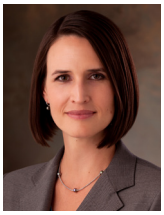
Space Law Perspective
Summer 2015

HOLLAND&HART LLP



Janna J. Lewis
719.475.6489
jjlewis@hollandhart.com

Janna J. Lewis is a registered U.S. patent attorney and a member of Holland & Hart's Intellectual Property and Government Contracts groups. 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.

Lauren R. Caplan
202.654.6919
lrcaplan@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 subcontract.

Drones to Satellites: Should Commercial Aerial Data Collection Regulations Differ by Altitude?

by **Janna J. Lewis** and **Lauren R. Caplan**

The news and social media commentary of late reveals considerable discomfort with the idea that "drones," or Unmanned Aircraft Systems (UAS), could be used to collect images and data for commercial purposes. The idea that a flying machine —say, a 6-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 non-commercial 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 smart phone 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.[7] 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 U.S. 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,[8] and an increasing number of states have proposed legislation to govern commercial drone use within state borders.[9] The federal agencies that regulate aspects of commercial satellites use include the National Oceanic and Atmospheric Administration (NOAA)[10] 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,[16] the U.S. 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.[17] 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 aligned 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,[18] 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 U.S. private remote sensing space systems,[19] can require specific and enforceable limitations on operational performance of commercial satellites, which can include limitations on data collection and dissemination.[20] Private satellite operators must submit a Data Protection Plan (DPP) as part of their license application to NOAA.[21] 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 and advancements in technology.[22] 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.[23]

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.[24]

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.

End Notes

[1]*See, e.g.,* UAS Privacy Considerations, The Aerospace States Association, *availible 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 U.S. 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 U.S.—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 U.S. 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?"