AIRCRAFT BUILDERS COUNCIL, INC. LAW REPORT

THE *GAME OF DRONES*:
COMMERCIAL UNMANNED AIRCRAFT OPERATIONS ARE NOT YEARS AWAY – JUST AN OCEAN
Christopher S. Hickey, Los Angeles

SUPREME COURT REVIVES PERSONAL JURISDICTION AS VIABLE DEFENSE FOR PRODUCT MANUFACTURERS
Mark R. Irvine, Los Angeles

CYBERSECURITY: ARE YOU DOING ENOUGH TO PROTECT YOUR BUSINESS?
Ralph V. Pagano, New York
Paul M. Tyson, Los Angeles

USE OF VIDEOCONFERENCING TECHNOLOGY TO GLOBALIZE U.S. LITIGATION
Stephanie B. Gonzalez, Los Angeles

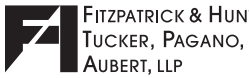
PRESENTED BY:
FITZPATRICK & HUNT,
TUCKER, PAGANO, AUBERT, LLP

Fall 2015

The ABC Underwriters, as part of their comprehensive insurance plan, have requested Fitzpatrick & Hunt, Tucker, Pagano, Aubert, LLP to prepare periodic reports on topics of interest to the members. Four articles appear in this Law Report relating to various aspects of products liability law.

The ABC Underwriters invite the insureds to take advantage of the services available under their comprehensive insurance plan. Your brokers can make appropriate arrangements.

TABLE OF CONTENTS



THE *GAME OF DRONES*: COMMERCIAL UNMANNED AIRCRAFT OPERATIONS ARE NOT YEARS AWAY—JUST AN OCEAN

By
Christopher S. Hickey

Introduction:

Hovering a few hundred feet in the air, a small unmanned aircraft fitted with several cameras begins to survey a sprawling railroad network of tracks, bridges and electrical wiring. It is time for an annual rail inspection and the aircraft's operator, sitting several hundred yards away, begins to slowly maneuver his aircraft over the railway's infrastructure recording areas of weakness revealed on his laptop screen that might require repair or at least further human evaluation. What just a few years ago took an army of maintenance crews in trucks, elevated work platforms and cranes weeks to accomplish, now takes one small unmanned quadcopter a few days—without the need to stop the operation of a single train!

The future? No, Australia. The company is Aurizon, Australia's largest rail freight company. In 2013, it purchased two German made md4-1000 drones or, as is becoming the preferred term by regulators and the industry, Remotely Piloted Aircraft Systems (RPAS), and began deploying them in 2014 to inspect company assets.[1]

---

[1] Terminology has been a moving target in the unmanned aircraft industry for years. This article will primarily adopt the term "remotely piloted aircraft system" or RPAS. RPAS is the term used by the international Civil Aviation Organization (ICAO) and will become the recommended term internationally once ICAO develops standards for member states. Australia has already announced that it will adopt the term in new unmanned aircraft regulations being developed by its civil aviation authority. Drone or unmanned aerial vehicle (UAV) will be used in this article only when discussing the aircraft portion of the larger system. However, it should be noted that the term "unmanned aircraft system" or UAS is still used by the U.S. Congress and the Federal Aviation Administration (FAA) and there is no indication from either that they plan to adopt RPAS as the preferred nomenclature.

Aurizon is not alone. Commercial RPAS operations in the U.S. are struggling somewhat to get off the ground but from the Australia outback to Canada's frozen tundra, and many points between, commercial RPAS are already flying in the world's airspace.

Global RPAS operations:

Australia's accomplishments aside, Japan is perhaps the "gold standard" when it comes to the commercial use of RPAS—at least with regard to agriculture. For over 20 years, farmers in Japan have utilized the Yamaha R-MAX, an unmanned helicopter about the size of a small motorcycle with a 10 ft rotor span and 24 hp engine. The use of this machine has become so extensive that today 60% of all rice crops are sprayed, seeded and/or monitored by more than 2,500 of these unmanned helicopters. That equates to about 2.5 million acres being cared for by aerial robots. While other countries around the world have made great strides in integrating unmanned aircraft into their airspace, only in Japan are RPAS dominating a market.

Australia can however claim to be the first country to regulate commercial drones. Partly due to its relatively light population density when compared Asia, Europe and North America, Australia in 2015 now has over a decade history of commercial RPAS use in a number of industries. In addition to the aforementioned Aurizon railroad example, RPAS are also used to survey and map known and potential mining locations, by real estate agents to market properties, and in farming to care for crops and monitor livestock. Australian news organizations were also the first in the media/entertainment industry to make use of this emerging technology—the most notable example being the Fox channel's "Foxcopter" which has been covering sporting events since 2012.

Europe has also been steadily increasing its RPAS commercial activity. The United Kingdom has approved over a

1,000 unmanned commercial operations and in Germany last year, the parcel company DHL performed the world's first commercial beyond-line-of-sight (BLOS), autonomous RPAS operation when it delivered a package of medicine from the German seaport of Norden to the island of Juist, 12-kilometers away in the North Sea.

Canada has developed a quick, flexible system for issuing commercial RPAS permits (1,647 permits granted in 2014 alone) and as a result unmanned aircraft are being used in a variety of applications, including the inspection of roads, bridges and pipelines, delivering goods to the Arctic, providing heat maps to firefighters, scanning for icebergs in shipping lanes and even prospecting for gold.

It is not just private commercial activity making use of this technology. Many public agencies in these countries are either developing an RPAS capability or contracting with private companies for that expertise. Local governments in Australia are using RPAS to watch beaches for sharks; Canadian police routinely use RPAS for search and rescue operations; and Japan uses unmanned aircraft to monitor potentially threatening geological features such as volcanoes and landslides; Japan also performed numerous RPAS flights during the 2011 Fukushima nuclear disaster.

This is not to say that commercial drone use in the US is non-existent. Far from it. The first half of 2015 saw the Federal Aviation Administration (FAA) reach several milestones in its move to integrate RPAS into the national airspace. In February, the FAA issued a Notice of Proposed Rule Making (NPRM) outlining a set of detailed regulations that, when enacted, will allow commercial RPAS to utilize U.S. airspace; it has granted over **1,200** section 333 exemptions allowing temporary commercial use in a host of industries (real estate, film production, mining, farming, and many more); and in April the FAA introduced the "Pathfinder Program," which will allow certain companies to experiment with drones beyond-line-of-sight (BLOS). These recent measures are a

vast improvement over 2014 when the FAA was more typically issuing cease and desist letters to drone operators. Nonetheless, the US is still far from the "tip of the spear" when it comes to commercial drones.

How certain countries have pulled ahead of the US and the rest of the world:

Why then did some nations which, like the US, also have crowded airspace, manage to approve so many commercial operations without causing an airspace apocalypse so often predicted by the media? They all developed a set of comprehensive regulations that ensure (1) commercial RPAS operators have at least a basic understanding of airspace, flight regulations and the RPAS they will be operating; (2) wide separation between manned aircraft and drones; (3) drones are always under the active control of a qualified operator; and (4) a process to address and ground unsafe operators.

Australia:

Australia began to regulate unmanned aircraft in 2002 when its Civil Aviation Safety Administration (CASA) issued Civil Aviation Safety Regulation part 101 (CASR 101). CASR 101 consolidated all the existing rules applicable to unmanned aircraft and rockets into one body of legislation, and created additional regulations addressing the growing use of RPAS by hobbyists and businesses. The law set forth the general operational limits for both recreational and commercial unmanned aircraft operations, as well as the requirement for registration and certifications necessary to perform a flight for commercial, governmental or research purposes.[2]

---

[2] Under CASR 101, the difference between a "model aircraft" and "remotely piloted aircraft" is the intended use of the aircraft. A "model aircraft" is an unmanned aircraft flown for sport and recreation, while a RPAS, UAV, or UAS is one used for commercial, government or research purposes. CASR 101 defines "commercial use" of RPAS as anything relating to business operations. It is not necessary that an operator receive compensation for the flight, only that the flight was conducted for some business purpose.

Airmanship knowledge:

Although many RPAS operators argue that their machines are no different than the model aircraft flown by children for decades, CASA regulators recognized the difference between radio controlled toys flown at parks and playgrounds and modern drones that can be flown miles, either manually or autonomously, from their operator and into the path of manned aircraft. Thus, Australia's RPAS regulations require that businesses undergo a certification process in order to operate a RPAS for commercial purposes. The first step is to obtain one of two types of pilot certificates: a UAV Controller Certificate (UAV CC) or, as of 2013, a Remote Pilot's Certificate (RPC). The RPC and the UAV CC both require the following:

- an Aeronautical Radio Operator Certificate (AROC);
- passing an English Language Proficiency Assessment;
- manufacturer training and assessment on the aircraft to be flown (i.e.: demonstrate that you understand how to fly your RPAS); and
- 5 hours of logged flight time with the drone to be flown.

In addition, for a UAV CC an applicant needs to pass a Private Pilot License (PPL) theory exam with at least a 70% score. The Australian's PPL theory exam covers topics taught during the ground school portion of pilot training: basic aerodynamics, aircraft flight controls and instruments, aircraft systems, airspace classifications, communication with air traffic control, and weather.

The RPC was developed to simplify the pilot training requirement. The training must cover normal private pilot ground school material, but with more focus on RPAS issues. The RPC does not have an exam requirement.

Operator's Certificate:

Flying commercially also requires a UAV Operator's Certificate (UOC). The pilot certificate (UAV CC or RPC) and the UOC do not necessarily have to be held by the same individual but both are required to perform a commercial operation. In other words, a business that obtains a UOC can hire a person with a UAV CC or RPC to fly the drone. The UOC certainly requires significantly more time and effort than the UAV CC or RPC but Australia has issued approximately 180 UOCs so it is apparently not particularly difficult—certainly much easier than what a company conducting manned flight operations could expect.

The following are the primary steps to obtaining the Operator's Certificate (assuming a UAV CC or RPC has already been obtained):

- creation of operations, flight and maintenance manuals (CASA provides a generic operations manual as a guide);
- completing the application form and submitting it and the manuals to CASA;
- CASA assessment of the paperwork submitted;
- CASA assessment of the applicant and the flight-crew's knowledge of regulations; and
- CASA-conducted practical flight test of operator competency and safety relating to the proposed commercial operation.

If all paperwork is in order (CASA can and frequently does request further information) and the company passes the CASA practical flight test, the entity will be issued a UOC. It takes a minimum of about three months for CASA to process an application but some UOC holders report it took over a year. CASA approximates the cost to be AUS $4,000 but the actual amount charged depends on the complexity of the application.

UOC holders report costs exceeding AUS $5,000 and in one case AUS $7,000. A UOC is valid for 12 months but can be renewed.

Flight Limitations:

Obtaining the UAV CC/RPC and an Operator's Certificate allows for commercial operations but not *carte blanche* access to civilian airspace. First, these simplified aviation regulations apply only to unmanned airplanes up to 150kg (330 lbs) and unmanned rotorcraft up to 100kg (220 lbs).[3] Second, all commercial unmanned flight operations must adhere to the following parameters designed to maintain sufficient separation between RPAS and manned aircraft, persons and buildings:

- visual line-of-sight flying (VLOS) only ("line-of-sight" means with your own eyes—not through binoculars or first-person-view (FPV) cameras);
- visual meteorological conditions (VMC) only;
- day light flights only;
- 30 meters from people and buildings;
- below 400 feet AGL;
- greater than 3nm from airports or a place where aircraft take off or land (such as a helipad);
- remain outside controlled airspace;
- cannot operate above large gatherings of people (i.e. at sporting events, over crowds at the beach or groups of protestors); and
- no autonomous operations (a human must always be in control).

---

[3] Larger RPAS designs require a certificate of airworthiness.

Persons or companies holding a UOC can apply to conduct operations beyond the above parameters but that is a separate application process and permission is granted on a case-by-case basis.[4] For example, flights into controlled airspace are possible but prior permission must be obtained and the RPAS operator must have the ability to actively communicate with air traffic control.

Violation of any of these rules can result in fines up to AUS $8,500 per offense (about US $7,000) or even revocation of a company's UOC. For flights risking or causing serious injury, the penalties are far more serious and are dealt with by CASA on a case by case basis.

The Future:

Although CASR 101 has been a "trend-setter," the pace of technological change in the unmanned aircraft industry since 2002 has rendered parts of CASR 101 outdated. For this reason, CASA is currently reviewing CASR Part 101, and has plans to modernize it into CASR Part 102 in a two-phase program over the next several years. This will involve a complete re-write of the regulations that will distinguish between the different classes of RPAS, primarily based on their weight. The new regulations will also formalize the name change from UAV and UAS to RPAS.

Canada:

Like Australia, Canada developed RPAS regulations relatively early and commercial RPAS operations have been allowed since 2003. Until last year, this required a commercial operator to apply for and receive a Special Flight Operating Certificate (SFOC).[5] Canada's Civil Aviation Regulations (CAR)

---

4 AC101-1, para.12.2.1.

5 CAR section 602.41 (no person shall operate an unmanned air vehicle in flight except in accordance with a Special Flight Operation Certificate).

required the submission of an application with Transport Canada at least 20 days prior to the proposed flight(s). The applicant was required to provide such information as the model of the unmanned aircraft; the details of the proposed flight—altitude, boundaries, the date and time of the flight; plan for clearing and avoiding hazards; emergency contingency plan; and a contract number for contacting the operator directly during the flight.[6] The more complex the RPAS and job task, the more comprehensive the SFOC application. However, while time-consuming, the process was not too difficult and obtaining a SFOC eventually became rather commonplace: In 2010, just 66 SFOCs were issued whereas in 2014 the number reached 914.

Not content with that success, in November 2014 Transport Canada modified this system in an attempt to simplify the rules even further for RPAS up to 25 kg (55 lbs). Commercial RPAS operations utilizing aircraft at or under 25 kg take-off weight are now exempt from the SFOC requirement.[7] The new regulations set forth two separate classes of RPAS: (1) aircraft with a maximum take-off weight of 2 kg (4.4 lbs); and (2) aircraft with a maximum take-off weight exceeding 2 kg but not exceeding 25 kg (55 lbs).[8]

For the smaller category of RPAS, no prior permission must be obtained from Transport Canada to conduct a commercial operation. However, the operator must abide by a detailed set of "General Conditions" and "Flight Conditions" which limit the type of operations that can be performed. Below are some of the key conditions (out of a total of 58) that must be followed:

- VLOS only;

---

6 CAR section 623.65(d) outlines information that should be submitted when making an application.

7 Advisory Circular (AC) 600-002 and 600-004.

8 The exemptions are due to expire in December 2016 but Transport Canada has issued proposed amendments to its RPAS regulations so the changes will become permanent.

- VMC only;
- daylight flights only ;
- below 300 ft AGL;
- remain in Class G (uncontrolled) airspace;
- 5nm from any airport;
- 5nm from built up areas;
- 100 ft from building/person;
- only one UAV may to be operated at a time even if the system is designed to fly multiple platforms simultaneously;
- yield to manned aircraft; and
- no autonomous flights.

The exemption also tasks the operator with confirming the RPAS operator is fit to fly the machine, understands all relevant CARs, and that the machine has been properly maintained and is fit for flight. Of financial significance, the operator must also have no less than CAN $100,000 of liability insurance coverage.

For RPAS in the weight range exceeding 2 kg but no more than 25 kg, the operator also does not need to receive permission to conduct the flight but must notify Transport Canada, prior to commencement of flight, of the name and contact information of the operator, the type of RPAS, the type of work being done, and the geographical boundaries of the operation.

The flight parameters are also slightly different. For example, there must be a 500 ft separation from people and buildings instead of just 100 ft, and the flight speed cannot exceed 87 knots. The operator must also have an emergency plan for losing the communication link between controller and aircraft and have the ability to contact the applicable ATC if control over the UAV is lost.

The operator of the larger class RPAS must also now attend a pilot ground school in order to obtain knowledge of (1) airspace classification and structure; (2) weather and NOTAMs (Notice To AirMen); (3) aeronautical charts and Canada flight supplements; and (4) the relevant sections of the CARs.[9]

Canada's 2014 rule changes are probably a preview of the next generation of RPAS regulations that will eventually be implemented by other countries. As mentioned earlier, Australia is also developing new regulations that will include different regulations for different weight classes of RPAS. The International Civil Aviation Organization (ICAO), too, has also hinted that its standards, when issued, will differentiate between RPAS on the basis of weight with less regulation for machines under 25 kg.

By comparison, the NPRM issued by the FAA in February of this year contained a set of RPAS regulations very similar to Australia's current 2004 rules. Thus, at the pace Australia, Canada and other countries are moving, the FAA's unmanned aircraft regulations may turn out to be somewhat "behind the times" even before they are adopted.

***United Kingdom*:**

In 2010, the United Kingdom's Civil Aviation Authority (CAA) first adopted regulations allowing small RPAS commercial operations or "aerial work," to use the regulation's terminology.[10] The CAA defined "small" as 20kg or less, and "aerial work" as meaning any purpose (other than public transport) for which an aircraft is flown "if valuable consideration is given or promised with respect to the purpose of the flight."

Having a small enough drone is only the first the step, though, in guaranteeing a gainfully employed robot. In order to ensure that sufficient safety measures have been put in place,

---

9 AC 600-004.

10 ARTICLE 166/167/253 OF AIR NAVIGATION ACT, 2009 (CAP 393).

potential commercial operators are required to obtain CAA permission for the specific operations being contemplated. The applicant must demonstrate that safety has been considered and that steps have been taken to avoid endangering anybody. This may be as simple as preparing a safety case for a one-off flight or, for operators contemplating regular flights, the submission of an operations manual for approval.[11] There is a charge for each application and the permission granted is only valid for a maximum of 12 months.

The CAA also requires some proof of the operator's overall airmanship skills and his/her ability to operate the aircraft safely. This is not a requirement for a pilot's license but it is an independent assessment of an individual's knowledge and operating capabilities and is also a means for the CAA to ensure that everyone has at least some basic airmanship knowledge. There are two companies which are currently able to assess operator competence on behalf of the CAA.[12] The potential commercial operator will be charged for this service. These organizations also offer a service to help people through the process of obtaining permission to conduct a specific commercial operation.

As with the regulations in Australia and Canada, the UK also places additional (and similar) operational limits on commercial RPAS flights that are approved:

- VLOS only;
- below 400 ft AGL;
- remain clear of controlled airspace unless operator has clearance from ATC;
- no flights further than 500 meters from pilot operator;

---

11 CAP 722.

12 EuroUSC, which conducts the "Basic National Unmanned Aircraft Systems Certificate-Small" (BNUC-S) assessment; and Resource UAS, which conducts the "Remote Pilot Qualification-Small" (RPQ-S) assessment.

- 150 meters from any event/assembly; and
- 50m from person/building (<7kg); or 150m from person/building (7kg to 20kg)

Drones 20-150 kg must be registered with the CAA and qualify for a certificate of airworthiness.

***Germany*:**

There is also a regulatory framework in place in Germany for the commercial use of drones. Germany's Aviation Act has been amended to recognize RPAS as aircraft and the federal aviation authority implemented legal guidelines on permits, licenses, distances, required insurance coverage and many more practical and legal details.[13]

The Act classifies drones up to a weight of 25 kg as aerial vehicles, which are partially exempt from the demanding standard approval process for aircraft. Any drone over 25 kg requires a special permit to operate. Germany is unique in one aspect compared to other European states in that it is the individual German federal states, and not the national government, that provide the permission to operate within their borders. The individual states are also allowed to create additional operating requirements as each sees fit.

Exempt drones are further classified in Germany according to two weight categories: (1) up to 5 kg; and (2) over 5 kg but less than 25 kg. Those wanting to operate RPAS smaller than 5 kg for commercial purposes must apply for a flight permit from the relevant federal state authority. Depending on the state the RPAS will be operated in, there are different lengths for which a permit will be valid and different criteria for receiving a permit. For example, in North-Rhine Westphalia the authorities responsible for

---

[13] German Aviation Regulation (LuftVO), Article 15a, 16 and 16a.

issuing permits are the district councils of Dsseldorf and Mnster, which offer two-year "general flight permits."

During the permit process, a potential operator must also provide evidence of pilot training and experience, and demonstrate an understanding of the RPAS to be used. In addition, German regulations require operators to have insurance.

If the UAV is over 5 kilograms, the operator must additionally get permission from local police for each flight. They must also receive permission to fly the drone over any private property prior to flight.

As with the regulations in other countries already discussed, Germany also places additional (and, again, similar) operational limits on commercial RPAS flights that are approved:

- VLOS only;
- 30m to 100m AGL (depends on the state)
- flights cannot exceed 200m to 300m from pilot operator
- 1.5 km from any airport
- Flights over public gatherings need special permit

European Union Regulations:

In addition to their own national regulations, commercial operators within the European Union (EU) will one day likely be subject to regulations promulgated by the European Aviation Safety Agency (EASA).[14] Currently no regulations exist save for a requirement that unmanned aircraft 150 kg or more pass design and manufacture certification specifications. However, EASA, like ICAO, plans to have a first set of regulations in place by 2018.

---

[14] European Regulation No. 216/2008.

Japan:

Surprisingly, Japan, the nation whose commercial drones are so fully integrated into its agricultural industry, does not actually have a comprehensive set of RPAS regulations. In fact, its national aviation agency, the Japan Civil Aviation Bureau (CAB), has promulgated no common regulatory rules concerning the operation of unmanned aircraft in Japanese airspace.[15] This, however, is the result of how the Japanese government is structured rather than some national cavalier attitude toward aviation safety.

In Japan, the individual cabinet level ministries possess significant political power. Agriculture is regulated by the Ministry of Agriculture, Forests and Fisheries. Under this Ministry's control is the Japan Agricultural Aviation Association, an association comprised of RPAS manufacturers, RPAS dealers and agricultural businesses. It is this organization that recognized the benefit of using RPAS in agriculture and established standards for their operation in the areas of (1) operator training; (2) flight parameters and limitations; (3) aircraft registration; and (4) aircraft maintenance. Specifically, flight operations on the farm are limited to an altitude of 3 meters (10 ft), a maximum speed of 20 km/hour (12 mph), and must remain within 200 meters (650 ft) of the operator. Operator training consists of obtaining the drone manufacturer's required training and maintenance and quality requirements are also per the manufacturer's recommendations. Design requirements are not extensive but do require that the drone drop on the spot in the case of engine failure or communication link interruption. All these rules apply only to farmers using RPAS and to no other segment of Japanese society.

---

[15] Japan's Civil Aeronautics Act No. 118 (2006) does prohibit "rocket, fireworks, or other item" within 9 km of any airport and these items must remain with 150m AGL but it is unclear if this law applies to RPAS.

While definitely a much different approach to RPAS regulation than the national regulatory schemes developed by Australia, Canada and other countries, Japan's system has resulted in a segment of their economy quickly and completely adopting RPAS technology. It's tough to argue against that level of success. However, to date, that approach has also failed to lead to the expansion of RPAS use into any other Japanese industry. That will probably require CAB regulations that apply nationwide.

In 2015 Japan's legislature and the CAB have begun to propose statutes and regulations that if enacted would apply to all RPAS activity within Japanese airspace. Unfortunately, though, most of the laws being proposed are aimed at simply prohibiting RPAS from flying. Local governments in Japan have passed numerous ordinances banning drones from parks, near buildings, etc. and imposing hefty fines for any violation.[16] For the time being, the national legislature appears to be continuing this approach rather than proposing a plan for the full integration of RPAS into civil airspace.

The Sky Did Not Fall—Accidents and Injuries:

Reports of near misses between drones and aircraft and the dangers of manned and unmanned aircraft sharing the same airspace have almost become a daily news item in the US. So, one would believe that any country crazy enough to allow extensive commercial drone operations must by now be experiencing the wrath of the aviation gods upon them in the form of aircraft falling from the sky like raindrops. Happily, that has not been the case. There have certainly been accidents involving commercial RPAS: in Japan, a farmer was killed by a Yamaha R-MAX during a botched landing; in Australia, the Fox News Foxcopter crashed into a wedding party, and in Canada a drone struck and damaged a building while filming a commercial. There are other examples, but

---

[16] Flying a drone too close to the Imperial Palace in Tokyo, for example, could result in a year in jail and a JPY 500,000 (US $4,000) fine.

the vast majority of incidents being reported are the result of recreational use and unregulated commercial use of drones.

A near mid-air collision in Australia in 2013 might actually attest to the benefits of well-regulated RPAS operations. On 12 September 2013, the pilot of a manned aircraft, an Ayres S2R, began an aerial agricultural spraying operation. At about the same time, the operator of a RPAS, Sensefly eBee, arrived at a nearby mine site to conduct an aerial photography survey. After completing his pre-flight preparation and risk assessment of the operation, the RPAS operator broadcast on the area frequency advising his intention to conduct operations over the mine site. Not receiving a response from the Ayres pilot he knew to be in the area, he then asked the mine manager to contact the farmer to advise him of the drone operating in the area.

Unfortunately, the farmer only informed the Ayres pilot that there would be an "aircraft" conducting aerial photography over the mine site. The pilot assumed that this would be a fixed-wing aircraft operating at or above 500 ft AGL. During their operations the two aircraft came within 100 meters of each other. Although a failure to communicate created an unfortunate danger, the efforts of the RPAS operator to conduct a pre-flight made him aware of another aircraft in the area and his efforts to communicate his presence and operational area would, in most cases, have increased safety. The RPAS operator's actions are a direct result of the training and flight approval process mandated by Australian unmanned aircraft regulations.

The risk of unmanned aircraft to manned aircraft is patent. Careless, and intentionally unsafe operators, will constantly serve to highlight the challenges of having a diverse mix of aircraft operating in the same airspace. However, the extensive regulatory framework for commercial RPAS activity developed by Australia, Canada, and others, does not appear to add to that risk, but rather helps to minimize it.

SUPREME COURT REVIVES PERSONAL JURISDICTION AS VIABLE DEFENSE FOR PRODUCT MANUFACTURERS

By
Mark R. Irvine

Recent opinions by the U.S. Supreme Court have recast long-held assumptions about personal jurisdiction—the doctrine that limits a court's power to enter judgment against out-of-state or foreign defendants. This change in law curtails a plaintiff's choices in terms of where to sue, and provides corporate defendants a much stronger basis to challenge personal jurisdiction.

I. Background Concepts

A. Court Jurisdiction Generally

Jurisdiction of a court is the power to decide a certain case. A court must have jurisdiction over both the subject matter of the case and the parties. Jurisdiction over parties is referred to as personal, or *in personam*, jurisdiction.

B. Personal Jurisdiction Origins

In recognition of the sovereign nature of states and the U.S. system of interstate federalism, courts historically held that those living or primarily operating outside a particular state have a constitutional right not to be subject to jurisdiction of that state's courts. In an 1877 case, the U.S. Supreme Court focused on the "elementary principle" that no state court "can extend its process beyond [its] territory so as to subject either persons or property to its decision."[1]

As business expanded across state lines, courts began to relax this rigidly territorial approach, and instead determined whether a defendant was subject to suit by assessing the

---

1 *Pennoyer v. Neff*, 95 U.S. 714, 722 (1877).

defendant's "contacts" with the state, regardless of whether it was physically present. In the landmark 1945 case *International Shoe Co. v. Washington*, the U.S. Supreme Court established a "minimum contacts" standard. The Court held that a nonresident shoe manufacturer was subject to suit in the state of Washington over delinquent payments to a state unemployment compensation fund based on the presence and sales activity of about a dozen salesmen who resided in Washington. The Court explained in an oft-quoted passage that the Due Process clause of the U.S. Constitution requires only that the nonresident defendant have "certain minimum contacts with [the state] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[2]

C. General and Specific Personal Jurisdiction

There are two types of personal jurisdiction: general and specific. When a defendant is subject to a court's general jurisdiction, it can be sued in that state for any and all claims, whether or not the claim has any connection to the state and wherever in the world the claim arises. By contrast, specific jurisdiction subjects a defendant to personal jurisdiction only for those claims that arise from the defendant's activity in the state.

D. Stream of Commerce

This theory of personal jurisdiction applies to product manufacturers and refers to the distribution channel by which products reach consumers. As one commentator noted, "few issues of personal jurisdiction are more important than the status of this stream of commerce theory."[3] Nor has a theory proved as vexing for courts. As discussed below, the U.S. Supreme Court is divided on the applicable standard for stream-of-commerce cases. The

---

2 *Int'l Shoe Co. v. State of Wash., Office of Unemployment Comp. & Placement*, 326 U.S. 310, 316 (1945).

3 4 Charles Alan Wright et al., Fed. Prac. & Proc. Civ. § 1067.4 (3d ed.)

question typically boils down to the degree of involvement a manufacturer must have in placing its product in a particular state's market.[4] The more involvement, the more likely jurisdiction will be upheld.

II. The Customary Challenge

Before the recent cases discussed below, the Court's last major opinion on personal jurisdiction was close to twenty-five years ago, and took the form of a divided plurality decision.[5] Thus for many years, practitioners and courts alike addressed personal jurisdiction by analyzing a customary set of facts submitted by the defendant challenging jurisdiction, showing by affidavit that the defendant does not have necessary business contacts in the state that would support personal jurisdiction:

- Defendant is not qualified to do business in the state;
- Defendant has no employees in the state;
- Defendant pays no taxes in the state;
- Defendant has no officers in the state;
- Defendant has no office or facility in the state;
- Defendant has no telephone listings, bank accounts or books of record in the state.

Such challenge often did not differentiate between general and specific jurisdiction, but rather attempted to show the lack of "minimum contacts" regardless of which theory applied.

---

4 *Compare World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980) (Oklahoma court lacked jurisdiction over New York car seller who sold car to New York residents who in turn drove to Oklahoma where accident occurred) *with Richtek Tech. Corp. v. uPI Semiconductor Corp.*, No. C 09-05659 WHA, 2011 WL 2470341, at *1-3 (N.D. Cal. June 21, 2011) (jurisdiction proper over chip maker in infringement case where defendant placed chips into a stream of commerce directed at California).

5 *Asahi Metal Industry Co. v. Superior Court of Cal.*, 480 U.S. 102 (1987).

Results varied, depending on the extent of contacts as determined by the court.

III. Recent U.S. Supreme Court Cases

The Court has significantly clarified personal jurisdiction in three recent opinions, and left aspects of stream of commerce unsettled in a fourth. The most important change affects a plaintiff's choice of where to sue. Before the recent cases, plaintiffs routinely filed suit against foreign or out-of-state defendants in states lacking any connection to plaintiffs' claims (apart from the location of their counsel's offices). A Los Angeles Superior Court trial judge noted as much in a recent ruling:

> "Over the years any number of suits have been brought and tried to conclusion in California where the connection of the facts giving rise to the suit to events occurring in California has often been slim or non-existent. Indeed, a sophisticated practice of law has developed in California where claims of plaintiffs from across the entire country are brought together to be litigated as Judicial Council Coordinated Proceedings in this court and in several other urban locations throughout the state."[6]

This tactic of suing without a state connection often succeeded in establishing jurisdiction over large corporate defendants, because large corporate defendants typically conduct substantial business in most states. It has been widely assumed for decades that such substantial business met or exceeded *International Shoe's* "minimum contacts" standard.[7] The new cases

---

[6] *Robinson v. Johnson & Johnson*, 2015 WL 3923292 (Cal.Super.).

[7] A standard California practice guide characterized the prior practice as follows: "The court *must* deny a motion to quash if there are 'minimum contacts' with the nonresident defendant; and many opinions broadly construe what constitutes 'minimum contacts'!" Weil & Brown, California Practice Guide: Civil Procedure Before Trial (Rutter Group 2014) § 3:417.6.

make clear that "doing business" is an obsolete notion for determining personal jurisdiction—even when on a scale conducted by large multi-national corporations. Rather, a plaintiff may now only sue in a state where the defendant is "at home" or domiciled, or where defendant engages in activity that gives rise to plaintiff's claims.

Goodyear Dunlop Tires Operations, S.A. v. Brown

The first in the recent series of U.S. Supreme Court decisions on personal jurisdiction arose from a bus accident in France that killed two 13-year-old boys from North Carolina.[8] The boys' parents sued the tire manufacturers in North Carolina state court. The European-based tire manufacturers challenged personal jurisdiction, which issue reached the U.S. Supreme Court.

Before the change in law made by this case, distinctions between general and specific jurisdiction were sometimes overlooked. For example, the North Carolina state court concluded, correctly, that the European tire manufacturer was not subject to specific jurisdiction in North Carolina, because the lawsuit arose from a bus accident in France involving tires made in Europe. But the lower court alternatively concluded that the tire manufacturer was subject to North Carolina's general jurisdiction, because the manufacturer placed other tires in the "stream of commerce" that led to North Carolina. The U.S. Supreme Court said this analysis "elided the essential difference between case-specific and all-purpose (general) jurisdiction." Quoting *International Shoe*, the court held in a unanimous decision that "'continuous activity of some sorts within a state ... is not enough to support the demand that the corporation be amenable to suits unrelated to that activity'", i.e. under a general jurisdiction theory.

The Court further explained that "stream of commerce" is a specific jurisdiction concept, and that the flow of a

---

8 *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 131 S.Ct. 2846 (2011).

manufacturer's products into the state does not support general jurisdiction. The Court also suggested that *International Shoe*, a case studied by all law students in first-year civil procedure courses, may have been misunderstood, because it too was mainly about specific jurisdiction. General jurisdiction, by contrast, is something altogether different, for which the Court fashioned an entirely new test: where the defendant is "at home". The Court defined "at home" for corporations as either the state of incorporation or principal place of business.

The Court accordingly reversed the North Carolina state court, which had neither specific nor general jurisdiction over the European tire manufacturer. There was nothing about the plaintiff's claim that related to the tire manufacturer's activity in North Carolina, thus foreclosing specific jurisdiction. Nor was the tire manufacturer "at home" in North Carolina, because it was not incorporated or principally based there.

Daimler AG v. Bauman

The Supreme Court elaborated on these new restrictions to personal jurisdiction in a second case entitled *Daimler AG v. Bauman*.[9] This case also involved injuries that occurred outside the United States. Argentine plaintiffs claimed damages against the German car maker, Daimler AG, based on allegations that Daimler's subsidiary in Argentina collaborated with a military dictatorship in committing human rights violations in Argentina. The lawsuit filed in California was based on contacts of Daimler's U.S. subsidiary with California, which the appellate court agreed could be imputed to Daimler based on an agency theory.

The Supreme Court rejected the agency theory, but went further, explaining that even if the U.S. subsidiary's contacts were imputed to Daimler, those contacts did not make Daimler "at home" in California—the new test for general jurisdiction. This

---

[9] 134 S.Ct. 746 (2014).

point is significant because the contacts in question were extensive, including being the largest supplier of luxury vehicles to California, with multiple California facilities. Indeed, the plaintiffs argued that a corporation should be subject to general jurisdiction in its home state, as well as where it "engages in a substantial, continuous, and systematic course of business." The Court rejected this formulation as "unacceptably grasping." Referring back to an *International Shoe* key phrase, the Court said "continuous and systematic" was used to describe instances when *specific* jurisdiction was appropriate. General jurisdiction, by contrast, requires "affiliations with the State [that] are so continuous and systematic as to render [it] essentially at home in the forum State." The Court reasoned that if merely doing business were the test for obtaining general jurisdiction over out-of-state defendants, then a corporation operating in many places could be deemed at home in all of them, which would "scarcely permit out-of-state defendants 'to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.'"

Daimler Footnote 19—the Exceptional Case

The Court in *Daimler* reiterated that a corporation's "paradigm" home for purposes of general jurisdiction is either its place of incorporation or its principal place of business. But, and despite the opinion's clear directive that "doing business" is no longer relevant, the court stated in footnote 19 that it does not "foreclose the possibility that in an exceptional case" a corporation's operations in a state "may be so substantial and of such nature as to render the corporation at home in that State." The Court made clear that the operations at issue in *Daimler* "plainly do not approach that level." Plaintiffs' counsel can be expected to explore what level would suffice as an exceptional case.

Walden v. Fiore

In this specific jurisdiction case, the plaintiffs were carrying $97,000 cash on a flight from Puerto Rico to Nevada.[10] A Drug Enforcement Administration agent seized the cash during a stop in Atlanta. Plaintiffs said they won the cash gambling, and the agent eventually returned the cash. Plaintiffs filed suit against the agent in Nevada. The agent challenged Nevada's personal jurisdiction over him.

The Supreme Court held that the Nevada court lacked personal jurisdiction over the Georgia agent because the agent had no "jurisdictionally relevant contacts" with Nevada. Plaintiffs insisted there were sufficient contacts because the agent knew the plaintiffs were heading to Nevada and that his wrongful forfeiture of the cash would have an effect there. Plaintiffs relied on an earlier libel case in which the Supreme Court upheld jurisdiction of a California court over Florida journalists for a libelous article that had its injurious effect against the plaintiff in California.

In rejecting these arguments, the Court held that "minimum contacts" is a "defendant-focused" test that examines what contacts the defendant had with the forum state, not with a resident of the state. The focus of the inquiry concerns "'the relationship among the defendant, the forum, and the litigation'", and thus the "proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant's conduct connects him to the forum in a meaningful way." The Court distinguished the libel case by noting that the "reputation-based 'effects' of the alleged libel connected the defendants to California, not just to the plaintiff." The Court accordingly concluded that there was no jurisdiction over the Georgia agent in Nevada.

---

[10] *Walden v. Fiore*, 134 S. Ct. 1115 (2014).

J. McIntyre Machinery Ltd. v. Nicastro

While the three cases discussed above were essentially unanimous, this "stream of commerce" decision was not.

The New Jersey plaintiff in this case severed his fingers while working on a metal-shearing machine.[11] He sued the machine's British manufacturer in New Jersey state court. There was no question, in light of *Goodyear*, that the New Jersey court lacked general jurisdiction over the foreign manufacturer, because it was in no sense "at home" in New Jersey. Rather, the question was over specific jurisdiction.

The New Jersey court held the foreign manufacturer was subject to specific jurisdiction on grounds that the manufacturer knew its products were distributed through a nationwide distribution system "'that might lead to those products being sold in any of the fifty states.'" In a fragmented, plurality decision, the U.S. Supreme Court reversed the New Jersey court, disagreeing on a "stream of commerce" rationale.

Six of nine justices, in two separate opinions, found error in the New Jersey court's rendition of the stream-of-commerce test, because specific jurisdiction cannot be based merely on a manufacturer's knowledge that its products are distributed through a system that *might* lead to sale in any state. But these six differed in articulating what test does apply.

Ironically, four of the justices noted at the outset of their opinion that the case presented an opportunity to "provide greater clarity" on "decades-old questions left open in *Asahi Metal Industry Co. v. Superior Court of Cal.*", the previous "stream of commerce" case last considered by the Court some twenty-five years earlier.[12] However, a majority of justices could not agree on a

---

11 *J. McIntyre Machinery Ltd. v. Nicastro*, 131 S. Ct. 2780 (2011).

12 *Asahi Metal Industry Co. v. Superior Court of Cal.*, 480 U.S. 102 (1987).

unified stream-of-commerce standard, and thus the identical questions have been left open again by this case.

Below is a brief summary of the three separate opinions generated by this case.

Four-justice plurality opinion: Four justices (Kennedy, Roberts, Scalia and Thomas) focused on the fact that the manufacturer in this case never marketed the machine in, nor shipped it to, New Jersey. Rather, an independent distributor sold the machine to plaintiff's employer. For these four justices, specific jurisdiction requires that a manufacturer "seek to serve" a given State's market, and is proper only where the manufacturer "can be said to have targeted" the state, by "manifest[ing] an intention to submit to the power of the sovereign." These four rejected the assertion that an intent to serve the entire U.S. market as a whole is sufficient.

Two-justice concurring opinion: Two justices (Breyer and Alito) focused on the same facts as the plurality—a single isolated sale with no showing of any specific effort by the manufacturer to sell in New Jersey—which they agreed did not establish specific jurisdiction. However, they concurred only in the judgment of reversal, expressing reluctance to join the "seemingly strict no-jurisdiction rule" contained in the plurality opinion. They saw no need to fashion such a new standard. Taking the facts as presented, these justices concluded that the plaintiff did not meet his burden under existing precedent of showing "some specific effort by the British Manufacturer to sell in New Jersey."

Three-justice dissenting opinion: Three dissenting justices (Ginsburg, Sotomayor and Kagan) would have upheld the state court's finding of specific jurisdiction because the foreign manufacturer targeted the whole United States: "when a manufacturer or distributor aims to sell its product to customers in several States, it is reasonable 'to subject it to suit in [any] one of those States if its allegedly defective [product] has there been the

source of injury.'" The dissenters focused on the defendant's "purposeful step" to reach customers "anywhere in the United States," which made it fair for the manufacturer to defend where its machine caused injury.

The McIntyre v. Nicastro Aftermath

Although one of the opinions garnered more votes than the other two (4 votes to 2 to 3), and is thus known as the "plurality," it did not constitute a majority of five, leaving lower courts in a quandary on how to apply the case. In these circumstances the holding is to be viewed "as that position taken by those Members who concurred in the judgments on the narrowest grounds ...."[13] But gleaning a holding from Justice Breyer's concurring opinion is not so easy. As one court observed: "Like one of Dr. Rorschach's amorphous ink blots, Justice Breyer's opinion is susceptible to multiple interpretations."[14]

Most courts have concluded that Justice Breyer's concurring opinion made no change in law, and that therefore the uncertainties created by *Asahi* endure.[15] Other courts read Justice Breyer's concurring opinion as making new law by endorsing a "stream-of-commerce plus" test, one of the competing standards from *Asahi* which requires the defendant to have purposefully directed the product toward the forum state, as opposed to merely being aware that the product may end up there.[16]

---

13 *Marks v. United States*, 430 U.S. 188, 193 (1977).

14 *State v. NV Sumatra Tobacco Trading Co.*, 403 S.W.3d 726, 759 (Tenn. 2013).

15 *Id*.; *Monge v. RG Petro-Mach. (Grp.) Co. Ltd*., 701 F.3d 598, 619-620 (10th Cir. 2012); *Hatton v. Chrysler Canada, Inc.*, 937 F. Supp. 2d 1356, 1366 (M.D. Fla. 2013); *Ainsworth v. Moffett Eng'g, Ltd*., 716 F.3d 174 (5th Cir. 2013); *AFTG-TG, LLC v. Nuvoton Tech. Corp*, 689 F.3d 1358 (Fed. Cir. 2012).

16 *E.g*., *Smith v. Teledyne Cont'l Motors, Inc.*, 840 F. Supp. 2d 927, 929 (D.S.C. 2012).

IV. Conclusion

Despite the unsettled "stream of commerce" theory, the impact of the other decisions could be dramatic, and may more often than not limit lawsuits to a defendant's corporate home. No longer may a corporation be sued wherever it conducts business, even on a substantial scale. Plaintiffs must now show some connection between their claims and choice of forum, or be confined to the defendant's home forum.

CYBERSECURITY: ARE YOU DOING ENOUGH TO PROTECT YOUR BUSINESS?

By
Ralph V. Pagano & Paul Tyson[1]

"There are two kinds of companies in the world: Those that have been hacked and know it, and those that have been hacked and don't."[2]

In April 2015, the FBI detained a prominent cybersecurity consultant after he claimed he hacked into an in-flight aircraft and issued commands to the engines.[3] He gained entry through the in-flight entertainment system and then accessed the airplane computer's nerve center where he could force commands such as activating the emergency passenger oxygen masks. In one such hack, he claims he overwrote code, enabling him to issue a climb command to an in-flight aircraft. The involved aircraft manufacturers dispute the legitimacy of the hacker's claims saying the entertainment systems are isolated from the flight navigation systems. Whether or not the consultant's claims were true, the FBI thought they were serious enough to question the consultant for several hours and seize some of his personal computing devices. After examining the consultant's thumb drives, the FBI discovered they were filled with malware that could be used to compromise computer networks.

Over the years, hackers have demonstrated their ability to breach and exploit nearly any institution, ranging from an

---

1 Many thanks to Los Angeles summer associate Jasmin Motlagh, Loyola Law School, for her assistance in preparing this article.

2 Popular saying in the cybersecurity industry, http://fortune.com/2015/03/20/corporate-hacking/

3 Justin Wm. Moyer, *Hacker Chris Roberts Told FBI He Took Control of United Plane, FBI Claims* (May 18, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/05/18/hacker-chris-roberts-told-fbi-he-took-control-of-united-plane-fbi-claims/.

individual's smart phone to the highest state secrets. With the great surge of cyber attacks, it is no surprise that in 2015 cyber attacks have been named as one of the top potential emerging threats and vulnerabilities of the U.S. financial system.[4]

Recent attacks on U.S. defense contractors illustrate that the aviation industry is another target for worldwide cyber hacking. In July 2014, a Chinese aviation technology company with an office in Canada, conspired with two unidentified individuals in China to hack into Boeing and Lockheed's computer networks. They were successful in stealing 65 gigabytes of data and trade secrets from the two U.S. companies, including confidential information on military projects related to the C-17 military cargo plane, the F-22 and F-35 fighter jets, and other aircraft.[5]

Cyber attacks have the capability to physically disrupt industries. In August 2012, cyber criminals attacked Aramco, Saudi Arabia's national oil company and one of the biggest suppliers of the world's oil, with the aim of stopping oil and gas production. Although it failed, it damaged 30,000 computers and was one of the most destructive cyber strikes conducted against a single business.[6] One can only imagine the impact on the world economy if the attacks had been successful.

While the headlines of cyber breach usually involve huge corporate and governmental entities (e.g., Target, Boeing, Wyndham Worldwide, United States Office of Personnel Management), the fact is small and midsize companies are major

---

4 Financial Stability Oversight Council, 2015 Annual Report, *available at* http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2015-Annual-Report.aspx.

5 *Id.* at 374; Edvard Pettersson, *Chinese Man Charged in Plot to Steal U.S. Military Data* (July 11, 2014, 9:01 PM), http://www.bloomberg.com/news/articles/2014-07-11/chinese-citizen-charged-with-hacking-boeing-computer-in-u-s-.

6 *Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow* (Dec. 9, 2012, 2:30 PM), http://www.reuters.com/article/2012/12/09/saudi-attack-idUSL5E8N91 UE20121209.

targets for hackers. Even if they do not have a substantial online presence, companies should be asking themselves: Am I at risk of a cyber attack? Have I taken proper precautions? Do I know what to do if I am hacked? Will my current insurance policy protect me if I am hacked? This article seeks to provide a general understanding of the threat that cybersecurity poses for businesses today, what companies can do to protect themselves both before and after a breach, and steps to ensure proper insurance coverage.

WHO GOES THERE?

Law enforcement agencies typically identify three major adversaries in the cyber crime world. Threat Level 1 is the individual hacker operating independently or maybe in a small group that typically takes on hacking for personal challenges or possibly some kind of activist activity (i.e., "hacktivists.") Typically, their activity leads to a nuisance but there is still capability to do great harm. Threat Level 2 consists of criminal organizations conducting more nefarious activities, e.g., identity theft, fraud, phishing scams, etc. Many of these organizations are located overseas so capturing them can be problematic. Threat Level 3 is foreign governments conducting state espionage, e.g., classified information, intellectual property and trade secrets. Some conduct this activity in secret while others are very open. A good example is the Chinese government's stealing of DuPont's intellectual property to produce titanium dioxide, a product used to whiten everyday objects. This theft resulted in at least one engineer being sentenced to 15 years in prison and $28 million in fines. The case generated over 19 terabytes of evidence.[7]

---

[7] Associated Press, *California Man Sentenced to 15 Years for Corporate Spying on DuPont* (July 2014), http://touch.latimes.com/#section/-1/article/p2p-80769812/.

It is important to note that despite the distinctions among the three threat levels, there is no distinction as to the amount of damage that any threat level actor can enact on an unsuspecting target. An individual hacker sitting in his basement alone who is willing to sell access to a foreign or criminal interest is functionally no different than a criminal organization or a foreign government conducting cyber warfare.

Assessing the Cost of a Cyber Attack

Corporate data breaches typically involve the theft of sensitive or confidential information, such as client records, trade secrets or financial records.[8] Even the personal data of employees can be a target for hackers. Regardless of the size of the breach, the resulting damage can be catastrophic. One study estimates the average global cost of a data breach is now $3.8 million, or about $154 per record lost or stolen.[9] Inevitably, companies can expect a data breach to also result in numerous individual and class action third-party liability claims.

Additional costs include compliance with state and federal notification laws. Presently, forty-seven states have enacted breach notification laws that require private or government entities who have experienced an unauthorized security breach to notify affected state residents, state agencies, consumer protection agencies and, in some instances, statewide media.[10] Complicating matters is the fact that under the current regulatory scheme, there

---

8 Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 Quinnipiac L. Rev. 369, 371-72 (2015).

9 Bill Rigby, *Cost of Data Breaches Increasing to Average of $3.8 million*, http://www.reuters.com/article/2015/05/27/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527 (May 27, 2015, 6:03 am EDT).

10 National Conference of State Legislatures, Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Only Alabama, New Mexico, and South Dakota have not instituted notification laws.

are no standard definitions for terms such as "breach," "protected information," and who has to notify affected persons.[11] Each state has unique and different requirements for how to handle notification to the harmed individuals, once a breach has occurred. Therefore, a company that maintains information for individuals or customers that reside in different states, could be facing a costly endeavor to comply with these state regulations.

Compliance with federal regulatory schemes is also a costly endeavor. As with state cybersecurity regulations, the scope and comprehensiveness of federal cybersecurity laws are varied. Individual agencies will tailor their regulations to specific industries (e.g., finance versus healthcare), but as of yet, there is no comprehensive federal law on the issue. In February 2015, President Obama met with top executives of Silicon Valley, Wall Street, and the federal government. The goal of this summit was to create awareness for comprehensive cybersecurity legislation and the need for companies to maintain a proactive approach towards ensuring their own cybersecurity.[12] The government also tasked the National Institute of Standards and Technology (NIST) for creating standards for companies to ensure the use of appropriate levels of cybersecurity to protect consumers and businesses.[13]

While NIST and other agencies develop these standards, other federal entities have taken strong actions to enforce tough cybersecurity practices. The FTC has become one of the most aggressive cybersecurity regulators in the federal government,

---

11 E.g., "protected information" under California law includes Social Security numbers (SSN), financial account numbers, and medical information; under New York law this will include SSN, driver's license, financial account numbers, passwords, mother's maiden name; under Texas law, this will include the same as New York, but also medical information, medical insurance, date of birth and electronic identification numbers.

12 Damian Paletta, *White House Cybersecurity Event to Draw Top Tech, Wall Street Execs* (Feb. 2015), http://www.wsj.com/articles/white-house-cybersecurity-event-to-draw-top-tech-wall-street-execs-1423659629

13 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

targeting major corporations, such as Google and AT&T, for enforcement actions related to cybersecurity.[14] These enforcement actions can result in significant fines and penalties, as when Google paid $22.5 million to settle the FTC's largest fine ever.[15] In addition to the assessment of fines, organizations accused by the FTC are exposed to consumer class actions and state level litigation for violations of specific state consumer protection laws.[16]

Many companies have started to recognize the responsibility to exercise good cybersecurity practices. Boards of directors are asking more difficult questions of CEO's and CIO's. Some companies are adding "cyber-seat" positions to their boards or adding specialized board advisors.[17] Often mergers and acquisitions firms require cybersecurity assessments of companies for potential investments.

---

14 Josh Bradford, *The FTC: What You Need to Know About One of the Most Relentless Federal Cyber Regulators* (June 3, 2015), http://www.advisenltd.com/2015/06/03/the-ftc/.

15 *Id*.

16 *Id*.

17 Paresh Dave, *Companies Hope Cybersecurity Experts in the Boardroom Can Counter Hacks* (Aug. 16, 2015), http://www.latimes.com/business/la-fi-cybersecurity-board-20150817-story.html.

PROTECTING AGAINST CYBERATTACKS

There is no one single method to protect against cyber attacks. The method and manner of attacks change year by year and hackers engage in more and more complicated tactics. Hackers can develop bot programs which search organizations for weak points and then attack, all of which is automated without the hacker monitoring the process. The use of asymmetrical attacks also complicates the protection of unsuspecting targets.[18] While the titans of industry and retail merchants are generally aware of the risk, small businesses and even non-profits have data that outside forces would like to access. As an example, local schools and universities contain a host of data on individuals that could be very valuable in the right hands.

Also complicating matters is the fact that most companies do not even know what assets they have at risk or what data they possess. They may be unaware of how many computers or servers they have, where they are all located, what is stored on them, or what other computer or machines those computers may have access to. As a result, it is extremely difficult to know whether those assets have been affected. A hacker can often get in and get out with very little indication that he was ever there until it is too late.

With the above in mind, here are some basic steps that every company should take to protect themselves:

1. Develop an information security policy.
2. Designate an individual responsible for your information security program

---

[18] In the Target hack of 2014, hackers did not gain access to Target's credit card database by hacking directly into Target's computer systems. Another company had been hired by Target to perform HVAC work on Target stores. This company was granted computer authorizations by Target so that it could install heating and cooling systems. The hackers took the credentials of the HVAC company and used them to gain access to Target.

3. Audit what personal information your business possesses, where it is and who has access to it.

4. Place reasonable restrictions (both physical and electronic) on access to personal information.

5. Ensure that third-party service providers have the capacity to protect personal information.[19]

The best way to get an understanding of the situation is to conduct frequent inventories and audits so that there is a continued awareness of data and assets that are at risk. Some questions to consider include the following: What kind of information do we have? Why do we have it? Where is it located? Who controls it? Why do they control it? Who else can access it? What would be the reaction to an accidental disclosure of this data? What kind of safeguards (physical, technical, administrative) do we have in place to protect it? Cybersecurity firms can be an invaluable resource in providing assistance with these evaluations and helping to create better protections. In the end, however, it is the individual company's own vigilance that will be the most effective method to prevent a cyber attack.

WE'VE BEEN HACKED!

If the unthinkable does happen, companies should take certain steps immediately to ensure that the breach is effectively stopped, mitigated, and that the appropriate people are notified.

1. *Identification of the Breach*: This can often be the most difficult problem in a data breach. Hackers often infiltrate a company and escape without anyone being alerted until months, sometimes years, later. Another popular method of hacking is the creation of back door entrances that let hackers come back at

---

[19] Christopher E. Hart, *Data Breach Response: Avoiding Pitfalls and Protecting Your Company, Clients and Customers* (Webinar, June 25, 2015).

a future time. Therefore, it will be imperative to determine if an incident has occurred, when it occurred, how it occurred, whether the intrusion has been definitively stopped, and then hope it is possible to determine the perpetrators.

2. *Response Resources Should Be Identified and Contracted Pre-Breach*: When the house is on fire is not the time to realize you did not fill the fire extinguishers. Failure to identify and contract response resources before a breach has occurred may cause a catastrophic delay in response. Insurance providers may already have identified forensic experts to help with these issues, but the time to figure that out is not after a breach has occurred.

3. *Who/What/When of Deadline Notification*: It will be imperative to quickly determine who needs to be notified and when. State and federal guidelines vary on this matter so ensuring that legal counsel, who is knowledgeable of the requirements is involved early on, will be essential. Failure to comply with notification laws can be very costly.

4. *Training*: There is no telling when a breach will occur. Sometimes the breach has been around for a substantial period of time, yet never detected. Key personnel must be ready to act and react when called upon. Additionally, employees must be trained on proper storage and handling protocols, as well as following good practices when accessing email and downloading programs off the internet.

5. *Using Outside Sources to Monitor*: The use of outside companies to monitor and evaluate breaches and implement remedial measures is often the best

way to get honest assessments of risk and setting up preventative measures.[20]

Insuring Against the Inevitable

The rise in frequency and economic cost of cyber attacks has spurred increased interest in cybersecurity insurance policies. Companies are increasingly turning to these novel insurance policies to mitigate the harsh aftermath of a data breach. A recent study revealed that almost one third of companies currently have cyber insurance policies and over half the companies that do not have policies plan on purchasing one in the future.[21]

Cyber insurance policies emerged a little over a decade ago and are continuously evolving in order to meet the demands of the rapidly advancing cyber crime market.[22] Consequently, there is no standard "one size fits all" policy that companies can purchase. Companies must understand the nature and extent of the risks they are facing to determine exactly what coverage is required.[23] While the terms of coverage may vary, the following discussion is about general coverage in the cybersecurity insurance industry. Companies should find out the specifics of their own coverage to make sure they are sufficiently protected.

Typically, cyber insurance falls into two general categories: first-party coverage and third-party coverage.[24] First-party coverage protects against the policy holder's own expenses and damages and can include, but is not limited to, funds for the

---

20 Hart, *supra* note 19.

21 John P. Mello, Jr., *Rise in Data Breaches Drives Interest in Cyber Insurance* (Aug. 15, 2013, 8:00 AM), http://www.csoonline.com/article/2133800/compliance/rise-in-data-breaches-drives-interest-in-cyber-insurance.html.

22 Mary K. Pratt, *Cyber Insurance Offers IT Peace of Mind—or Maybe Not* (Jan. 13, 2012, 6:00 AM), http://www.computerworld.com/article/2501281/security0/cyber-insurance-offers-it-peace-of-mind—-or-maybe-not.html.

23 *Id*.

24 *Id*.

following: (1) notification costs, (2) purchasing credit monitoring services for victims of the cyber attack, (3) public relations expenses associated with restoring the reputation of the company and appropriately communicating news of the cyber attack to customers and the public in order to limit lost business, (4) lost profits and other business interruption expenses following the cyber attack, (5) paying a cyber extortionist, (6) computer and data loss replacement or restoration costs, and (7) forensic investigation expenses associated with investigating the cause and scope of the breach.[25] Technically, breach response coverages (e.g., notification costs, crisis management, forensic expenses, credit monitoring) are not first-party coverage because they do not make up the loss of the insured for his own property. They do, however, make the insured whole against costs they may be legally or ethically required to take care of and this is not really a first-party issue.

Third-party coverage insures for the liability of the policyholder to third parties arising from a cyber attack.[26] Available third-party coverage includes the following: (1) costs associated with defending your company from civil suits by customers, business partners, and shareholders, and the resulting settlements or judgments that may be entered against you and (2) costs associated with defending your company from regulatory or administrative agency investigations and prosecutions (i.e., the FTC) and the fines and penalties that may result.[27]

---

25 Brenna, *Third-Party Vs. First-Party Cyber Risk Insurance: Protect Your IT Firm Right* (June 13, 2013, 9:04), http://www.techinsurance.com/blog/cyber-liability/third-party-vs-first-party-cyber-risk-insurance/; Rick Grimes & Karen Kutger, *Cyber Coverage: The New 'Must-Have' in the Property & Casualty Portfolio?* (Mar. 15, 2010), *http://www.propertycasualty360.com/2010/03/15/cyber-coverage-the-new-must-have-in-the-property;* Podolak, *supra* note 8, at 374-75.

26 Pratt, *supra* note 22.

27 Brenna, *supra* note 25.

OBJECTIONS & MISCONCEPTIONS

Even with the publicity of the recent high profile cyber crime and data breaches worldwide, which has brought the issues associated with cyber risk into sharp focus, many U.S. companies are not buying cyber risk insurance. Experts have offered several explanations for this lack of wide-spread adoption, including the slow economy, confusion about how these policies work, lack of awareness about their exposure to a breach, the view that their company is too small to need coverage, belief that they already have a secure system, and the assumption that an existing insurance policy will cover them in the event of a cyber attack.[28] However, these common objections are troubling as they are often inaccurate and misleading.

A. Misconception #1: Small Companies Are Not Targets

Small and medium-sized businesses are just as susceptible to cyber attacks as are large companies and government agencies.[29] A single newsstand operator was hacked when someone installed a skimmer on his debit/credit card reader. The hack cost him $26,000 to resolve the breach. One study revealed that out of 855 data breaches examined, 71% occurred in businesses with fewer than 100 employees.[30] Another statistic states that one in five small businesses falls victim to cyber crime each year.[31]

Unfortunately, there is a false sense of security among small businesses and that might be one of the reasons they may

---

28 *Id*.

29 Mike Pugh, *No, Your Small Business is not Safe From Cyber Attacks* (Oct. 25, 2013, 7:00 PM), http://www.huffingtonpost.com/mike-pugh/no-your-small-business-is_b_4164015.html.

30 Cheryl Conner, *Are You Prepared? Record Number of Cyber Attacks Target Small Business* (Sept. 14, 2013, 11:45 AM), http://www.forbes.com/sites/cherylsnappconner/2013/09/14/are-you-prepared-71-of-cyber-attacks-hit-small-business/.

31 Pugh, *supra* note 29.

take less care to protect themselves, thereby increasing their chances of becoming a target.[32] As a result, smaller businesses generally have less sophisticated cybersecurity and data-protection protocols, making them more vulnerable targets.[33] Also, hackers can use the credentials granted to smaller businesses to gain access to larger businesses.[34]

B. Misconception #2: A Secure System is Enough Protection

While some of the risks associated with IT security are due to software or system vulnerabilities, the "human factor" is often the leading cause of data breaches.[35] A 2014 study revealed that globally, 59% of all breaches are caused by some form of human error.[36] It has been estimated that 36% of all intrusions are generated by employees' negligence or ignorance of security rules and inappropriate use of personal data or company files.[37] Inadvertently clinking on a malicious link in an email or unknowingly downloading infected software, can allow hackers to take over your organization's computers, gather confidential information, and then resell it to parties around the world.[38]

C. Misconception #3: Cyber Insurance Policy Provides Adequate Protection

The biggest misconception that companies have is the false assumption that an existing insurance policy will provide

---

32 *Id*.

33 *Id*.

34 *Id*. E.g., the hacking of Target (http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/)

35 *#Cyber-Attacks: Are Employees the Weakest Link in Security?* (May 5, 2015), http://blog.econocom.com/en/blog/cyber-attacks-are-employees-the-weakest-link-in-security/.

36 Podolak, *supra* note 8, at 372.

37 #Cyber-Attacks, *supra* note 35.

38 Sherri E. Davidoff, *How Attorneys Get Hacked (And What You Can do About it)*, Montana Lawyer, May 2014, at 25.

coverage in the event of a cyber related incident. The majority of businesses purchase commercial general liability (CGL) insurance for coverage related to possible future losses, such as damages caused to third parties as a result of company negligence.[39] However, there is a limit as to what type of damages a CGL policy will cover as there are several coverage gaps present in general liability insurance policies that preclude recovery for losses incurred as a result of data breaches.[40] This coverage gap creates a problematic barrier for companies who have suffered intangible losses as a result of data breaches.[41]

Furthermore, today's CGL policies typically cover damages as a result of "bodily injury" or "property damage."[42] Since "bodily injury" is unlikely to be present in a cyber-related incident, an organization's ability to obtain coverage under their CGL policy really hinges on the interpretation of "property damage."[43] For more than twenty years, courts have struggled to come to grips with the question of whether electronic data is considered tangible property in order to determine whether coverage exists for loss of (or damage to) data under CGL policies. To preemptively avoid these types of ambiguities, insurance companies have recently been tightening up their CGL policies by specifically excluding data breaches and security compromises.[44]

---

39 Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 269 (2012).

40 *Id*. at 270.

41 *Id*.

42 *Id*.

43 *Id*.

44 Mello, *supra* note 21.

A recent legal dispute between Sony Corporation and Zurich American Insurance Co. served as a glaring warning to companies that they cannot blindly rely on their CGL policies to cover damages and expenses arising from cybersecurity incidents.[45] The dispute began in 2011 after data breaches at Sony exposed account data on close to 100 million individuals and information on over 12 million credit and debit cards.[46] As Sony turned to Zurich for assistance with coverage, Zurich turned to the New York State Supreme Court to absolve it of any responsibility for defending or indemnifying Sony against claims arising from the data breaches.[47]

Zurich claimed that the CGL insurance policy that it had with Sony only covered "bodily injury" and "property damage" caused by occurrences other than the kind of cyberattacks Sony experienced.[48] The Supreme Court of the State of New York agreed with Zurich's position and granted summary judgment in its favor.[49] This decision highlights the dangers that a company faces when it depends on its traditional CGL policy to protect it in the event of a data breach.

---

45 Jaikumar Vijayan, *Zurich Lawsuit Against Sony Highlights Cyber Insurance Shortcomings* (July 26, 2011, 7:00 AM), http://www.computerworld.com/article/2509419/disaster-recovery/zurich-lawsuit-against-sony-highlights-cyber-insurance-shortcomings.html; *See also* Jaikumar Vijayan, *Insurer Says It's Not Liable for University of Utah's $3.3M Data Breach* (June 4, 2010, 9:12 PM), http://www.computerworld.com/article/2518592/data-security/insurer-says-it-s-not-liable-for-university-of-utah-s—3-3m-data-breach.html (Colorado Casualty Insurance Co. sought declaratory judgment from Utah federal court contending that it was not obligated to reimburse it's insured, the University of Utah, for $3.3 million in costs it suffered after a data breach).

46 Vijayan, *supra* note 45.

47 *Id*.

48 *Id*.

49 Young Ha, *N.Y. Court: Zurich not Obligated to Defend Sony Units in Data Breach Litigation* (Mar. 17, 2014), http://www.insurancejournal.com/news/east/2014/03/17/323551.htm.

What to Consider When Purchasing Coverage

Despite the spike in interest, cyber insurance policies are still relatively novel and undeveloped. All cyber policies are not created equal and there are certain guidelines that a company should consider when it finally decides to add seek out protection.

A. Risk Assessment

The first step in buying cyber insurance is to perform a comprehensive data security risk assessment in order to identify the extent of the risks facing your company. If a company does not have an accurate understanding of its potential exposure, it won't be in the best position to consider the type and amount of insurance coverage that it requires to adequately protect itself.[50] Moreover, many insurance companies require an analysis of what security measures exist in order to help determine premiums.[51] Things to consider are: (1) what information is maintained and how is it protected; (2) what is the nature and extent of a company's system security; (3) are transactions conducted over the internet; (4) to what extent are machines and manufacturing processes at risk from a hack; and (5) are any customers or employees at risk of physical harm as a result of a hack. Hiring a third party to perform the risk assessment can help a company fully identify its security risks, and some insurers require a third-party audit.[52] Even if a company conducts a risk assessment and then ultimately decides not to purchase the insurance, it is a valuable educational experience that can provide insight into the company's vulnerability and exposure to cyber attacks.

---

50 Pratt, *supra* note 22.

51 *Id*.

52 *Id*.

B. Accurate Representations

Inaccurate representations, whether made intentionally or unintentionally, can lead to an unanticipated forfeiture of coverage in the future.[53] Insurers include language in their agreements that undoubtedly express this warning. For instance, a Travelers' cyber risk insurance agreement contains the following provision: "If any statement or representation in the application is untrue, then no coverage will be afforded under this CyberRisk Policy."[54]

C. Retroactive Coverage

Companies should request "retroactive coverage" for prior, unknown breaches when negotiating a cyber insurance policy. Most cyber policies only provide coverage for breaches that occur after a specified "retroactive date," such as the inception date of the policy.[55] Many cyber breaches go undiscovered for quite some time before any claims are made, so requesting a retroactive date that is earlier than the inception date will ensure coverage for unknown breaches.[56]

D. Exclusions

Exclusions might be the most important thing companies should be aware of. Cyber insurance policies often contain broad exclusions that can completely contradict the insured's purpose for purchasing the coverage. The policy wording needs to clearly convey what the insured is actually going to be covered for in the event of an incident. Otherwise, a company might be left in the dark because the language in their cyber policy does not require the insurer to get involved.

---

53 Podolak, *supra* note 8, at 406.

54 *Id.* at 406-07.

55 Jay Shelton, *10 Tips for Buying Cyber Insurance* (Sept. 25, 2014), http://www.assuranceagency.com/blog-post/10-tips-for-buying-cyber-insurance.

56 *Id*.

A May 2015 decision from a federal district court in Utah demonstrates that just because a company has cyber insurance does not mean that an insurer is going to cover all cyber-related claims. In *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs. Inc*,[57] an insurance company sought a declaration of no coverage when one of its insureds sought coverage after being sued over a data-related dispute. The insured's cyber policy protected against any *"error, omission or negligent act."*[58] ultimately, the court decided that the cyber policy did not cover the underlying claims because all the allegations sounded in intentional and willful conduct of the policyholder, not neglect.

Another recent lawsuit highlights the importance of clear wording in a policy. On May 7, 2015, Columbia Casualty Insurance Company filed a lawsuit against its insured to recoup the settlement funds and defense costs that it provided for a privacy class action under a cyber insurance policy.[59] The policy had a coverage exclusion requiring that the insured meet certain "minimum required practices" and if the insured failed to continuously implement such procedures, coverage would be eliminated.[60] Columbia alleged that the insured failed to follow the minimum required practices and failed to provide complete and accurate information in the application, thereby forfeiting coverage.[61]

While there is a risk that a company having a cyber policy could find itself in a precarious situation if a "minimum required practices" exclusion is contained in the policy, a company should

---

57 No. 2:14-CV-170 TS, 2015 WL 2201797 (D. Utah May 11, 2015)

58 *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs. Inc.*, No. 2:14-CV-170 TS, 2015 WL 2201797, at *1 (D. Utah May 11, 2015).

59 Complaint for Declaratory Judgment and Reimbursement at 1, *Columbia Cas. Co. v. Cottage Health Sys*., (No. 2:15-cv-03432)d, 2015 WL 3751196 (C.D. Cal. 2015).

60 Complaint for Declaratory Judgment and Reimbursement, *supra* note 59, at 4.

61 Complaint for Declaratory Judgment and Reimbursement, *supra* note 59, at 11-15.

always exercise prudence and diligence before making security representations in their applications. As with all cybersecurity issues, the most effective way a company can protect itself is to stay involved and vigilant.

CONCLUSION

As this article demonstrates, there are many cybersecurity threats and companies need to take to steps to counter those threats and to protect themselves. The reality is that these are just the tip of the iceberg. Cybersecurity is an issue that affects all businesses, not just the government or online retailers. In today's world, data (also known as "information") is power. The world is full of bad actors that will do anything to gain access to a company's data, including trade secrets, intellectual property, employee and customer information, or even to commit sabotage. Companies need to be proactive in protecting themselves not only in the digital world, but in the legal and insurance worlds as well.

USE OF VIDEOCONFERENCING TECHNOLOGY TO GLOBALIZE U.S. LITIGATION

By
Stephanie B. Gonzalez

It is well recognized that foreign claimants routinely file lawsuits in the United States, hoping to receive the type of substantial jury verdicts for which the U.S. justice system has become infamous. As long as the defendant is a U.S. corporation or has significant ties with the U.S., these lawsuits often survive jurisdictional and forum *non conveniens* challenges. However, an issue that arises in the context of such international litigation is that key evidence and witnesses are often located abroad, making the discovery process challenging and expensive for all parties. This can be problematic at the trial stage, where the litigants often find themselves needing to present the testimony of a key foreign witness who may be unwilling or unable to travel to the U.S. for trial.

A seemingly simple solution would be to transmit the live testimony of an "unavailable" foreign witness via videoconference from the remote location. However, despite the increased reliability and availability of modern-day videoconferencing technology, this remains a somewhat disfavored practice in U.S. courtrooms, and a party seeking to present remote testimony faces significant legal hurdles. Even where a U.S. court allows remote video testimony by a witness abroad, compliance with international law presents yet another obstacle to be overcome.

Instead, common practice for decades has been to take deposition testimony of witnesses unable to appear live in the courtroom, and to present that pre-recorded testimony to jurors during trial. However, it is becoming apparent to courts and litigants that the contemporaneous transmission of live testimony can be a more effective method of presenting testimony to the jury. As a result, parties to international litigation would benefit from

updated rules allowing greater use of videoconferencing technology as an effective means of bringing important foreign witnesses into U.S. courtrooms.

I. *U.S. Law Governing Remote Testimony at Trial*

Federal Rule of Civil Procedure 43 was amended in 1996, almost twenty years ago, to allow "testimony in open court by contemporaneous transmission from a different location."[1] This rule specifies that such testimony should only be permitted "[f]or good cause in compelling circumstances and with appropriate safeguards." In essence, the decision of whether to allow a remote witness to testify by contemporaneous transmission rests within the sound discretion of the trial judge. Not surprisingly, courts around the country have reached different results regarding what constitute "compelling circumstances" sufficient to justify remote testimony, and what safeguards are considered "appropriate" to protect the sanctity of trial testimony.

A. Good Cause in Compelling Circumstances

Twenty years ago, the Advisory Committee to Rule 43 conveyed a very conservative view of what would be considered "compelling circumstances" justifying contemporaneous transmission of remote testimony.[2] Specifically, the Committee made it clear that foreseeable difficulty in attending trial, such as the witness living far away from the courthouse, is not a sufficient reason to allow video testimony.

However, as videoconferencing technology has improved and become more commonplace in our society, courts seem to be moving away from this conservative approach. In *In re Actos (Pioglitazone) Products Liab. Litig.*, a federal court in Louisiana permitted plaintiffs, who were a part of a complex multi-party, multidistrict litigation, to present live videoconference testimony of

---

1 Fed. R. Civ. P. 43(a).

2 *Id*. at advisory committee's notes.

several remote witnesses during trial, recognizing that "as technology has continued to evolve, so have the applicable rules."[3] Similarly, in *F.T.C. v. Swedish Match N. Am., Inc.*, a District of Columbia court permitted the plaintiff to present the live video testimony of a remote witness, explaining, "the Advisory Committee Notes to Federal Rule 43(a) . . . are more hostile than I am to live video transmission. I suggest, however, that the courts are much more receptive to this new technology than the Advisory Committee."[4]

In fact, several courts have found that the restrictions of international travel can provide good cause for contemporaneous transmission of a foreign witness's testimony. In *Lopez v. NTI, LLC*, a federal court in Maryland permitted plaintiffs located in Honduras to testify at trial via videoconference, noting that there is a growing trend to allow remote videoconferencing in civil actions.[5] The court sympathized with plaintiffs: "When viable alternatives like videoconferencing are available, compelling individuals who make no more than $7,000 a year to travel hundreds of miles seems fundamentally unjust." In *Angamarca v. Da Ciro, Inc*., a New York district court found that "the legal infeasibility of attending a deposition or trial in person because of one's immigration status rises to the level of compelling circumstances."[6]

---

3 No. 12-CV-00064, 2014 WL 107153, at *10 (W.D. La. Jan. 8, 2014).

4 197 F.R.D. 1, 2 (D.D.C. 2000).

5 748 F.Supp.2d 471, 480 (D. Md. 2010); *see also Dagen v. CFC Group Holdings*, 00-CV-5682, 2003 WL 22533425, at *2 (S.D.N.Y. Nov. 7, 2003).

6 303 F.R.D. 445, 447 (S.D.N.Y. 2012).

However, other courts continue to follow the conservative approach espoused two decades ago by the Advisory Committee to the federal rules. In *Sec. & Exch. Comm'n v. Yang*, the Northern District of Illinois denied a motion to present the testimony of three Chinese witnesses by videoconference during trial, despite the fact that the witnesses could not obtain visas to travel to the United States due to financial hardship.[7] The court held that the witnesses' reasons for being unable to appear at trial were foreseeable at the beginning stages of the litigation, which "should have spurred defendants to take the appropriate steps to take and preserve their testimony far sooner than the eve of trial." Similarly, in *Rodriguez v. SGLC, Inc.,* a federal court in California denied the request of plaintiffs residing in Mexico to present their testimony via videoconference, despite the difficulties they faced obtaining visas to travel to the U.S., as such circumstances were "foreseeable."[8]

B. Appropriate Safeguards

The Advisory Committee to the federal rules advises that, in order to properly admit contemporaneous transmission of remote testimony, "[s]afeguards must be adopted that ensure accurate identification of the witness and that protect against influence by persons present with the witness. Accurate transmission likewise must be assured."[9] Courts have contemplated additional safeguards such as ensuring the opposing party's ability to cross-examine the witness, and the fact-finder's ability to assess the credibility of the witness. In *Warner v. Cate*, a California district court found that, "[a]ppropriate safeguards exist where the opposing party's ability to conduct cross-examination is not impaired, the witness testifies under oath in open court, and the witness's credibility can be assessed adequately."[10] Similarly, in

---

7 No. 12-C-2473, 2014 WL 1303457, at *6 (N.D. Ill. Mar. 31, 2014).

8 08-CV-01971, 2012 WL 3704922 (E.D. Cal. Aug. 24, 2012).

9 Fed. R. Civ. P. 43 advisory committee's note.

10 No. 12-CV-1146, 2015 WL 4645019, at *1 (E.D. Cal. Aug. 4, 2015).

Lopez, the Maryland court found that videoconference testimony would not prejudice the opposing party where "[e]ach of the witnesses will testify in open court, under oath, and will face cross-examination."[11]

i. Oath and Penalty of Perjury

It is well accepted that a remote witness located within the U.S. can be placed under oath by the courtroom deputy via video.[12] However, where the witness is located in a foreign country, the seemingly simple act of taking the oath becomes more complicated, and is usually governed by local laws, as well as treaties and bilateral agreements. For example, Germany and France both require government pre-approval for taking sworn testimony, and require a U.S. consular officer to administer the oath.[13] Germany requires that the oath and testimony be given on U.S. consulate grounds, whereas France does not permit testimony to take place on consulate grounds for security reasons.[14] (To ensure compliance with local procedures and any bilateral agreements with the U.S., litigants are encouraged to consult the U.S. Department of State for judicial assistance,[15] as well as the U.S. Embassy for the specific country from which the evidence is sought).

---

11 748 F.Supp.2d at 480.

12 *See, e.g., In re Actos, 2014 WL 107153* at *13 (instructing that "the courtroom deputy in Lafayette [courtroom location] will administer the oath to the [remote] witness.").

13 U.S. Consulate General, *Deposition at the U.S. Consulate General Frankfurt Am Main, Germany,* at http://germany.usembassy.gov/english-speaking-services/2008-deposition-instructions.pdf (last visited August 14, 2015); *Taking Evidence in France in Civil and Commercial Matters*, at http://france.usembassy.gov/judicial.html (last visited August 17, 2015).

14 *Id*.

15 http://travel.state.gov/content/travel/english/legal-considerations/judicial/country.html (last visited August 14, 2015).

Even when the oath is administered in accordance with international protocol, there is a question as to whether the remote testimony is truly sworn where the foreign witness is not subject to prosecution for perjury. Under U.S. law, a witness can be prosecuted for perjury whether the false statement is made inside or outside the U.S.[16] Because perjury is a crime of moral turpitude,[17] a witness who perjures himself in a foreign country may be extradited to the U.S. for prosecution where there is an extradition treaty with that country. In *Harrell v. State*, a criminal case heard in Florida, the court stated:

> [t]o ensure that the possibility of perjury is not an empty threat for those witnesses that testify via satellite from outside the United States, it must be established that there exists an extradition treaty between the witness's country and the United States, and that such a treaty permits extradition for the crime of perjury.[18]

In that case, there was an extradition treaty between the U.S. and Argentina which listed "[f]alse statements, accusations or testimony effected before a government agency or official," as one of the extraditable offenses. As a result, the court held that the oath taken by the foreign witness was valid. In *U.S. v. Oudovenko*, a New York court declined to allow the contemporaneous transmission of testimony by foreign nationals located in Russia, in part because there was no extradition treaty with Russia:

> [E]ven if the witnesses in this case are placed under oath, the significance of that oath is diminished because there is no realistic perjury sanction. An oath to tell the truth, in whatever form, is designed to 'awaken the witness' conscience and impress the witness' mind with the duty' to

---

16 18 U.S.C. § 1621 (1994).

17 *U.S. v. Carrollo*, 30 F.Supp. 3 (W.D. Mo. 1939).

18 709 So.2d 1364, 1371 (Fla. 1998).

> tell the truth. But that impression is difficult to make when the witness is beyond the reach of the court.[19]

However, in the later case of *El-Hadad v. United Arab Emirates*, a District of Columbia court declined to apply the reasoning from *Harrell* and *Oudovenko*, and admitted the sworn testimony of a foreign national from the United Arab Emirates, despite the lack of an extradition treaty with the U.S.[20] In *U.S. v. Cooper*, the District of Columbia found that the oath was valid where the foreign witness could be prosecuted for committing perjury under local law, and did not consider whether there was an extradition treaty with the U.S.[21]

Importantly, if the witness testifying from abroad is a U.S. citizen or resident, federal courts have the power under the Walsh Act to order their return to the U.S. for prosecution for perjury.[22] If the witness fails to comply with the subpoena, he or she can be held in contempt of court, at which point the court can seize any property that person has within the U.S., and sell the seized property to satisfy a fine.[23] Additionally, the witness risks being prosecuted for perjury if he or she ever attempts to return to the U.S. As a result, remote testimony given by a U.S. citizen or resident under oath will always be under penalty of perjury.

II. *Can a Foreign Witness be Compelled to Provide Remote Testimony via Videoconference?*

Where a U.S. court is receptive to the use of videoconferencing technology to contemporaneously transmit the

---

19 00-CR-1014, 2001 WL 253027, at *3 (E.D.N.Y. March 7, 2001).

20 496 F.3d 658, 669 (D.C. Cir. 2007).

21 947 F.Supp.2d 108, 115 (D.D.C. 2013).

22 28 U.S.C. § 1783; *see U.S. v. Thompson*, 319 F.2d 665 (2nd Cir. 1963) (recognizing that the "Walsh Act" authorizes the issuance of subpoenas in criminal proceedings to witnesses outside the U.S.).

23 28 U.S.C. § 1784 (1964).

testimony of a witness located abroad, can that witness be compelled to appear via video? The short answer is, maybe.

Under Federal Rule of Civil Procedure 45, a federal court has the power to subpoena a U.S. citizen or resident located in a foreign country to appear "as a witness before it," upon tender of the necessary travel expenses.[24] In *Wultz v. Bank of China*, a New York district court used its Rule 45 subpoena power to compel a non-party Israeli bank to provide testimony via videoconference from Israel, where the bank had a branch office in New York and therefore was within the court's domestic subpoena range (limited to within the state where the trial is held, or 100 miles from the witness's residence).[25] In *In re Actos*, a Louisiana federal court went a step further, and used its subpoena power to compel a U.S. witness located beyond the court's domestic subpoena range to appear via videoconference at trial.[26]

If the U.S. court agrees to subpoena a U.S. citizen or resident abroad to appear via videoconference at trial, litigants must be mindful not to violate any local law of the foreign country in doing so. For instance, in Germany, testimony must be fully voluntary and pre-approved by the German Ministry of Justice, regardless of the witness's citizenship, otherwise the participants may face criminal penalties.[27]

If the witness is a foreign national, the ability to compel them to appear "in open court" in the U.S. is much more attenuated, and in most cases nonexistent. The U.S. and 57 other

---

24 Fed. R. Civ. P. 45; 28 U.S.C. § 1783.

25 298 F.R.D. 91 (S.D.N.Y. 2014).

26 2014 WL 107153 at *9; *but see Ping-Kuo Lin v. Horan Capital Management, LLC*, 14-CV-5202, 2014 WL 3974585, at *2 (S.D.N.Y. Aug. 13, 2014) (holding that videoconferencing technology does not operate to expand the reach of the court beyond its statutory subpoena range).

27 U.S. Department of State, *Judicial Assistance Germany*, at http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/germany.html (last visited August 17, 2015).

States are signatories to the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("the Hague Evidence Convention"), entered into force in 1972, which was brought about to supply a "model system that bridges the gap" between civil and common law State procedures when a trial takes place in one State but evidence is located in another.[28] The Hague Evidence Convention specifies that the State responding to a request for evidence "shall apply the appropriate measures of compulsion in the instances and to the same extent as are provided by its internal law."[29] As a result, the Hague Evidence Convention does not provide an effective means for compelling testimony of a foreign witness beyond the local law of the contracting State.

Even more problematic is that the Hague Evidence Convention, which is now over forty years old, does not provide procedures for taking live testimony of a foreign witness at all, much less contemplate the use of videoconferencing technology. Examination of a witness abroad must be done in writing, and through the onerous "letters of request" process, requiring involvement of the foreign state's "central authority" and judicial authority. The burdensome nature of these procedures led to the U.S. Supreme Court decision of *Societe Nationale Industrielle Aerospatiale v. U.S. D. for the S. Dist. of IA*, which states that parties to U.S. litigation have the discretion to use the procedures set forth in the Federal Rules of Civil Procedure rather than the Hague Evidence Convention.[30]

Some signatories to the Hague Evidence Convention, such as Singapore and Australia, have, like the U.S., enacted

---

[28] Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Evidence Convention"), Mar. 18, 1970, 23 U.S.T. § 2555, 28 U.S.C. § 1781; Letter of Submittal from Secretary of State William P. Rogers to the President Regarding the Evidence Convention, S. EXEC. DOC.A., at V, 92d. Cong., 2d Sess. (Feb. 1, 1972), *reprinted in* 12 INT'L LEGAL MATERIALS 324 (1973).

[29] Hague Evidence Convention, Art. 10.

[30] 482 U.S. 522 (1987).

domestic laws allowing live transmission of remote testimony, and have video-conferencing facilities in their courtrooms.[31] As long as both U.S. law and local law are complied with, it may be possible to bypass the Hague Evidence Convention entirely and compel a foreign national located in these countries to testify in a U.S. court via videoconference. However, other signatory States are staunch observers of the Hague Evidence Convention, and require use of formal procedures to obtain testimonial evidence within their borders. For instance, in Argentina, a willing witness cannot provide voluntary testimony, unless a formal request is made under the Hague Evidence Convention.[32]

III. *How is Testimony Best Presented? In-Person, Remote Video, or Deposition*

Where a foreign witness is available and willing to travel to the U.S. for trial, for a variety of reasons it is unquestionably preferable for the court and litigants that the witness appear live at trial to testify. In fact, the Advisory Committee to Rule 43 notes:

> The importance of presenting live testimony in court cannot be forgotten. The very ceremony of trial and the presence of the factfinder may exert a powerful force for truthtelling. The opportunity to judge the demeanor of a witness face-to-face is accorded great value in our tradition.[33]

---

31 Martin Davies, *Bypassing the Hague Evidence Convention: Private International Law Implication of the Use of Video and Audio Conferencing Technology in Transnational Litigation*, 55 Am. J. Comp. L. 205, 209 (2007).

32 U.S. Dept. of State, Judicial Assistance, at http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/argentina.html (last visited August 17, 2015).

33 Fed. R. Civ. P. 43, advisory committee's notes.

In *Thornton v. Snyder*, the Seventh Circuit court of appeal also expressed the sentiment that videoconference testimony is an imperfect replacement for live testimony:

> Virtual reality is rarely a substitute for actual presence and ... even in an age of advancing technology, watching an event on the screen remains less than the complete equivalent of actually attending it. The immediacy of a living person is lost with video technology .... Video conferencing ... is not the same as actual presence, and it is to be expected that the ability to observe demeanor, central to the fact-finding process, may be lessened in a particular case by video conferencing.[34]

But is there actually a difference in terms of impact of the testimony on jurors? Several years ago, researchers conducted an experiment in the context of a civil personal injury trial where the damages verdicts were dependent on the testimony of medical experts.[35] They found there was no significant difference in the verdict whether the experts were physically in the courtroom or appeared via videoconference from a remote location. Consistent with this finding, in *FTC v. Swedish Match N.A*., a District of Columbia judge took the minority view that, "there is no practical difference between live testimony and contemporaneous video transmission."[36] "To prefer live testimony over testimony by contemporaneous video transmission is to prefer irrationally one means of securing the witness's testimony which is exactly equal to the other."

Despite this, it seems unlikely that the majority of courts will ever view videoconference testimony as equal to live in-person testimony, if for no other reason than the logistics of presenting

---

34 428 F.3d 690, 697 (7th Cir. 2005).

35 Lederer, Fredric, *The Legality and Practicality of Remote Witness Testimony*, THE PRACTICAL LITIGATOR (2009).

36 197 F.R.D. at 2.

video testimony are inherently more complicated, difficult to control, and less reliable.

However, courts are starting to agree that live video testimony is preferable to the more traditional approach of presenting pre-recorded deposition testimony at trial. In *In re Vioxx Products Liability Litigation*, a Louisiana federal court stated, "the deposition is 'a substitute, a second-best, not to be used when the original is at hand' ... by allowing for contemporaneous transmission, the Court allows the jury to see the live witness along with 'his hesitation, his doubts, his variations of language, his confidence or precipitancy, his calmness or consideration,' and, thus, satisfies the goals of live, in-person testimony and avoids the short-comings of deposition testimony."[37] Similarly, in *U.S. v. Gigante*, the Second Circuit court of appeal upheld a trial judge's decision that "contemporaneous testimony via closed circuit televising affords greater protection of [the criminal defendant's] confrontation rights than would a deposition," finding that the live video testimony "forced [the witness] to testify before the jury, and allowed them to judge his credibility through his demeanor and comportment."[38] In *In re Actos*, the Court expressed a preference for videoconference testimony over deposition testimony based on efficiency, stating that it "likely would be substantially less expensive and faster, than use of video depositions when one considers not only the time and expense required to take the video depositions, but also the attorney time and expense inherent in identifying deposition excerpts, and the time required to make the necessary rulings by the Court on those objections, as well as the

---

[37] 439 F.Supp.2d 640, 644 (E.D.LA 2006) (internal citations omitted); *see also Sallenger v. City of Springfield,* 03-CV-3093, 2008 WL 2705442, at *1 (C.D. Ill July 9, 2008) (videoconferencing "satisfies many of the goals of in-person testimony, while avoiding the shortcomings that accompany the reading of deposition testimony at trial.").

[38] 166 F.3d 75, 81 (2nd Cir. 1999).

time and expense of editing by a videographer after the rulings are made."[39]

In this regard, courts are moving beyond the outdated guidance provided by the federal rules, which twenty years ago stated that, "[o]rdinarily depositions, including video depositions, provide a superior means of securing the testimony of a witness who is beyond the reach of a trial subpoena."[40] Revising these guidelines to acknowledge that live videoconference testimony of a remote witness at trial can be preferable (and likely more cost-effective) than presentation of pre-recorded deposition testimony would likely be well received by the courts and litigants, and would have the potential to greatly improve the presentation of testimony at trial.

IV. ***Case Study from Recent Fitzpatrick & Hunt Trial***

In recent litigation arising from the crash of a Black Hawk helicopter overseas, which we defended through verdict in a month-long trial in federal court, we were able to present the live testimony at trial of a key witness located in the United Arab Emirates via videoconference. The witness was a U.S. citizen residing abroad, who was unavailable to travel to the U.S. for trial due to his work schedule and the considerable travel time involved. Plaintiffs strenuously objected to the remote testimony, arguing that an oath given remotely from the courtroom in Texas would have no effect, and that use of videoconferencing technology might impede their ability to effectively cross-examine the witness and lead to a mistrial. The judge granted our request to present the remote testimony, provided that the witness waive his right to contest jurisdiction for prosecution for perjury, which he did, and provided that no one was in the room with the witness during his testimony.

---

39 2014 WL 107153 at *7.

40 Fed. R. Civ. P. 43, advisory committee's notes.

The live video testimony by this witness was very compelling. A two-way monitor set up on the witness stand projected a life-size image of the witness to the jury. The witness was able to interact with the judge and attorneys, and could see documents projected in the courtroom in order to effectively testify about their contents. The jury was clearly engaged with this witness and attentive to his testimony.

This was in stark contrast to the presentation by both sides of excerpted pre-recorded video deposition testimony of other "unavailable" witnesses. The testimony itself, which in some instances was taken years in advance of trial, was not necessarily tailored to the evidence actually presented at trial, and was often disjointed due to edits by the parties and judge (after ruling on objections) in advance of trial. Furthermore, with the lights dimmed and no one in the courtroom speaking, the judge and jurors sometimes appeared to lose focus.

V. *Conclusion*

What we learned from the recent trial, and what courts are increasingly acknowledging, is that use of modern videoconferencing technology to present remote testimony of a key foreign witness can be an extremely effective alternative to in-person testimony (when such testimony is not possible), and is a more compelling method of presentation to a jury than the more traditional approach of playing or reading pre-recorded and edited deposition testimony. As a result, the federal rules should be updated to more freely permit use of modern technology to transmit live remote testimony at trial.

Similarly, the Hague Evidence Convention is critically in need of updating to provide international protocols for contemporaneous transmission of live testimony between contracting States. Specifically, it should provide a means for compelling a foreign witness to appear live to testify via videoconference, and should specify when and how an effective

oath can be administered. There is no telling which countries would sign on to such an amendment, but for those willing to participate it would provide uniform guidance for the cross-border presentation of videoconference testimony, rather than the piecemeal regulations that have grown into the void left by the outdated Hague Evidence Convention.

Aircraft Builders Council, Inc.