- Unlimited access to over 20 free hot-topic committees and list serves
- Free access to Section articles via the SciTech e-Archive and ABA Web Store
- Members-only discounts on Section books (save 10% or more) and CLE programs (save $100 off the public rate, $50 off the ABA rate)
- Exclusive career and business development resources
- Free access to our podcast archive on emerging issues
- Four selected chapters from preeminent SciTech books (delivered electronically) and access to chapter archive
- Two free webinars/teleconferences: one practice-focused and one on a hot substantive topic (notices sent electronically)
- Limited-time special offers

# CALENDAROFEVENTS

June 22, 2015
**Understand Drones: State and Federal Privacy and Safety Regulation**
CLE Webinar

June 24, 2015
**Flying Under the Radar Screen: Aviation, Psychology, and Fitness for Duty**
CLE Teleconference

July 30–August 1
**ABA Annual Meeting**
Chicago, IL

August 25, 2015
**Understand How to Overcome Implicit Bias and Other Cognitive Bias to Be Better Lawyer**
CLE Webinar

September 9, 2015
**Lawyer Interrupted: Ethics and Workplace Distractions**
CLE Webinar

September 22, 2015
**Privacy, Probate, and What Happens to Your Digital Data After You Die**
CLE Webinar