



NICOLLE LAFOSSE
Of Counsel, Diaz Reus

WHO IS WATCHING THE DRONE? PRIVACY, SECURITY, AND LIABILITY IN AN ERA OF AUTONOMOUS FLIGHT

This conversation explores the key legal challenges arising from the growing use of drones, from privacy and data protection to security, surveillance, and liability for potential damages.

As this technology becomes increasingly integrated into business operations, understanding its legal implications is essential for companies, operators, and users.



Who Is Watching the Drone? Privacy, Security, and Liability in an Era of Autonomous Flight

By Diaz Reus International Law Firm

Drones are no longer confined to recreational photography or specialized aviation. They are increasingly being deployed for security, surveillance, infrastructure inspections, agriculture, real estate, logistics, and other commercial applications.

Their expanding capabilities, particularly when combined with artificial intelligence and autonomous systems, are creating a more difficult legal question: the fact that a drone can observe, record, collect information, or make operational decisions does not necessarily mean that every use of those capabilities is legally permissible.

In a recent Diaz Reus conversation, Nicole Lafosse, an international attorney focused on emerging technologies, examined the evolving legal landscape surrounding drones and the intersection of aviation regulation, privacy, data protection, cybersecurity, and liability.

Her analysis highlights a fundamental challenge for businesses: regulating the flight itself is only one part of the equation. Organizations must also consider what a drone captures, how that information is used, who controls the technology, and who may ultimately be responsible when something goes wrong.

Drones Present a Different Regulatory Challenge

Unlike some emerging technologies, drones already operate within an established aviation framework. In the United States, the Federal Aviation Administration (FAA) regulates the national airspace and establishes rules governing drone operations.

But having an identifiable aviation regulator does not eliminate legal uncertainty.

As Lafosse explained during the conversation, some of the most significant unresolved issues surrounding drones fall into five broad categories: privacy, liability for autonomous operations, federal-state-local jurisdictional tensions, counter-drone authority, and supply-chain and data security.

This fragmentation matters because a single drone operation may implicate several different areas of law.

The FAA may regulate whether and how an aircraft can operate in the airspace, while other federal or state authorities may become relevant when the same drone records individuals, collects location information, monitors employees, causes property damage, or processes personal information.

For companies, therefore, regulatory compliance cannot end with permission to fly.

The Drone May Be Regulated Differently From the Data It Collects

One of the most important distinctions discussed during the interview was between regulating the aircraft and regulating the information captured by the aircraft.

A drone may collect video, photographs, audio, geolocation information, vehicle license plates, and potentially other identifiable information. When those datasets are combined with technologies such as facial recognition or external databases, seemingly ordinary footage can become significantly more revealing.

Lafosse illustrated this distinction by comparing a single image of someone walking on a public sidewalk with a sequence of recordings showing that person entering a vehicle, leaving a residence, and moving through identifiable locations. Individually, those images may reveal relatively little. Collectively, however, they may create a detailed picture of a person's activities and routines.

That distinction is particularly important as drones become more sophisticated.

The legal question may no longer be limited to whether an individual was visible from a public location. Businesses may also need to ask what information was collected, whether individuals can be identified, whether geolocation or audio was captured, how long the information will be retained, whether it will be combined with other datasets, and what the organization ultimately intends to do with it.

Capturing Information and Using It Are Not the Same Thing

Another important issue is the distinction between incidental collection and subsequent use.

Commercial drones conducting inspections, mapping, security, or logistics operations may unintentionally capture neighboring properties or individuals who were not the intended subjects of the operation.

According to Lafosse, the purpose and subsequent use of that information become central considerations. An organization that incidentally records information may face a different legal analysis from one that deliberately stores, analyzes, combines, or repurposes that information. At the same time, claiming that collection was accidental does not automatically resolve the issue; intent itself may be difficult to establish.

For companies, this suggests that drone governance should address the entire data lifecycle, rather than merely flight operations.

Organizations should understand why information is being collected, what categories of data may be captured, who can access it, how it will be used, how long it will be retained, and when it should be deleted.

When a Drone Causes Harm, Liability Can Become a Chain

Liability becomes even more complicated when a drone causes physical injury, damages property, or improperly collects or uses information.

The natural question is: Who is responsible?

The pilot? The owner? The company deploying the drone? The manufacturer? The software developer?

Lafosse's answer was that liability may potentially involve multiple participants, depending on the nature and cause of the harm.

Different actors may have different responsibilities. One may be responsible for aviation compliance, another for operational decisions, another for defective equipment, and another for the collection or misuse of data. In significant incidents, this can produce a chain of potential responsibility that must be reconstructed through evidence and legal analysis.

For businesses, this makes contractual allocation of risk particularly important when drone operations involve third-party pilots, technology vendors, software providers, maintenance contractors, or data-processing companies.

Autonomous Drones Complicate Traditional Liability Rules

Artificial intelligence introduces an even more difficult question.

Traditional negligence law frequently evaluates conduct by asking what a reasonable person would have done under comparable circumstances. Autonomous drones complicate that framework because an algorithm may make an operational decision without a human pilot controlling the aircraft in real time.

Lafosse identified this as one of the developing gray areas in drone law.

If one individual supervises multiple autonomous aircraft, for example, determining responsibility for a decision made independently by one system may require examining not only the human operator, but also the software, the organization's operating procedures, the level of human oversight, and the circumstances surrounding the incident.

This creates a broader legal challenge shared by many AI-enabled technologies: legal frameworks designed around human decision-making must increasingly account for systems capable of acting with varying degrees of autonomy.

Workplace Surveillance Raises Another Set of Questions

Drones are also increasingly relevant to corporate security and surveillance.

Businesses may use them to monitor facilities, inspect perimeters, protect assets, or observe operational areas. But surveillance can also capture employees and third parties.

Here, Lafosse emphasized several practical considerations: notice, consent, purpose, retention, and the nature of the information being collected.

Organizations should understand why surveillance is necessary, what the drone will record, how the resulting information will be used, how long it will be retained, and whether it constitutes personal information. Expectations of privacy may also differ depending on whether an individual is in a workplace, a private residence, or another environment.

The broader lesson is that replacing a fixed security camera with a mobile aerial platform does not eliminate existing privacy obligations. In some circumstances, mobility and expanded observational capabilities may make governance even more important.

Real Estate, Agriculture, and Other Commercial Uses Carry Their Own Risks

The interview also examined sectors where drones are already becoming routine.

In real estate, aerial photography may inadvertently capture neighboring homes or individuals in areas where they expect privacy. In agriculture, companies must consider operational parameters, flight permissions, location, altitude, and the scope of the activity being performed.

These examples illustrate why a single generic “drone policy” may be insufficient.

The legal risk profile of an agricultural drone used for crop operations is fundamentally different from a drone monitoring employees, photographing a residential property, inspecting industrial infrastructure, or operating autonomously as part of a fleet.

A Better Starting Point: Define the Purpose First

One of Lafosse's most practical recommendations was to approach drone compliance in reverse.

Rather than purchasing or deploying a drone and then determining which rules apply, an organization should first define the intended outcome.

What will the drone do? Where will it operate? What information will it capture? Will it record video or audio? Will it collect geolocation information? Will it operate autonomously? Will the information be stored or analyzed?

Once those questions are answered, the organization can work backward to determine the permissions, limitations, privacy considerations, operational requirements, and internal controls that may apply.

This purpose-driven approach is particularly valuable for businesses because drone risk rarely belongs exclusively to one department. Depending on the operation, legal, compliance, cybersecurity, privacy, insurance, operations, procurement, and information-governance teams may all need to participate.

The Future of Drone Regulation Is Likely to Remain Multi-Layered

The future regulatory framework for drones is unlikely to consist of a single comprehensive rule.

As Lafosse noted, a drone itself combines multiple components and activities: hardware, software, data collection, video, audio, aviation, property rights, and

potentially autonomous decision-making. Different consequences may therefore trigger different legal regimes and different authorities.

That complexity will only increase as drones become more autonomous and increasingly integrated with artificial intelligence and other emerging technologies.

For businesses, waiting for every regulatory uncertainty to disappear is unlikely to be a workable strategy.

The more practical approach is to establish governance before deployment: define the business purpose, understand the data involved, determine applicable operational requirements, establish accountability, evaluate third-party relationships, and maintain records capable of explaining how and why decisions were made.

From Permission to Fly to Permission to Use

The central legal issue surrounding drones is becoming broader than aviation.

A company may be permitted to operate a drone and still face separate questions about privacy, surveillance, data processing, cybersecurity, property rights, or liability.

That distinction is likely to become increasingly important as drones move from individually piloted devices toward interconnected and autonomous systems capable of observing, analyzing, and acting at scale.

The question for businesses, therefore, is no longer simply “Can we fly this drone?”

It is also:

What will it observe? What information will it create? What will we do with that information? Who controls its decisions? And who will be responsible if something goes wrong?

Those are the questions that should be addressed before the aircraft ever leaves the ground.