

Morrison & Foerster Client Alert

April 16, 2014

Next Generation State Privacy Law: Regulating the Commercial Use of Drones

By Nathan D. Taylor

When most Americans think of drones, they think of unmanned, often weaponized aircraft that are used by governments in areas of conflict for intelligence or combat purposes. However, the proverbial sky is the limit on the potential commercial use of drones. For example, in a December 2013 *60 Minutes* interview, Jeff Bezos, the founder of Amazon.com, described his company's efforts to develop GPS-programmed, autonomous drones (or in his words, "octocopters") to serve as "delivery vehicles" to provide half-hour delivery of your future Amazon order. Although there will be hurdles to the widespread commercial adoption of drones as the Federal Aviation Administration works out the regulatory issues surrounding the licensing and use of drones in our airspace, our not-too-distant future could involve a world in which drones are literally buzzing above our heads.

Drones are, among other things, unmanned, light, easy to deploy and relatively cheap. As a result, companies could use drones for numerous purposes, including scientific research and exploration, monitoring livestock or gas pipelines, remote troubleshooting of technology, finding lost shipments or even as a substitute for the Super Bowl blimp. Because of advances in camera, video and audio technology (and the decreasing cost of that technology), however, drones could also be used to collect and communicate massive amounts of information about individuals and their everyday lives. Imagine a company taking its drones out for a spin on a Saturday morning in your town to conduct market research, observing how the average person mows the lawn, when the average person goes to grab coffee or how many bags of groceries the average person leaves with from the supermarket. Or, imagine a company flying a drone around its factory or retail location to monitor when its employees go on break or what end-caps its customers gravitate to or avoid. As is true with many new technologies, drones raise complex and often troubling privacy issues (remember your first cell phone...it didn't have a camera or location services, right?).

In fact, it's safe to say that many Americans would view the commercial use of drones with suspicion. Consistent with those suspicions, state legislatures have begun scratching the surface on some of the privacy implications of drones. Over the past two years, legislatures in almost every state have considered some form of legislation. As of today, at least twelve states have enacted laws regulating the

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Sotirios Petrovas	(212) 336-4377
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

Patrick Bernhardt	(202) 887-8771
L. Richard Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
D. Reed Freeman, Jr.	(202) 887-6948
Julie O'Neill	(202) 887-8764
Obrea O. Poindexter	(202) 887-8741
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Berlin

Hanno Timmer	49 30 72622-1346
--------------	------------------

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808
------------------	---------------

Singapore

Daniel P. Levison	65 6922 2041
-------------------	--------------

Tokyo

Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

Client Alert

use or licensing of drones. Many of these laws are focused on limiting government and law enforcement activities. See, e.g., the Florida Freedom from Unwarranted Surveillance Act, Fla. Stat. § 934.50; the Illinois Freedom from Drone Surveillance Act, 725 Ill. Comp. Stat. §§ 167/1–167/35. Other laws have a more unique focus, including an Illinois law criminalizing a person from committing “hunter or fisherman interference” by knowingly “us[ing] a drone in a way that interferes with another person’s lawful taking of wildlife or aquatic life.” 720 Ill. Comp. Stat. § 4/48-3.

However, several new state “drone” laws are clearly intended to address privacy concerns beyond those raised in government and law enforcement contexts, and could impose limitations on a company getting drones off the ground for commercial purposes. For example, an Idaho law, effective July 1, 2013, prohibits any person from using a drone “to intentionally conduct surveillance of . . . or collect information about, or photographically or electronically record specifically targeted persons or specifically targeted private property.” Idaho Code § 21-213(2)(a). In fact, the Idaho law would require that a company first obtain an individual’s written consent to use a drone to collect information about an individual or that individual’s dwelling. Idaho Code § 21-213(2)(a)(i). The Idaho law also imposes a written consent requirement for the public dissemination of any photograph or recording of an individual obtained by a drone. Idaho Code § 21-213(2)(a).

Similarly, a Texas law, effective September 1, 2013, criminalizes and creates a private right of action for the use of a drone “to capture an image of an individual or privately owned real property . . . with the intent to conduct surveillance on the individual or property” or to possess, disclose or otherwise use such images. Tex. Gov’t Code §§ 423.003, 423.004. Although the Texas law includes nearly 20 exceptions to this broad prohibition, including permitting the collection of images with the consent of the individual who owns or lawfully occupies the real property captured in the image, these exceptions are largely limited to government, law enforcement and energy-related purposes. See Tex. Gov’t Code § 423.002.

In addition, an Oregon law provides a private right of action for any person who owns or lawfully occupies real property against a person that “operates a drone . . . flown at a height of less than 400 feet over the property if” that operator has previously flown a drone over the property at a similar low altitude and the owner/occupant of the property notified the operator that she “did not want the drone flown over the property at a height of less than 400 feet.” Ore. Rev. Stat. § 837.380. That is, the Oregon law essentially creates a low-flying drone “opt out,” if you will.

IMPLICATIONS FOR BUSINESS

As state legislatures continue to grapple with the privacy implications of drones, it is safe to say that the Idaho, Texas and Oregon laws will not be the last state laws that impose privacy requirements or limitations that would apply to the commercial use of drones. As with the underlying technology, this will continue to be a rapidly changing legal front. Because drones have not yet been adopted in this country for commercial purposes in any meaningful way, your company likely has not begun considering how it could use drones in the future in its day-to-day operations. However, as noted above, the proverbial sky is the limit. Inevitably, many companies will consider whether they have any viable use of drones. If you are asked about the legal implications to your company, it will be critical to be mindful of potentially applicable state limitations. Moreover, you will have to revisit and consider any privacy policies or other public statements your company has made regarding if, when and how the company collects information about consumers and how it uses and discloses that information.

Client Alert

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "[*Global Employee Privacy and Data Security Law*](#)," or our free online Privacy Library, please visit: <http://www.mofo.com/privacy--data-security-services/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.