

## **Risk, Product Liability Trends, Triggers, and Insurance in Commercial Aerial Robots**

by

**David K. Beyer, Donna A. Dulo, Gale A. Townsley, and Stephen S. Wu**

**April 5, 2014**

### **Abstract**

The commercialization of autonomous aerial robots, also known as drones or unmanned aerial systems, will make autonomous aerial robots pervasive and ubiquitous across the national airspace within the next few years. Yet even today with a highly limited number of drones operating in restricted airspace, accidents are making national news, including ones with fatalities and property damage. How can drone operators and drone manufacturers protect themselves from risk and liability once commercial operations are opened up in the national airspace in 2015?

Drones are essentially robotic aircraft. They can be operated with a “pilot” sitting in a ground station, but many will have autonomous capabilities where the aircraft will operate on its own. These autonomous aircraft will operate through advanced software systems coupled with sensing hardware and GPS navigation packaged in a highly maneuverable airframe. A key feature will be an autonomous anti-collision system that must not only protect the drone from collisions with other drones but also protects it from collisions with birds, other aircraft, buildings and structures.

The risks of crashes and incidents caused by drones in the national airspace are currently unknown. Risk profiles have yet to be determined due to the lack of available information. Insurance carriers may be able to extrapolate loss experience from the aviation industry but will need to be adjusted for the issues of robotic autonomy in flight, autonomy in collision avoidance, and autonomy in critical issues such as lost links, in which communications are cut off and the drone must make decisions on its own.

This paper will discuss drones in the national airspace from an autonomous robotics point of view. An original set of data will be presented with analysis based on studies of unmanned military aircraft accidents. These data and analysis will be applied to the current issues of national airspace integration to help determine liability triggers and trends to help answer insurance underwriting trends and products liability questions. In addition, the paper will discuss theories of product liability that plaintiffs may assert against drone manufacturers. For instance, plaintiffs may allege causes of action

such as strict product liability, negligence, breach of warranty, and the violation of laws against unfair and deceptive trade practices. The paper will apply these theories to the context of piloted and autonomous unmanned systems. It will also cover methods for mitigating product liability risks.

Finally, the paper will discuss the unique insurance issues that may arise as commercial owners, manufacturers, and operators of drones seek to limit their risks of liability and damage exposure through the purchase of insurance. The paper will discuss the current emerging market of available insurance as well as the likely trend of insurance coverage including scope, limits, restrictions and availability as more drones are deployed commercially and claim experience grows. Both domestic and Lloyd's of London based markets will be discussed.

## **I. Introduction**

The commercialization of autonomous aerial robots, "drones" will become pervasive and ubiquitous across the national airspace over the coming years resulting in an increasing risk potential for drone operators and manufacturers. The risk and liability exposure of these entities is entirely unknown due to the lack of historical data from which to determine liability triggers and trends to facilitate the development of accurate insurance underwriting. Product liability questions as well remain unanswered, with causes of action such as strict product liability, negligence, breach of warranty, and the violation of the laws against unfair and deceptive trade practices looming in the near future against operators and manufacturers.

This paper presents these issues in light of available risk and accident data, centered primarily on historical military accident data for accidents and mishaps that have occurred in the national airspace. It will address these issues in the context of manned and unmanned systems with the unique insurance issues and product liability issues facing commercial owners, operators and manufacturers of drones seeking to limit their risks of liability and damage exposure through the purchase of insurance in both domestic and Lloyd's of London based markets.

## **II. The Future Pervasiveness of Aerial Robots**

The mandate of the Federal Aviation Administration to integrate unmanned aircraft into the national airspace makes abundantly clear that the era of aerial robots is upon us. While estimates vary widely, we must assume that the number of unmanned aircraft that will enter and operate in the national airspace will be in the tens of thousands within the next five years. This includes unmanned systems of all kinds, from large government operated systems to small personally operated systems such as model aircraft.

Regardless of the size or configuration of the unmanned aircraft, every aircraft that enters the airspace poses a particular danger. A model aircraft, for example, has killed a person in this country within the past year, while the use of what is technically classified as a drone has not. So while the legal wrangling over the classification of a drone and which classification the FAA has jurisdiction over lingers, the overarching issue still remains: what are the potential risks and liabilities of operating an unmanned aircraft and how will they affect insurance underwriting trends?

This question is difficult to answer because unmanned aircraft are not flying at the rate that they will be in the near future in the national airspace. In fact, currently, commercial use of unmanned aircraft in the national airspace is prohibited by FAA regulation, and the FAA has been judicious in shutting down operators who have attempted to use drones in this manner. Thus, it may take a decade or more to establish accurate liability trends to be able to effectively gauge the true risks and liabilities of unmanned aircraft in the national airspace.

Unfortunately, operators are waiting in the proverbial wings to lift their unmanned aircraft programs off the ground. Major corporations like Amazon and Facebook have not been shy concerning their intended use of drones when technologically and legally feasible. Private operators are already putting their craft into the sky, for fun and future profit, edging as close to the commercial limitations as possible. As a result, the industry does not have time to wait to evaluate long-term liability trends and triggers.

Herein lies the challenge: is there any accurate data available to assist legal professionals, insurance underwriters, unmanned systems operators and interested parties now? The approach of this paper is to study the current power user of unmanned systems, the United States Air Force. This study, while not directly applicable to the commercial and civilian use of unmanned systems, does provide important information about the issues and effects of operating unmanned aircraft over an extended period of time.

Additionally, the study highlights possible and probable issues that may arise in the commercial or civil operation of unmanned systems in the national airspace, since the mishaps in this study are all non-combat flights and directly relate to the operation of the aircraft themselves without issues of malicious external forces at play when aircraft are operated in the heat of battle. The study, therefore, provides an initial level of theoretical guidance and practical applicability to the current integration of unmanned systems into the national airspace.

### **III. A Formal Unmanned Systems Mishap Study**

The formal investigation undertaken in this paper is a study of all US Air Force Class A unmanned aircraft mishaps over a ten year period, from fiscal year 2004 through fiscal year 2013. The US Air Force defines a “mishap” as an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. It defines a “Class A mishap” as a noncombat accident that results in a death, a permanent total disability, or damage of at least \$1 million<sup>1</sup>.

The mishap studies in our analysis were of unmanned systems of all types operated by the US Air Force. The accident reports were publically available from the US Air Force Judge Advocate General’s Corps Legal Operations Agency Claims and Tort Litigation site<sup>2</sup>.

The mishap reports are distinguished in the study between manned and unmanned aircraft exclusively. All other instances of Class A mishaps such as satellite, missile, ground station, and non-aviation related mishaps were excluded from the study. Unmanned tethered balloon mishaps were also

---

<sup>1</sup> Air Force Safety Agency (July, 2000). Air Force System Safety Handbook. HQ AFSC/SEPP Kirtland AFB, NM.

<sup>2</sup> US Air Force Judge Advocate General’s Corps Legal Operations Agency Claims and Tort Litigation (2014). <http://usaf.aib.law.af.mil/>

excluded from the study, as they do not fall into the category of unmanned aircraft but rather of tethered balloons under FAA regulations in US national airspace.

The mishap reports provided by the Air Force are extensive and provide the results of formal investigations into the causes of the mishaps. It must be noted, however, as with all formal mishap and accident reports under 10 U.S.C. § 2254(d), the opinion of the accident investigator as to the cause of, or the factors contributing to, the accident set forth in the accident investigation report, if any, may not be considered as evidence in any civil or criminal proceeding arising from the accident, nor may such information be considered an admission of liability of the United States or by any person referred to in those conclusions or statements.

The mishap reports cover the background of the unit operating the aircraft, the sequence of events, the maintenance on the aircraft, the aircraft systems, the weather, the crew qualifications, the operations and supervision of the aircraft, the governing directives and any other areas of concern. Within the report, the Abbreviated Accident Investigation Board identifies a cause of the mishap by “clear and convincing evidence”. Additional contributing factors are presented by a “preponderance of evidence” if applicable. All investigations were conducted in accordance with Air Force Instruction 51-503.

### ***A. Results of the Study***

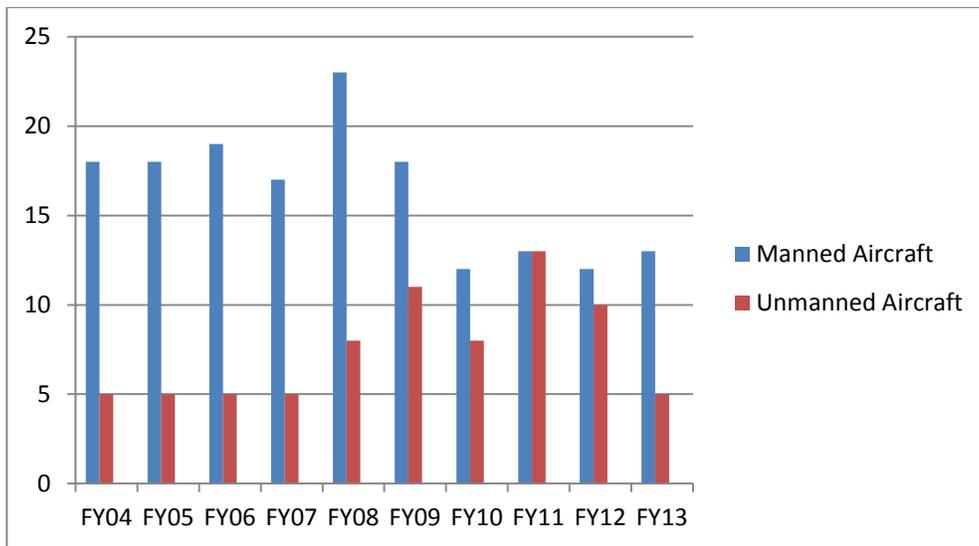
The first task of the study was to determine the frequency of manned mishaps versus unmanned mishaps over the ten year period. The results of this analysis are rather striking and match the commercial news reports highlighting the high incident rates of military unmanned aircraft. For example, the Bloomberg BGOV Barometer statistics indicate that Northrop’s Global Hawk and General Atomic’s Predator and Reaper have a combined 9.31 accidents for every 100,000 hours of flying time which is the highest rate of any aircraft of any category and more than triple the Air Force fleet wide average of 3.03 accidents for every 100,000 hours<sup>3</sup>.

Figure 1 demonstrates the results of our study, which clearly shows the high accident rates of unmanned aircraft. The blue lines represent all accidents of all manned aircraft in the Air Force while the red line represents the unmanned accidents of all aircraft models. The earlier years indicate a lower rate of mishaps, but this can be explained by the fact that all military services (Army, Navy, Air Force and Marines) logged more than 500,000 unmanned flying hours in 2008, representing a 16-fold increase over 2002<sup>4</sup> due mainly to the advances in technology and the policies of unmanned integration into military operations.

---

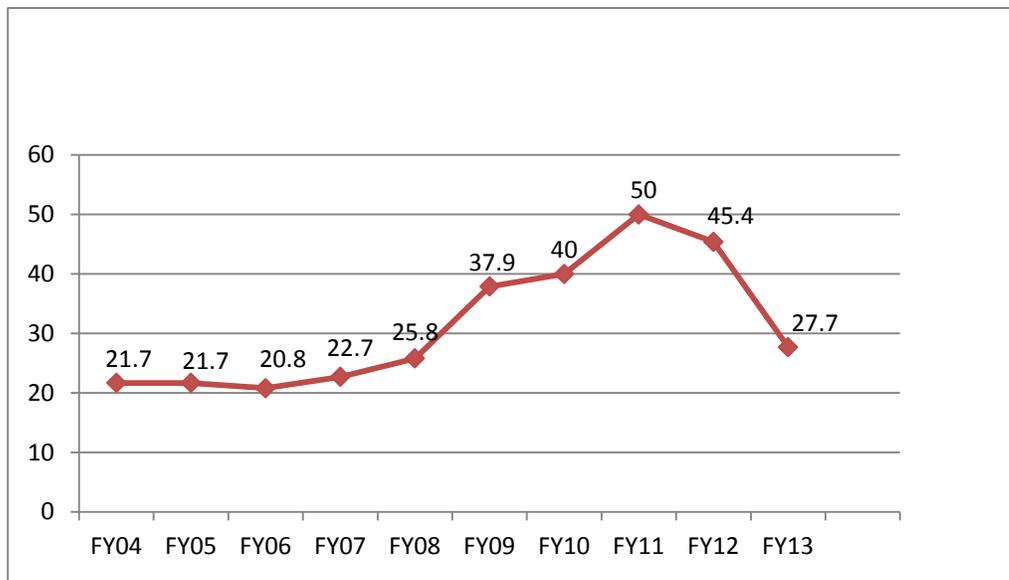
<sup>3</sup> McGarry, B. (June 17, 2012). Drones Most Accident-Prone U.S. Air Force Craft: BGOV Barometer. <http://www.bloomberg.com/news/2012-06-18/drones-most-accident-prone-u-s-air-force-craft-bgov-barometer.html>

<sup>4</sup> Bowie, C. & Isherwood, M. (Sept. 2010). The Unmanned Tipping Point. Air Force Magazine. <http://www.airforcemag.com/MagazineArchive/Pages/2010/September%202010/0910rpa.aspx>



**Figure 1 Air Force Class A Mishaps 10 Year Comparison of Manned versus Unmanned Aircraft**

Note in particular the fiscal year 2011 when the unmanned and manned mishap numbers were equal. This was the worst performing year of unmanned aircraft in the study, although fiscal years 2009 through 2012 demonstrate a pronounced increase in unmanned mishaps while manned aircraft mishaps have decreased. To provide a further graphic illustrating the trend of unmanned mishaps, Figure 2 demonstrates the percentage of unmanned mishaps in relation to overall manned and unmanned mishaps.

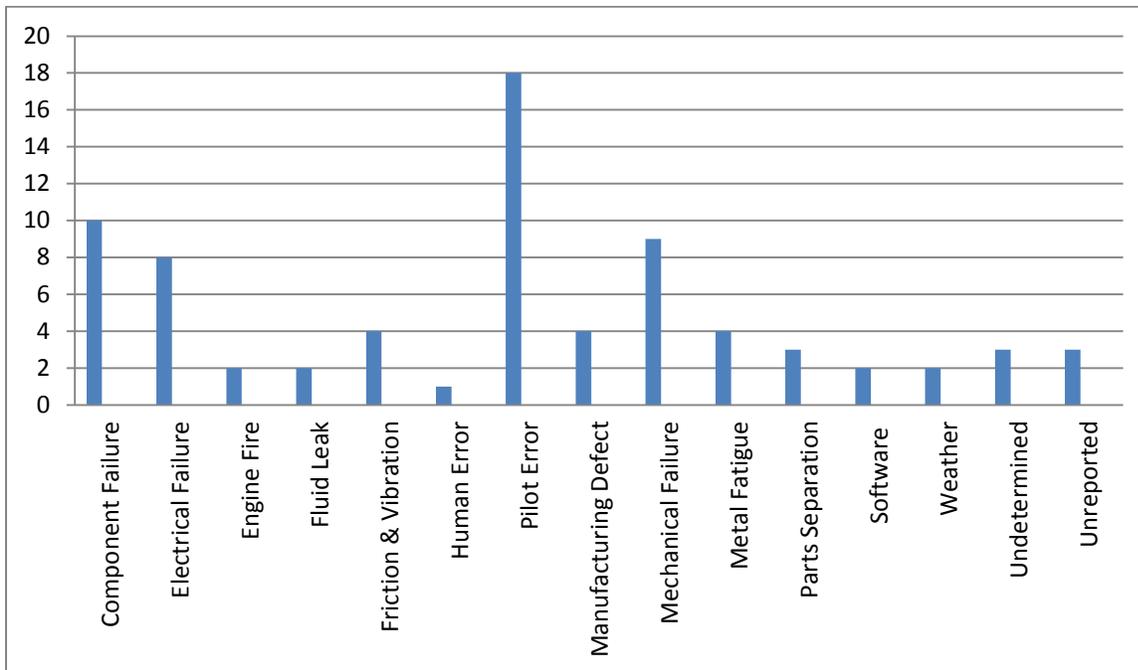


**Figure 2 Unmanned 10 Year Percentage of Class A Air Force Aviation Mishaps**

As can be seen, the increased participation of unmanned aircraft in Air Force operations has resulted in a dramatic increase in the percentage of overall Class A mishaps. The fiscal year 2013 provided a respite, with an accident rate just slightly higher than the early integration years of unmanned aircraft. From fiscal year 2004 through fiscal year 2013, there were a total of 75 Class A Air Force

mishaps, for which 72 accident reports or (in the earlier years) accident report summaries were provided by the Air Force Judge Advocate General.

The unmanned aircraft involved in the accidents during the ten year study were the Global Hawk, the Predator, the Reaper and the QF and QRF series Target Drones. The causes of the accidents are of critical importance to determine future risk and liability trends. As such, each accident report was carefully examined, including the cause of the accident as well as an analysis of the systems that failed as detailed in each report. Upon analysis, a specific set of categories was developed, and each primary cause was categorized into this set. These data are reflected in Figure 3. Aircraft categories were also noted as were the specific systems that were a cause of the mishap.



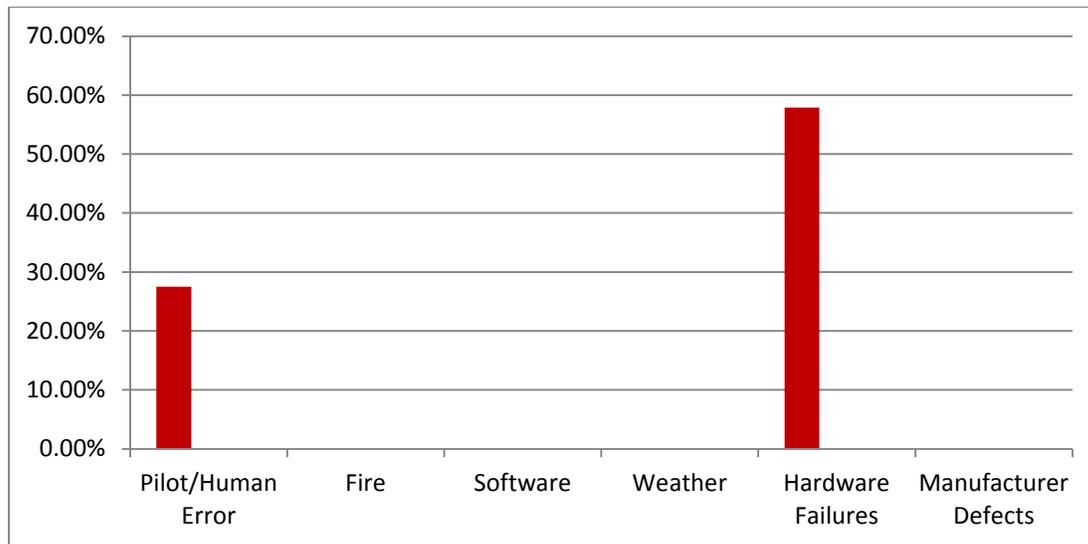
**Figure 3 Air Force Class A Unmanned Aircraft 10 Year Cause of Mishaps**

Clearly, pilot error was a major cause of unmanned aircraft mishaps across the decade of the study. The “human error” category is slightly different in nature and reflects an incident in one of the ground stations where the pilot station throttle was improperly configured between drone models MQ-1 and MQ-9 resulting in an unrecognized command, hence the separate classification.

The aircraft hardware failures were led by individual component failures followed by mechanical failures of parts systems, followed thirdly by electrical failures which included short circuits as well as unexplained power anomalies. Weather was a minimal factor in the mishaps as was system software. In the midrange were metal fatigue and catastrophic damage as a result of friction and vibration. The difference between these two categories is that components in the friction and vibration category were from non-metal sources or they were a component that was dislodged and jammed into a moving mechanical part resulting in the failure of the system. An example of this was a mishap caused by loss of control due to partially dislodged computer chip in the right aileron.

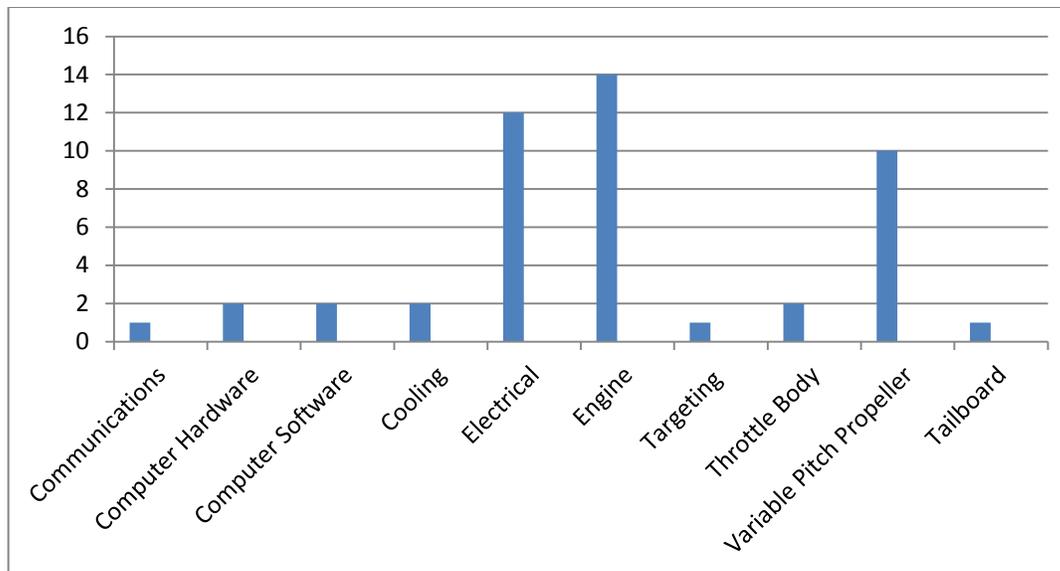
Of all of the causes, in summary, pilot/human error accounted for 27.5% of the determined and reported mishaps, .03% were due to engine fire, .03% were due to software, and, 03% were due to

weather, .06% were due to manufacturer defect in the hardware, while 57.9% were due to failure issues with the hardware of the aircraft. These data are represented graphically in Figure 4.



**Figure 4 Air Force Class A Unmanned Aircraft Overall Mishap Cause Percentages**

To further investigate the mishaps from a systems point of view, the causes were categorized according to the systems of which they were a part. Human and pilot error, as well as weather and undetermined/unreported factors were eliminated. Figure 5 demonstrates this systems points of failure viewpoint.



**Figure 5 Air Force Class A Unmanned Aircraft Systems Mishap Causes**

The data clearly indicate that engine systems failure of various types is a major contributor to unmanned systems mishaps, followed closely by the electrical system, which included the alternator and the electrical circuitry in the aircraft. The variable pitch propeller in each system was also a central point of failure. Of note is the low incidence of computer hardware and software causes of failure. The multi-spectral targeting system was the cause of one incident as was the tailboard system and the communications system. The throttle body, which was classified in this study as a separate system, had 2

incidents as did the cooling system, which was also classified as a separate system from the engine, thus dividing out slightly the propulsion system.

## ***B. Study Conclusions***

The presented study has several interesting points. First, weather was a cause in a very minor percentage of the accidents. This indicates the judiciousness of the operators in avoiding poor weather conditions, most likely through advanced meteorological systems provided by the Air Force. Second, computer and software problems were also low, which is a strong indicator of the positive viability of these systems given that they are computationally intensive and driven aircraft systems. Third, the high incidence of pilot and human error indicates training and human factors issues, which affect both the pilots and ground station operators. Finally, the high incidence of engine, propeller, and electrical systems failures indicates pervasive weaknesses in these systems that should be noted by future unmanned systems manufacturers and operators.

The study's results are by no means a comprehensive set of statistics for the determination of liability triggers and trends or comprehensive risk assessment. Rather, they serve as a starting point for the discussion. These statistics, combined with those of other services and thereafter combined with statistics generated from non-military incidents occurring in the national airspace, will give a clearer picture of the issues and risks associated with operating commercial and civilian drones.

## **IV. Product Liability Implications of the Study Conclusions**

Part III above discusses the investigation undertaken to study US Air Force Class A unmanned aircraft mishaps from fiscal year 2004 through fiscal year 2013. The study shows high accident rates of unmanned aircraft and an increase in the accident rate over time, caused by the Air Force's increased use of unmanned vehicles. The study then analyzed the causes of accidents based on the limited data available from the Air Force.

Figure 3 lists the possible causes identified by the Air Force, which Part III groups into the categories of pilot/human error, fire, software, weather, hardware failures, and manufacturer defects. Figure 4 shows the magnitude of the causes attributed to these six categories of causes. Figure 5 focuses on the specific systems of hardware causing mishaps, such as electrical, engine, and propeller systems, in comparison with mishaps caused by computer hardware and computer software.

Based on the collected data, Part III points out the high incident of pilot error as a cause of mishaps. As shown in Figure 3, pilot error was the most common cause of mishaps. Nonetheless, when all hardware failures are considered collectively, hardware failures as a group are more common as a cause for mishaps than pilot error.

This Section discusses the implications of the findings in Section III from a product liability perspective. Subsection A describes the law of product liability. Subsection B applies the product liability doctrines described in Subsection A to the causes of mishaps discussed in Part III. What do the results from Part III say about a hypothetical plaintiff's chances for succeeding in an action against a drone manufacturer assuming that civilian mishaps resemble the ones experienced by the Air Force? Subsection C analyzes the conclusions we draw from Subsection B.

## A. *U.S. Product Liability Law*

In general, U.S. product liability law applicable to civilian commercial drones will be state law.<sup>5</sup> State law will dictate:

- The causes of action available to a plaintiff asserting a claim against a drone manufacturer arising out of an accident or other event.
- The essential elements the plaintiff must prove to establish a *prima facie* case of liability under these causes of action.
- The test the courts apply to determine if a certain product's design is defective.
- Whether the defendant ever has a burden to prove the absence of a defect in a product.
- The role of the plaintiff's conduct as a partial or complete defense to a product liability claim.
- Other defenses available to a defendant.<sup>6</sup>

These state laws may originate from statutes or the common law of torts. "Tort" law refers to law applicable to wrongs that give plaintiffs the right to seek remedies in a civil action. The common law has evolved over the last decades to create causes of action based on defects in products. Some states codified their common law in state statutory schemes to supersede state common law and implement the policies chosen by state legislatures.

Another persuasive source of legal doctrine is a series of books called "Restatements of the Law." Judges, lawyers, and scholars in an organization called the American Law Institute write these books and attempt to collect, summarize, and identify trends in the law. Sometimes Restatements persuade judges to recognize new doctrines in their individual jurisdictions. For this reason, Restatements may change the direction of law. Nonetheless, the doctrines in Restatements are not binding on courts when they determine the state of their jurisdictions' laws.

### 1. The Strict Liability Cause of Action

"Strict liability" or "strict product liability" is the cause of action easiest for a plaintiff to plead and prove against a manufacturer. Courts and legislatures have recognized a strict product liability cause of action in order to spread the risk of product defects and resulting accidents broadly through society and place the burden of managing the risk on manufacturers, rather than users of the product. The theory is that manufacturers are best able to reduce risk, and insure against hazards creating the risk. The inspiration for a strict liability cause of action is Section 402A of the Restatement (Second) of Torts. Many state supreme courts follow and incorporate Section 402A into state law when establishing

---

<sup>5</sup> This subsection does not attempt to survey the product liability law of all fifty states and the District of Columbia. Instead, it identifies commonalities among groups of states; it notes majority and minority positions.

<sup>6</sup> U.S. federal law may provide additional defenses. One example is the possible preemption of state law causes of action based on a conflict with federal law. Another example is the government contractor defense in which the federal government told the manufacturer to manufacture the product to precise specifications and the product conformed to those specifications despite the manufacturer's warning about the product. As a matter of federal law, the plaintiff cannot maintain a state law action based on a defect arising out of the danger identified by the manufacturer.

common law principles of liability. In turn, states with product liability statutes also track the concepts in Section 402A to create a strict liability cause of action by legislation.

Section 402A says:

**402A. SPECIAL LIABILITY OF SELLER OF PRODUCT FOR PHYSICAL HARM TO USER OR CONSUMER**

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

(a) the seller is engaged in the business of selling such a product, and

(b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

(2) The rule stated in Subsection (1) applies although

(a) the seller has exercised all possible care in the preparation and sale of his product, and

(b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.<sup>7</sup>

A plaintiff asserting a strict liability claim against a drone manufacturer must plead and prove, under a typical state's law, that the defendant manufacturer sold a product that was "defective" at the time it left the defendant's hands, the product reached the plaintiff without substantial change, and the defect was the proximate cause of the plaintiff's injuries. A product may be defective for one or more of three reasons: (1) the product's design was defective, (2) the product had a defect in manufacture, or (3) the manufacturer failed to warn about a condition of the product.

A design defect occurs when the manufacturer fails to design the product to be safe. All copies of that product would be defective. A manufacturing defect occurs when one or a number of copies of the product are defective, even if the design was safe. For instance, if the stamping equipment caused a metal part to be too thin in one section, thinner than the design specifications, the defect arose from the manufacturing process, not the design. Finally, a product may be considered "defective" in the absence of essential warnings to inform users about certain potentially harmful or hazardous characteristics of the product.

In this Subsection, we are most interested in design defects and failures to warn. Methods to ensure safe manufacturing and uniform quality of completed parts and products are beyond the scope of this paper.

Different states have different standards for establishing when a product's design is "defective." The two main tests for the existence of a design defect are the "consumer expectation" test and the "risk utility" test. Under the "consumer expectation" test, a product is defective if it is "dangerous to an extent beyond that which would be contemplated by the ordinary consumer who purchases it, with the ordinary knowledge common to the community as to its characteristics."<sup>8</sup> For instance, if a consumer purchases a lawnmower, and upon first use, the blades shatter and fly out the side, that lawn mower is dangerous and does not work in a way that an ordinary consumer would expect.

The "risk utility" test is somewhat more complex. Under this analysis, a product design is defective if the product's risks outweigh its utility or benefits to users and the public. Frequently, a plaintiff points to an alternative design that makes the product as useful, but would not be unsafe.

---

<sup>7</sup> Restatement (Second) of Torts § 402A (1965).

<sup>8</sup> *Id.* § 402A cmt. i.

Another common issue focuses on the manufacturer's ability to reduce the risk of the design without impairing its usefulness or making it too expensive. Most states use the "risk utility" test for defining design defects. A much smaller number of states permit courts to use either test for defining design defects. A handful of states define a defect solely under the "consumer expectation" test.

Under some states' laws, once a plaintiff has made out a *prima facie* showing that a product is defective, the burden shifts to the defendant to prove that the product is not defective.<sup>9</sup> This burden shifting process may play out at trial or in summary judgment proceedings. As a general matter, however, a plaintiff bears the burden of proof in a civil case to prove the essential element of the plaintiff's claim by a preponderance of the evidence.

## 2. The Negligence Cause of Action

Under a negligence theory, a plaintiff would seek to show a drone manufacturer had a duty to exercise reasonable care in designing and/or manufacturing the drone, the manufacturer breached that duty, and thereby proximately caused the plaintiff's damages. A negligence claim is harder for a plaintiff to establish than a strict liability claim, because the plaintiff must prove that the manufacturer acted unreasonably. For instance, a plaintiff may contend that the manufacturer knew or should have known about a design defect, but failed to exercise reasonable care and sold the product anyway despite the defect.

## 3. Breach of Warranty Causes of Action

A warranty claim may be based on express statements from the manufacturer promising certain features or characteristics of the product that the plaintiff alleges are false. These express statements may come from advertising materials about the product or other communications by the manufacturer. The law may also imply a warranty that the product will not harm consumers who use the product for its ordinary purposes. This warranty is known as the "implied warranty of merchantability." Alternatively, if the seller knows that the product will be used for a particular purpose, and the buyer is relying on the seller's judgment concerning the fitness of the product, the law will imply a warranty that the product is fit for the contemplated purpose. This warranty is called the "implied warranty of fitness for a particular purpose." If the product does not conform to an implied warranty, a plaintiff could assert a breach of the implied warranty.

In order to prevail under a warranty theory, the plaintiff would have to show the existence of a warranty and a breach of that warranty. In some states, a plaintiff might need to be a purchaser of the product or a household member. Moreover, a plaintiff may need to prove that he or she provided timely notice of the defect to the seller.

## 4. Statutory Causes of Action

States have passed various kinds of legislation to protect consumers from unfair and deceptive trade practices of businesses and to give plaintiffs the right to bring suit for violations. Examples include California's Unfair Competition Law (UCL),<sup>10</sup> False Advertising Law (FAL),<sup>11</sup> and Consumer Legal

---

<sup>9</sup> See, e.g., *Barker v. Lull Eng'g Co.*, 573 P.2d 443 (Cal. 1978).

<sup>10</sup> Cal. Bus. & Prof. Code § 17200 et seq.

Remedies Act (CLRA).<sup>12</sup> The UCL strikes at any unlawful, unfair, or fraudulent business acts or practices. The FAL bars untrue or misleading advertising practices. The CLRA prohibits a list of unfair business practices, such as misrepresenting the characteristics and qualities of a product.

These statutory causes of action are interesting because a plaintiff can bring a claim even though an accident may not have occurred. A plaintiff could assert that a defect in the product diminished its value. For instance, if the plaintiff purchased a car for \$20,000, but the car's defective state meant that the car was worth only \$15,000, a plaintiff could assert that the seller sold the car for \$5,000 more than it was actually worth. Under the UCL, a plaintiff could seek restitution of the purchase price (the \$20,000) or disgorgement of wrongful profits (the \$5,000).

## 5. Defense Based on the Conduct of the Plaintiff

All states recognize a defense to a product liability claim based on the conduct of the plaintiff. In some states, a plaintiff's "contributory negligence" in using the product is a complete defense to a liability claim. Other states create a "comparative negligence" regime. Under a pure comparative negligence regime, a defense based on the plaintiff's negligent conduct does not defeat the plaintiff's claim entirely. Rather, the trier of fact (a jury or, in the case of a bench trial, a judge) determines what percentage of the plaintiff's damages were caused by the plaintiff's own conduct and diminish any award to the plaintiff by that percentage. For instance, if a jury found that there were two causes of the plaintiff's total damages of \$100,000, a manufacturing defect and the plaintiff's negligent misuse of the product, and said 75% of the cause was the defect and 25% of the cause was the plaintiff's conduct, the jury would be instructed by the judge to render a verdict for the plaintiff, but award only \$75,000 in damages.

Other states have modified comparative negligence regimes. Their laws say that if a plaintiff's negligence is 51% or more of the cause of the damages, the plaintiff cannot recover at all. If it is less, than the plaintiff's negligence merely diminishes the plaintiff's recovery as described above.

### ***B. Application of U.S. Product Liability Law to the Results of the Study***

Having discussed the different causes of action a plaintiff may assert and one major defense a manufacturer may raise based on the plaintiff's own conduct, we now turn to the product liability implications of the findings of the study.

The first result deserving attention is the attribution in Figure 3 to a small percentage of mishaps caused by "manufacturing defects." We do not have enough information to know if the Air Force used the legal standards applicable to "manufacturing defects" described above. In fact, common sense suggests that investigators were probably not that precise in identifying "manufacturing defects" as a cause. Accordingly, the mishaps labeled as such may not have risen to a level sufficient to trigger manufacturing defect liability under the legal theories described above. Moreover, we also wonder if the term "manufacturing defect" may also have covered the category of "design defect." We do not have enough information to say that these mishaps would have given a plaintiff a successful claim for either manufacturing or design defect.

---

<sup>11</sup> *Id.* § 17500 et seq.

<sup>12</sup> Cal. Civ. Code § 1750 et seq.

It is also true that the absence of a designation of “defect” by the investigator does not mean the product would not, in fact, have triggered liability. The non-weather, non-pilot error causes listed by the investigators in Figure 4 focused on fire, software, hardware failures, or manufacturing defects. The fires, software failures, or hardware failures may have been caused by design or manufacturing defects. Again, we do not have enough information about these mishaps to say that a manufacturer would have escaped liability in civil actions based on these mishaps.

In litigation, each side would have experts who would analyze all the information about a given mishap to not only identify the immediate cause, such as a hardware failure, but also to determine why the hardware failure occurred. Was the hardware failure caused by a defect in the design, a defect in the manufacture, or some other cause? That other cause may have been ordinary wear and tear affecting a non-defective component. Each product has a lifespan and needs to be maintained. The failure to replace worn out components may be the cause rather than a defect or the manufacturer’s conduct. The information available for us to study is simply not detailed enough to answer these questions.

The final observation we make about the study’s findings and product liability concerns pilot error. It is apparent that if these mishaps were the subject of civil actions, contributory/comparative negligence would be a key issue in these cases. The pilot’s own error was the most common cause of mishaps. Nonetheless, a pilot error does not automatically mean the pilot was negligent. For instance, if the manufacturer failed to design the drone to prevent a reasonably foreseeable use of the drone or action by the pilot that might be erroneous, a trier of fact could find a defect notwithstanding the immediate cause of the pilot’s error. There might be an alternative design that prevents the pilot error.

An analogy would be anti-lock brakes in cars. It is reasonably foreseeable that some people using older braking systems would cause their cars to skid on icy roads. The immediate cause of these accidents might be the driver’s failure to pump the brakes properly. However, the alternative design in the form of anti-lock brakes can prevent skids caused by a driver’s failure to pump the brakes properly. In any case, even the incidence of pilot error does not show that a manufacturer would escape liability if these mishaps were ever the subject of a civil action. Again, the information available in the reports does not provide sufficient information to show whether the pilot that caused the accident acted negligently.

### ***C. Conclusions Concerning Application of U.S. Product Liability Law to the Results of the Study***

Although the information in the mishap reports are not very precise, we can at least say that pilot error is a chief cause of the mishaps and raises the prospects of a large incidence pilot error when drones are used for commercial applications. To manage these risks, commercial entities should train their pilots carefully to prevent accidents. They should also choose drones that are easy to use and have effective interfaces.

Manufacturers should implement risk management practices to reduce the incidence of mishaps caused by the particular components noted. There may be cost-effective engineering controls that could improve safety. Moreover, the results of this study can help them focus on particular components and systems that have proven to be the greatest source of risks. Figure 5 above shows that the components and systems creating the greatest risk are the electrical components, the engine systems, and the variable

pitch propeller. If manufacturers fail to address these system risks, they run the risk that plaintiffs will claim they knew of these potential risks and failed to exercise reasonable care to reduce them.<sup>13</sup>

## V. Limiting Risk of Liability and Damages Exposure Through the Purchase of Insurance

To help understand the need and complexity around drone specific insurance coverage, we offer the following scenario: imagine a videographer operating a drone buys a standard \$1 million liability policy to cover him if the drone fails or crashes at a spectator event. The drone crashes and hits an Olympic skier causing serious injury resulting in their career abandonment. The skier sues the drone operator for the loss of future earnings from endorsements amounting to millions of dollars and obtains a judgment against the drone operator. Alternatively, the drone merely gets in the way of the skier, adversely affecting their performance resulting in a lost medal and loss of revenue from future endorsements. Although difficult cases to prove, the likelihood of the drone operator being sued is possible, and even if the suit is unsuccessful, the legal defense costs of the operator may or may not be covered under existing policy language.

### A. Where to Start—Identifying Key Risks

Darryl Jenkins, an analyst for the Aviation Consulting Group, set the scene when he said, “Insurance is the 800 pound gorilla in the room no one is talking about.” Jenkins asserts: “While FAA integration is a sufficient event ... insurability is a necessary event before businesses can successfully use UAS [unmanned aerial systems] in the National Airspace System ... because no business is going to want to be on the line for the liability concerns.”<sup>14</sup> He concludes, “Insurability will determine which sectors of the UAS market will grow and which will die”.<sup>15</sup>

We know that the commercial use of drones will be a highly regulated industry, of significant concern to insurance underwriters. The FAA has said “as safety is our top priority, UAS integration must be accomplished without ... decreasing safety ... or placing other airspace users or persons and property on the ground at increased risk.” The FAA has identified another insurable risk as well: “While the expanded use of UAS presents great opportunities, it also raises questions as to how to accomplish UAS integration in a manner that is consistent with privacy and civil liberties considerations.” (Emphasis added.)<sup>16</sup>

---

<sup>13</sup> For a more thorough discussion of risk management methods in the manufacture of robots, see Stephen S. Wu, Risk Management in Commercializing Robots (Apr. 3, 2013), *reprinted at* <http://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/29/2013/04/Risk-Management-in-Commercializing-Robotics.pdf>.

<sup>14</sup> “What’s grounding the commercial drone industry?”, Brianna Ehley, The Financial Times, 21 May 2013, <http://www.thefiscaltimes.com/Articles/2013/05/21/Whats-Grounding-the-Commercial-Drone-Industry>.

<sup>15</sup> “Insurability of UAVs: The “Gorilla in the Room” Rotor News, Helicopter Association International, <http://www.rotor.org/Publications/RotorNews/tabid/843/articleType/ArticleView/articleId/3393/Insurability-of-UAVs-The-Gorilla-in-the-Room.aspx>, posted 21 August 2013.

<sup>16</sup> U.S. Department of Transportation, Federal Aviation Agency, “Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap” First Edition – 2013, [http://www.faa.gov/about/initiatives/uas/media/UAS\\_Roadmap\\_2013.pdf](http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf)

Operational aspects of drones, all on their own, present serious risks to consider when underwriting drone insurance. They can be operated through communication with a “pilot” sitting in a ground station, but many will have autonomous capabilities where the aircraft will operate on their own. They will operate through advanced software systems coupled with sensing hardware and GPS navigation packaged in a highly maneuverable airframe. A key feature will be an autonomous anti-collision system to protect the drone from collisions. They must be designed to handle “lost links,” in which communications are cut off and the drone must make decisions alone. In addition, depending on the type of drone, they will likely be gathering, storing and transmitting a variety of data. As drones pivot through the national airspace, all of these computer and electronic communication driven systems are exposed to all manner of cyber risk as well.

From an insurance point of view, then, drone risks fall into three broad categories that define the important directions in which drone insurance products must evolve: aviation safety, privacy, and cybersecurity. Those needing to limit these risks will include owners, operators, designers, programmers, manufacturers, distributors, component vendors, and end users.

## ***B. Drone Insurance Overview***

The length of the application to buy insurance, the amount of the deductible, and the cost of the policy are usually good guidelines to determine the scope and breadth of the coverage afforded under a policy. Long applications that ask detailed underwriting questions typically offer better coverage because the insurance company is able to more accurately qualify the risk. If the application and underwriting process is short, coverage is likely to be restrictive with significant conditions and exclusions.

Large commercial businesses with drone operations will likely find more options for coverage and limits than small companies and individuals who are not likely or capable of paying higher premiums for drone insurance. When buying drone insurance it will be important to take the time to read “specimen” insurance policies brokers provide prior to making the purchase. Brokers have a responsibility to discuss the various coverages and restrictions with their policyholders to help them make informed decisions.

As drones become more pervasive in the market, more insurance companies will consider offering broader-based insurance policies designed to include aviation safety, privacy, and cyber risk protection. Insurers such as AIG and Lloyd’s of London have a competitive advantage given their appetite for emerging risks and underwriting expertise on staff.<sup>17</sup> As drone operation historical data develops in each of these lines of risk, early market entrant underwriters will be able to use that data to suggest “best practices” behavior, provide good advice to operators, manage their own exposure, and price risks more accurately.

New insurance companies entering the drone insurance market will see opportunity, but will rightly take a cautious approach to offering coverage. They will have a limited appetite and will offer coverage that will be both restrictive and limited in their scope, including strategies to restrict the amount of coverage for certain types of loss events (using sublimits to cap liability in specific situations) or by including exclusions to deny coverage for certain types of events. They may also seek to develop detailed

---

<sup>17</sup> London Underwriters also have the capacity and expertise to work with companies to custom tailor an insurance policy that specifically meets the needs of the policyholder seeking coverage. Custom tailored policies (called “bespoke” policies) allow a company to propose their risk story to underwriters, and together they work through what the important coverages are and craft a policy to suit the needs of the enterprise.

underwriting questions to assess the enterprise risk of drones and may require the operator to meet more stringent "conditions" or engage in specific business practices in order to keep coverage in force. As more insurance companies enter the drone insurance market to offer coverage, enterprises will need to evaluate different coverage forms from different insurers to find the "best fit at the best price" for their situation.

### *C. Market Overview*

A nascent but growing insurance market provides limited drone insurance coverage to consumers and businesses today. Aviation insurers have been first to market with insurance policies for drones. These policies are predominantly focused on the legal liability conditions arising from the use of flying "remote controlled aircraft" or "unmanned aerial vehicles" (UAV's).

But a "new generation" of UAV's is flying in new territory with sophisticated onboard systems capable of capturing, storing and transmitting vast amounts of data and information. These devices are entering the market at a time when laws and cases are struggling to define operating protocols; this creates underwriting uncertainty. Insurers offering coverage to help manage drone risks face not only operational and failure risk, but regulatory uncertainty, and exposures arising from emerging technologies that are subject to significant vulnerabilities.

Aviation and cyber insurance underwriters are likely to compete for this new emerging market since underwriters will need to price both "aircraft type safety" as well as "technology oriented data security and privacy concerns". FAA regulations and guidelines, new constitutional and privacy law cases, state and local attempts to manage and regulate drones, and autonomy and operational component vulnerabilities form a cluster of forces which will affect how underwriters draft policies, underwrite premiums, and handle claims.

Operators of flying drones need to buy liability insurance for when a drone fails and causes a loss. Companies looking to buy liability protection find very few insurance companies willing to offer them "broad" flight risk coverage that includes today's data risk & cyber exposure. So far, insurers that offer coverage in 2014, provide full coverage for the UAV while in flight, loss or damage to the UAV and associated electronic equipment, replacement of incompatible software following a loss, costs to investigate repairs to damaged equipment, and public liability insurance—personal injury and property damage cover for businesses.

Underwriters look at the number of hours of operation, the experience of the operator, and permission or certification compliance. Underwriters may require the Insured to take security measures to protect the drone when unattended. Exclusions are many and several key risks are not otherwise explicitly covered.

Today's Aviation Insurers have a good foundation of insuring flight risk and offer important coverage to protect operators, but they fall short of insuring many types of other risks that operators should consider when making an insurance purchase.

## **D. Coverages & Underwriting Practices**

Insurance coverage is frequently described in terms of first party and third party coverage. The most familiar coverage is third party: you are liable for damage to someone else (a third party). First party coverage applies when you are damaged.

## **VI. Commercial Drone Liability Coverage Scope**

### **A. Property Damage**

Commercial owners or operators of drone liability policies should seek coverage for both first party and third party property damage. The policy would cover first party claims for damage to the drone itself and third party coverage for damage to the property of others, including both fixed property such as buildings, homes, and land, and mobile property, such as automobiles, livestock, and other aerial tangible objects.

### **B. Personal Injury & Third Party Loss**

The liability section of the policy should provide an owner or operator with liability coverage for personal injury to themselves and others, as well as third party liability coverage for damages arising out of privacy intrusions, security breaches, and communication network failures.

### **C. Data Liability**

If the drone has the potential to collect, store, or send data, a drone owner or operator should seek liability coverage for damages arising out of the capturing or transmission of personally identifiable information/personal health information (PII/PHI), non-public personal information (NPPI), business PII and NPPI (intellectual property, trade secrets, confidential, or sensitive data, and location data).

### **D. Other First Party Coverages**

Depending on the commercial enterprise deploying the drones, owners or operators may want to consider seeking first party coverage for business interruption, drone loss of use or replacement costs, reputational loss (future earnings), data breach notification costs, crisis management costs such as public relations expense.

### **E. Exclusions**

As in most liability policies, Underwriters are likely to exclude from coverage violations of law, criminal or malicious acts, gross negligence, and “acts of nature” or “*force majeure*”. Numerous other

exclusions may be added to these policies and should be carefully reviewed to be sure they do not remove key coverage of importance to the purchaser.

## **VII. Underwriting Practices**

### ***A. Underwriting Implications of the Study***

As noted in the summaries of both Part III and Part IV above, the study reveals two key findings: hardware failures caused 57.9% of the mishaps studied, and human error or factors caused 27.5%. Although from a non-commercial context, these findings carry major significance from an underwriting point of view. The study can help underwriters focus their underwriting decisions based on the purchaser's response to questions relating to potential mishap causes demonstrated to be responsible for creating the greatest risk in the operation of drones.

With respect to both property and liability coverage, key underwriting questions should be directed to identifying and quantifying any specific hardware weaknesses of the drone sought to be insured. Underwriters should also be very concerned with the drone operator: their training, licensing or permitting, and years of experience with respect to aerial vehicles, both manned and unmanned, their experience with the components and systems that comprise and operate the drones, as well as their understanding of privacy and data liability issues affected by the management, security, and protection of the drone and any data it gathers or uses for any purpose.

### ***B. Property Damage***

To determine whether to offer property damage coverage and at what premium, insurers will evaluate the type of drone, its design, including weight, range, capacity, payload, power train, and other onboard operational systems. They will also evaluate the costs of the drone, including repair, replacement, upgrades, and maintenance. The study suggests Underwriters should pay particular attention to the quality of the electrical, engine, and propeller systems. Aviation insurers offering drone coverage are starting the underwriting process with applications typically used for manned aerial vehicles adapted for drones.<sup>18</sup> The more sophisticated the drone or its use, the more detailed information underwriters will seek in order to most accurately quantify the risk.

### ***C. Liability***

For liability risk underwriting, insurers will evaluate the type of drone, intended uses, and venues in which it will be operated or used. They will take into consideration whether the drone will be operated in urban or non-urban environments, from or over transportation arteries or densely populated areas, on or near waterways, in what airspace, and under what legal authority.

---

<sup>18</sup> See, for example, Kiln Group Aviation Division UAS OPERATORS INSURANCE PROPOSAL FORM offered through the Unmanned Aerial Vehicle Systems Association at <http://www.uavs.org/document.php?id=168&ext=pdf>

Underwriters will pay close attention to the legal requirements for use of the drone(s) to be insured and the insured's ability to comply with them, including drone licensing and permitting, authorized situational environments, and attendant duties of care. Whether the anticipated risks to be underwritten are negligence, strict liability, or ultra-hazardous activities will affect premium, scope of coverage, and potential exclusions.

## **VIII. Drone Manufacturer Liability Insurance Coverage**

The good news is that there are reasonably substantial insurance policies available to drone manufacturers. The bad news, these rarely cover any risk for data privacy or cyber liability. Limits are available, however, up to \$100,000,000 and more with worldwide coverage territory. Nevertheless, the study suggests Underwriters of this type of insurance should also pay particular attention to the quality of the electrical, engine, and propeller systems used by the manufacturer.

## **IX. Unique Commercial Drone Data Privacy & Cyber Risk Issues**

### ***A. Coverage***

Unlike most commercial manned aerial vehicles, today's drones may be outfitted with an array of software, sensors, and cameras to capture large amounts of data. This creates risks related to the software running the systems and the data captured during drone operation.

In standard property and liability policies, tangible assets consisting of physical objects or "real property" are a key policy language cornerstone. In those policies, digital data, however, is considered to be an *intangible asset* and is typically excluded from coverage. The new generation of drone liability insurance needs to provide coverage for emerging risks related to digital data.

Drone insurers will need to have experience qualifying and managing these types of risk and will likely turn to cyber insurance experience to blend underwriting talent with aviation underwriting. Combining these two areas of discipline will improve an insurance company's chance of entering the market safely and confidently.

If the drone to be insured has the potential to collect, store, or send data, a drone owner or operator should seek liability coverage for claims arising out of the capture, storage, and transmission of personally identifiable information/personal health information (PII/PHI), non-public personal information (NPPI), business PII and NPPI (intellectual property, copyright, trademark, trade secret, confidential, or sensitive data, and location data. Such claims would include libel, slander, invasion of privacy, copyright or trademark infringement, and misappropriation of advertising ideas, resulting in a blend of privacy and media liability.

Software failure to perform as intended could cause a drone to crash resulting in personal injury or physical damage. Software can also fail by becoming corrupt, losing connectivity, or "crashing", sometimes wiping or rendering itself unusable. The software could mistakenly send legally protected data to an unintended recipient resulting in breach notification liability. Software data in transit could be hacked by a criminal who steals the data, or the drone itself could be hacked and taken over remotely.

Hackers could also gain access to video, camera, or other sensor feeds and use the information gained to commit other crimes. Owners and operators of drones will need coverage for these risks as well.

## ***B. Underwriting***

Data privacy and cyber security is a complex area of risk for underwriters to understand in order to predict and price premium for the wide range of evolving possible problems.

Cyber insurance underwriting focuses on the data: the type and sensitivity of the data and intended use; the practices, procedures, and security measures put in place to protect it; owner and operator care, custody, and control of the data; the drone vendor, manufacturer, and component parts suppliers and their care and control of data; third party access to on- and off-boarding of data, who will be granted access, and protections against unauthorized access.

Everything from software design and performance to network configurations, providers and cost will be reviewed in the context of the operator's experience and use of drones. Another key factor underwriters will review is Terms of Service (TOS) and End User License Agreements (EULA) that the operator enters into when using a drone. Many TOS/EULA contracts will likely be written in such a way as to push liability onto the drone operator and away from the supplier, manufacturer, service or software providers, and venue stakeholders. Additionally, data risk can include requests, demands, or compliance orders from law enforcement and other government agencies, which may impose another aspect of operator liability in need of evaluation by underwriters before issuing a policy.

## **X. Insurance Summary**

Adequate policies for drone insurance must provide coverage for three major areas of risk exposure: safety, privacy, and cyber security. The main challenges for underwriters of these policies include the lack of historical data for an actuarial approach to underwriting, the need to extrapolate from aviation risk data and military drone experience, and the highly regulated nature of the industry. Purchasers of drone insurance will want to carefully analyze their drone insurance needs, and work closely with a broker familiar with the drone insurance market place to find a suitable carrier. Before purchasing any policy, read, understand and compare policy wording to be sure you understand what will and will not be covered in each policy you are considering. Often times, buying insurance coverage for specialty risks such as these requires buyers to understand the trade-offs involved with the coverage available at a price they can afford.

## **XI. Conclusion**

Unmanned aircraft will become ubiquitous in the national airspace. At the same time, issues of risk and liability will move to the forefront as manufacturers and operators face significant challenges arising from aircraft operations. The risks and challenges will only increase as unmanned aircraft uses in the skies becomes the norm rather than the exception. Product liability issues will inevitably generate litigation, with causes of action such as strict product liability, negligence, breach of warranty, and the violation of the laws against unfair and deceptive trade practices facing all manufacturers of unmanned aircraft and their component parts. Insurance issues will also move to the forefront, as commercial

owners, manufacturers, and operators of drones seek to limit their risks of liability and damage exposure through the purchase of insurance. Thus, through proper analysis, risk management, and observations of the liability and risk trends and triggers, stakeholders in the unmanned arena will be well equipped to handle the emerging unmanned systems market. The unmanned systems future is well on its way.

## About the Authors

**David K. Beyer** ([david@digitalriskre.com](mailto:david@digitalriskre.com)) is a licensed insurance broker since 1990, has spent the last 19 years developing new insurance products for emerging technology risks. He specializes in technology, information security and privacy liability for main street and ecommerce companies. In the mid 1990's he helped identify, develop and bring to market some of the world's first cyber insurance products including; Security Breach Liability and Privacy Liability products. Today, he is the co-founder of Digital Risk Resources, an insurance product development and distribution company that enables insurance companies to offer cyber insurance to protect their small to mid-sized business policyholders.

**Donna A. Dulo** ([dadulo@nps.edu](mailto:dadulo@nps.edu)) is a senior mathematician, computer scientist, and systems engineer for the US Department of Defense where she has worked in military and civilian capacities for 26 years. She is currently at the US Naval Postgraduate School, performing research in aviation software systems focusing on aviation software safety, reliability, and resilience. She is also a systems and safety engineer at Icarus Interstellar where she focuses on spacecraft systems safety and unmanned spacecraft systems software. Donna is an adjunct faculty member at Embry-Riddle Aeronautical University where she teaches in the area of computer and systems security. She did her undergraduate work in economics at the US Coast Guard Academy. She holds a Doctor of Jurisprudence from the Monterey College of Law, an MS in Systems Engineering from Johns Hopkins University, an MS in Computer Science from the US Naval Postgraduate School, an MA in National Security and Strategic Studies from the US Naval War College, an MAS in Aeronautics and Aviation/Aerospace Safety from Embry-Riddle Aeronautical University, an MS in Computer Information Systems from the University of Phoenix, and an MBA in Engineering Management from City University. She is a graduate of both the Marine Corps Command and Staff College and the College of Naval Command and Staff, and has a certificate in Computer Security from Stanford University. Donna is currently a PhD candidate in software engineering at the US Naval Postgraduate School. She is currently the editor and contributing author to the American Bar Association's book on unmanned aircraft law and technology.

**Gale A. Townsley** ([gat@severson.com](mailto:gat@severson.com)) is a member of the ABA Science & Technology Section's Information Security Committee and the Robotics & Artificial Intelligence committee. She is Senior Counsel in the law firm of Severson & Werson's Insurance Law group in San Francisco where she is leading the expansion of the group's coverage and monitoring services to clients developing technology, privacy, and cyber security products and programs. With nearly 25 years of insurance coverage experience, Ms. Townsley advises insurers regarding coverage, product development, and policy drafting. She also serves as monitoring counsel for London, European, and US underwriters: negotiating pre-litigation settlements, handling claims, supervising outside coverage and litigation counsel, and counseling insureds on loss prevention, risk management, professional responsibility and ethics.

**Stephen S. Wu** ([swu@ckwlaw.com](mailto:swu@ckwlaw.com)) is a Silicon Valley partner at Cooke Kobrick & Wu LLP who advises clients on liability matters arising from the manufacture and use of drones and other robots. He also advises clients and resolves disputes in information technology matters in areas including privacy, information security, data breach response, computer fraud, and secure e-commerce. He served as the 2010-2011 Chair of the American Bar Association Section of Science & Technology Law and is one of the founding members of the Section's Artificial Intelligence and Robotics Committee. Mr. Wu holds a J.D. from Harvard Law School and received a B.A. from the University of Pittsburgh.