21ST CENTURY LIABILITY ISSUES: DRONES, CYBER LIABILITY, AND PRIVACY ISSUES

Presented and Prepared by:
Ann C. Barron
abarron@heylroyster.com
Edwardsville, Illinois • 618.656.4646
21ST CENTURY LIABILITY ISSUES:
DRONES, CYBER LIABILITY, AND PRIVACY ISSUES

I. THE DRONES ARE COMING, THE DRONES ARE COMING: AN INTRODUCTION TO REGULATION AND LIABILITY SURROUNDING DRONES ................................................................. M-3

II. FEDERAL REGULATION OF DRONES ................................................................. M-3

III. STATE REGULATION OF DRONES ................................................................. M-6

IV. APPLICATION OF STATE TORT LAW TO DRONES ........................................... M-7

V. CYBER AND PRIVACY LIABILITY: DOES THE PLAINTIFF HAVE STANDING TO PROCEED? ................................................................................................................................. M-8

A. Galaria v. Nationwide Mutual Insurance Company .............................................. M-9
B. In re Adobe Systems Privacy Litigation ............................................................... M-9
C. In re Science Applications International Corp. .................................................. M-10
D. Lewert v. P.F. Chang’s China Bistro, Inc. ............................................................. M-10

The cases and materials presented here are in summary and outline form. To be certain of their applicability and use for specific claims, we recommend the entire opinions and statutes be read and counsel consulted.
Unmanned aerial vehicles (UAV) or unmanned aircraft systems (UAS), more commonly called “drones,” are no longer used only in military or police operations. From Amazon wanting to deliver packages using drones, to firefighters using them to fight forest fires, to small businessmen using them for advertising, to retail estate agents creating property tours, to recording sporting events, to hobbyists using them for photography, drones are all around us. They were routinely advertised as the hottest gift late last year.

Today’s drones are not the old model aircraft from the 1980s which were operated with a large hand held device. Rather, they are operated either by a pilot or an on-board computer. Some basic hobby models of drones can be controlled by a smartphone or tablet. More sophisticated models use GPS coordinates which can be pre-programmed, and have a range of many miles.

Drones may contain still cameras, high definition video cameras, microphones, thermal imaging equipment or atmospheric and data collection equipment. This includes the aircraft itself and all of the associated support equipment, control station, data links, telemetry, communications and navigation equipment necessary to operate the unmanned aircraft.

But what happens when a drone crashes or is used for improper purposes? Who is at fault and can liability be assessed against a drone operator, manufacturer, or owner? The short answer is that improper use of a drone may subject the owner, manufacturer, or operator to federal or state criminal and/or civil liability.

Federal Aviation Administration regulations provide that “[n]o person may operate an aircraft in a careless or reckless manner so as to endanger the life or property of another.” 14 C.F.R. Section 91.13(a). The FAA has historically levied substantial fines on unapproved aircraft operators when there was a violation of Section 91.13(a). A crash of a drone may be a per se violation of this regulation as the FAA has long considered model aircraft, and now drones, as aircraft subject to this section.

Specific federal regulation of the use of model aircraft dates back to the 1980s when drones were a concept in science fiction. Although drones have become more common, federal statutes and regulations have not necessarily kept up.
In 2007, the FAA proclaimed that “no person may operate a UAS in the National Airspace System without specific authority.” Federal Register Notice – Clarification of FAA Policy (http://www.faa.gov/uas/media/frnotice_uas.pdf). This position by the FAA essentially banned all drone usage. The practical result was that someone using a drone for commercial purposes was required to comply with all FAA regulations.

As technology evolved, Congress passed the FAA Modernization and Reform Act of 2012 P.L. 112-095. That Act requires the FAA to issue by September 2015 rules for commercial drone use in the private sector. The Act also included a “Special Rule for Model Aircraft,” which specifically exempts “model aircraft” from the FAA’s reach and regulation if the aircraft is flown strictly for hobby or recreational use and weighs less than 55 pounds.

Troubled by the proliferation of drones in the marketplace, in June 2014, the FAA issued its interpretation of the “Special Rule for Model Aircraft,” stating that (1) all model aircraft are “unmanned aircraft” and thus “aircraft” subject to FAA regulation, and (2) any use of model aircraft by a business or a farm was a “commercial use.” Under this rule and interpretation, any use that is a “commercial use” is banned, even if no money changes hands. The FAA lists the following types of activities as banned:

- receiving money for demonstrating aerobatics with a model aircraft;
- a realtor using model aircraft to photograph a property he is trying to sell and using the photos in the real estate listing;
- a person photographing an event and selling the photos to someone else; and
- determining whether crops grown as part of a commercial farming operation need to be watered.

Interpretation of the Special Rule for Model Aircraft, June 18, 2014.

Similarly, an insurance company using a drone in a disaster situation would be a banned commercial use. Thus, if you fly commercially, without written permission of the FAA, you are violating federal regulations.

Under Section 333 of the Act, the Secretary of Transportation is permitted to issue waivers of the ban on commercial use. This section allows companies or individuals to file a petition seeking a waiver to use a drone commercially. This is the only way which a drone can be used by businesses or local governments. The FAA has been accepting and granting exemptions under Section 333 where the activity does not create a hazard to users of the national airspace system or the public or pose a threat to national security. Petitions are considered on a case by case basis. Most exceptions require a drone:

- weighing less than 55 pounds;
- not exceeding 50 knots of ground speed;
- flying below 400 feet;
- being operated in line of sight; and
• flown by a licensed pilot, generally with a private pilot license as compared to a commercial pilot license.

More recently, the Secretary of Transportation has been granting blanket waivers for drone flights below 200 feet by aircraft weighing less than 55 pounds, operated during daytime hours in the operator’s line of sight.

Finally, on February 23, 2015, the FAA proposed its “Small UAS Rule” in response to the FAA Modernization and Reform Act of 2012. The proposed rule follows the Section 333 waiver criteria, with the exception of relaxing the licensed pilot requirement and requiring vetting, testing and inspections of the UAS. The operator is required to be 17 years old and pass an aeronautical knowledge test. The proposed rule allows for the use of drones for commercial purposes only in the daylight hours at not more than 100 miles per hour. In addition, the line of sight requirement was not continuous, thereby potentially imposing significant limitations on commercial usage. The line of sight requirement further precludes the use of vision enhancing devices such as binoculars and night vision goggles.

The FAA has also issued the following safety guidelines with respect to model aircraft:

• if there is a risk of collision, the operator must be the first to maneuver away;
• the operator must stop the flight when continuing would pose a hazard to other aircraft, people or property;
• the operator must assess the weather, airspace restrictions and the location of people to lessen risks;
• the drone cannot fly over people except for those directly involved in the flight; and
• operators must stay out of airport flight paths and restricted airspace.

At the time of writing, the FAA is seeking comments on the proposed Small UAS Rule. The FAA has admitted, though, that it will not likely meet the September 2015 mandate for the rule.

In addition, the proposed “Small UAS Rule” does not address privacy or liability concerns, apparently leaving those to State regulation (see infra). As a result a “Drone Aircraft and Privacy Transparency Act of 2015” was introduced in Congress in March 2015. H.R. 1229. This proposed act directs the Secretary of Transportation to study and identify any threats to privacy protections posed by the integration of drones into the national airspace system. The bill would require businesses and individuals using drones to file with the FAA a statement of if the drone will be used to gather data, whether that data will be shared with third parties and how long the data will be retained. The bill would also require the FAA to provide a public database with this information. The bill would prohibit the government from using a drone for law enforcement or intelligence purposes without a warrant. Finally, the proposal would create a private right of action in any state or U.S. District Court for persons injured by a prohibited act.
III. STATE REGULATION OF DRONES

The FAA has acknowledged that it will rely on local law enforcement to investigate activity which is non-compliant with its regulations. But, in February 2015, a head FAA regulator discouraged states from regulating the use of drones suggesting that such action could disrupt a unified regulatory structure. There is sure to be a battle regarding primary jurisdiction and preemption between the federal government and the states and in civil litigation.

In the interim, however, several states have adopted laws regarding the use of drones.

Illinois adopted the Freedom from Drone Surveillance Act effective June 1, 2014. 725 ILCS 167/1, et seq. This Act provides that law enforcement cannot use a drone except in the following circumstances:

- to counter a high risk of a terrorist attack;
- where law enforcement has obtained a search warrant;
- where law enforcement possesses reasonable suspicion that swift action is needed to prevent imminent harm to life or to forestall the destruction of evidence;
- to locate a missing person;
- for crime scene and traffic scene photography;
- where consent to search is given; and
- during a disaster or public health emergency including during response efforts.

725 ILCS 167/10 and 725 ILCS 167/15. A “drone” is defined as any aerial vehicle that does not carry a human operator. 725 ILCS 167/5.

The Act provides that all information obtained via the use of a drone must be destroyed within 30 days unless reasonable suspicion exists that the information contains evidence of criminal activity or the information is relevant to an ongoing investigation or pending criminal trial. 725 ILCS 167/20. If law enforcement uses a drone, the agency shall not disclose any information gathered by the drone, unless the disclosure is to another government agency and there is a reasonable suspicion of criminal activity or the information is relevant to an ongoing investigation or pending criminal trial. 725 ILCS 167/25. In addition, a law enforcement agency cannot use information gathered by a third party who uses a drone, although nothing precludes the third party from providing that information to law enforcement. 725 ILCS 167/40.

If a law enforcement agency owns one or more drones it must report the number of drones it owns. 725 ILCS 167/35. By July 1 of each year, the Illinois Criminal Justice Information Authority must publish a report stating what agencies own drones. Id.

Illinois has also amended the Wildlife Code in response to reports that PETA was going to use drones to interfere with hunting or capture images of individuals violating hunting laws. The Wildlife Code now provides that a person commits hunter or fisherman interference when he intentionally or knowingly “uses a drone in a way that interferes with another person’s lawful
taking of wildlife or aquatic life.” 720 ILCS 5/48-3(b)(10). A drone is defined as any aerial vehicle that does not carry a human operator. Id.

Other states have passed even more stringent laws than Illinois, focusing largely on the privacy rights of individuals who may be “spied” on by a drone. For example:

In Tennessee, it is a crime of trespass to fly a drone over private property below navigable airspace. Similarly, in Wisconsin, it is a misdemeanor to use a drone with the intent to photograph, record, or otherwise observe any other individual in a place where that person has a reasonable expectation of privacy.

Idaho and North Carolina prohibit people from using drones to photograph or otherwise record an individual, without such individual’s written consent, for the purpose of publishing or otherwise publicly disseminating the photograph or recording. The North Carolina law does contain and exception for newsworthy events or places to which the general public is invited. The North Carolina law also prohibits the use of drones to conduct surveillance, although it does not define surveillance.

Other states have taken the restrictions on drones farther by creating private rights of action for anyone who suffers damage as a result of the improper use of drones. In Oregon, property owners can sue a drone operator if: (1) the drone has flown less than 400 feet above the owner’s property at least once; (2) the property owner has told the drone operator not to come over his property; and (3) the operator flies the drone less than 400 feet above the property again. The drone operator can be liable for treble damages for any injury to the person or the property and attorney’s fees if the amount of damages is less than $10,000.

Texas allows use of drones to capture images when people are on public real property or with the consent of the individual who owns or lawfully occupies the real property captured in the image. However, the law forbids the use of drones to capture images of people or privately owned property with the intent to conduct surveillance on the individual or property. Wrongful conduct is a misdemeanor. There is a defense when the image is destroyed as soon as the offender realizes it was captured and the image is not disclosed to anyone else. Texas also provides owners and tenants of private property the right to file an action with statutory damages up to $10,000 and actual damages if the images were distributed with malice.

IV. APPLICATION OF STATE TORT LAW TO DRONES

As the use of drones becomes more prolific, the number of negligence, property damage and invasion of privacy claims will rise. In Illinois, traditional concepts of state tort law will likely apply to resolve these claims. While, no Illinois reported cases involve the use of drones it is important to keep the following in mind.
Personal injury and property damage claims may be similar to those involving aircraft and involve issues such as aerodynamics, lift, thrust, weather conditions, flight control software, radio frequency interference, and battery charge duration.

There may be claims against the manufacturer of a drone for strict product liability for failure to warn, breach of warranty, and design defect. These types of claims raise questions of whether the manufacturer included warnings against using the drone in close proximity to persons or stationary objects or against use in rough weather conditions. Other considerations include whether the drone had an anti-collision system that allowed it to sense an imminent collision and avoid it, had a GPS "geo-fence" which forces the drone to land when nearing restricted areas such as an airport or government building or had a secure transmission system from operator to drone to prevent a cyber attack resulting in a crash.

Liability may attach if the drone operator or owner obtains images of individuals within or areas inside or outside their home if that image is not otherwise obtainable. In other words, a person cannot legally obtain something from the air that he could not obtain from the ground. At the same time, a person bringing a claim must have suffered damages. If the information obtained by the drone is not published, there may not be a cause of action. A claim for breach of privacy may be expanded when the device is transferring wireless data. The cyber transfer of data raises issues such data retention policies, and what protection the operating or collecting entity had in place against a cyberattack, and whether the drone had a secure transmission for the wireless transfer of any data.

Historically model aircraft have typically been for hobby or recreational purposes only. The technology associated with drones has advanced to the point where they can be used for commercial purposes, but the laws have not followed. If an operator is flying for any commercial, non-hobby, non-recreational purpose, the operator must have FAA authorization. Whether operating recreationally or commercially, if an operator is reckless and endangers people, he could be liable both civilly and criminally.

V. CYBER AND PRIVACY LIABILITY: DOES THE PLAINTIFF HAVE STANDING TO PROCEED?

It is rare that a month goes by without there being a news story about a “hack” of private information. From Target to Home Depot to Sony, many entities have faced data breaches. These entities have their reputations at stake and in most cases have made customers whole when they have been damaged or provided items such as free credit report monitoring. And when the compromised data includes credit card numbers, the credit card companies are quick to issue new credit cards.

While numerous lawsuits have been filed asserting claims of invasion of privacy and negligence with respect to cyber stealing of personal information, many have not survived the motion to dismiss stage. These cases are dismissed on the basis that plaintiffs lacked standing. Courts have
held that an increased risk of identity theft is insufficient to establish standing. See e.g. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (plaintiffs lacked standing and case dismissed because the harm depended on third parties reading, copying and understanding the plaintiffs’ personal information, intending to use such information to commit future criminal acts, and being able to make unauthorized transactions in plaintiffs’ names in the future); In re Barnes & Noble Pin Pad Litigation, No. 12-CV-8617, 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sept. 3, 2013); Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060 (RMB) (RLE), 2010 U.S. Dist. LEXIS 71996 (S.D. N.Y. June 25, 2010); Allison v. Aetna, Inc., No. 09-2560, 2010 U.S. Dist. LEXIS 22373 (E.D. Pa. Mar. 9, 2010). However, when the risk of harm is real and immediate, the cases may be allowed to proceed. See e.g. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (stolen laptop).

Cases from 2014 show that whether the claims can survive a standing challenge depends on the state law or statutes at issue, the jurisdiction where the claim is brought, and whether the plaintiff’s data has actually been used or compromised.

A. Galaria v. Nationwide Mutual Insurance Company

In Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014), plaintiffs filed a putative class action after providing personal information to the defendant in the course of purchasing insurance products. The plaintiffs later received a letter from the defendant stating that their personal information was stolen during a hack of defendant’s computer network. Plaintiffs filed suit against the defendant for violation of the Fair Credit Reporting Act, negligence, invasion of privacy and bailment, although neither plaintiff alleged that their personal information was misused or that their identity was stolen. The defendant moved to dismiss on the basis of lack of standing. The court agreed and dismissed the claims. The court found that plaintiffs’ arguments that they had an increased risk of identity theft did not give them standing. The court noted that whether future damages occurred was speculative and would depend on the decisions of independent actors – i.e. the criminals who took the information and what they did with it. While the court dismissed many of the claims, it found that plaintiff had standing to pursue an invasion of privacy claim alleged under Ohio state. The court noted that Ohio imposes liability for the publication of one’s private affairs with which the public has no legitimate concern. Ultimately, though, the court dismissed this claim as the plaintiffs had failed to allege that the defendant disseminated the information to the public.

B. In re Adobe Systems Privacy Litigation

were sufficient to plead standing, especially given that two of the plaintiffs had expended costs to mitigate the risk of harm.

**C. In re Science Applications International Corp.**

In September 2011 a thief broke into a car and stole the car’s GPS system, stereo and several data tapes. *In re Science Applications Int’l. Corp. Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.C. 2014). The car belonged to an employee of SAIC and the tapes contained personal information and medical records of members of the U.S. military. SAIC was the security firm that contracted with TRICARE to ensure the security of the personal and health information. Plaintiffs filed suit alleging harm from an increased risk of identity theft and an invasion of their privacy. The claims involved state law claims as well as violations of the federal Privacy Act of 1974. The court in considering the motions to dismiss explained that “[t]his case presents thorny standing issues regarding when, exactly, the loss or theft of something as abstract as data becomes a concrete injury.” *In re Science Applications Int’l.*, 45 F. Supp. 3d at 19. The court found that those plaintiffs who merely alleged a loss of data failed to allege standing and their claims should be dismissed. As the court explained, an increased risk of harm alone does not constitute an injury in fact to satisfy standing requirements. However, those plaintiffs who asserted that their data was accessed and used could move forward with their claims.

**D. Lewert v. P.F. Chang’s China Bistro, Inc.**

In *Lewert v. P.F. Chang’s China Bistro, Inc.*, No. 14-cv-4787, 2014 U.S. Dist. LEXIS 171142 (N.D. Ill. Dec. 10, 2014), plaintiff filed a class action against P.F. Chang’s arising from a data breach involving the theft of consumers’ credit card and debit-card data. The complaint alleged claims of breach of an implied contract and violation of the Illinois Consumer Fraud Act. To get around standing arguments, plaintiffs alleged that they suffered damages as a result of overpaying for the security measures associated with the personal information as the cost of the food they purchased implicitly contained the cost of sufficient protection of personal information. Plaintiffs further claimed that they suffered actual damages from monetary losses from unauthorized bank account withdrawals and related bank fees. Plaintiffs also claimed damages associated with the costs from identify theft and the increased risk of identity theft and the time spent monitoring their bank accounts.

The court rejected the overpayment argument, finding that plaintiffs had not pled that the defendant charged a higher price for goods when a customer paid with credit. The court also looked in-depth at the alleged unauthorized bank account withdrawals and noted that there actually was not an unreimbursed charge on a credit or debit card, and thus plaintiffs had not satisfied the standing requirement with respect to that claim. Next, the court rejected the plaintiffs’ lost opportunity claims based on an assertion that plaintiffs did not have their cards accessible for a few days and could not obtain rewards points. The court explained that simply being without a debit or credit card between learning of the fraudulent charges and receiving a new card was not actionable. Finally, the court rejected plaintiff’s claim for mitigation expenses as these did not qualify for actual injuries when the harm was not imminent. The court
specifically noted that plaintiffs “cannot manufacture standing by incurring costs in anticipation of non-imminent harm.” Lewert, 2014 U.S. Dist. LEXIS 171142, at *9. Since the plaintiffs did not have standing, the court dismissed the complaint.
Ann concentrates her practice in civil litigation, including environmental and business-related disputes, nursing home litigation, and personal injury defense.

Ann joined Heyl Royster in 2013. Before joining Heyl Royster, Ann served as in-house counsel at Valero in San Antonio, TX, where she managed complex environmental, commercial, class action and tort litigation. While at Valero, Ann also served on the Information Governance Committee, and was responsible for electronic discovery and electronic records implementation, retention and destruction. Ann communicated regularly with senior management and provided day-to-day business counseling and advice. Her experience at Valero has given Ann an unparalleled ability to effectively interact with in-house counsel.

Ann began her legal career in 1994, serving as a law clerk to the Honorable James D. Heiple of the Illinois Supreme Court. After her clerkship, Ann worked for two law firms in the St. Louis area. She represented clients in environmental, class action, commercial, and personal injury matters pending throughout the country. Her clients included railroads, refiners, utilities, municipalities, health care entities, franchisors, and auto manufacturers. Ann has represented clients before the Seventh Circuit Court of Appeals, the Illinois Supreme Court and various appellate courts in Illinois and Missouri.

Significant Cases
- Wilson v. Norfolk and Western Railway Company, 718 N.E.2d 172 - The Illinois Supreme Court ruled in case of first impression that a railroad employee must prove physical contact or the threat of physical contact to recover damages for intentional infliction of emotional distress under the FELA.

Public Speaking
- “How to Handle the Midnight Call and The Building Blocks of an Effective Defense” Heyl Royster 29th Annual Claims Handling Seminar (2014)

Professional Associations
- Illinois State Bar Association
- Association of Corporate Counsel

Court Admissions
- State Courts of Illinois, Missouri and Texas
- United States Supreme Court
- United States Court of Appeals, Seventh and Eighth Circuits
- United States District Courts, Southern District of Illinois, Central District of Illinois, Northern District of Illinois, and Eastern District of Missouri

Education
- Juris Doctor (magna cum laude), University of Illinois College of Law, 1994
- Bachelor of Science-Economics, University of Illinois College of Commerce, 1991