Published by the Federal Bar Association Transportation and Transportation Security Law Section

Fall 2017

TransLaw

Chair's Corner

Lisa A. Harig, Chair of the Transportation and Transportation Security Law Section

The Transportation and Transportation Security Law Section is off to a great start for the 2017-2018 year! We celebrated the annual Chief Counsel's Reception on October 26, 2017. This year, we honored Thomas W. Anderson, former General Counsel for the Minneapolis-St. Paul Metropolitan Airports Commission, as the John T. Stewart Transportation Lawyer of the Year, and Kevin G. Houlihan, Assistant Chief Counsel for Transportation Security Litigation at TSA, as the John T. Stewart Transportation Security Lawyer of the Year. Look for a more complete salute to the achievements of each of these outstanding lawyers, as well as pictures from the reception, in the next issue of TransLaw.

In this issue, we have a memorial for former TTSL Chair Frank Duggan, who passed away in November 2017. There is also a case summary by Jacob Spegal and Thomas Lehrich on the Third Circuit's decision on maritime subject-matter jurisdiction. We have an article by Allison Skopec on Blockchain technology, the next step beyond Bitcoin and potentially revolutionary for the transportation logistics industry. Finally, Michael Bahar contributed an article on marine cybersecurity.

I'd like to take this opportunity to thank Immediate Past Chair Kathy Gainey for her strong leadership over the past year. Kathy has been an active TTSL member for many years and we look forward to her continued participation and guidance in her role as Immediate Past Chair.

The Section will be holding its annual Holiday Happy Hour in the coming weeks – look for the announcement via email, as well as on the FBA website, LinkedIn, and Twitter. We hope to see many DC-area members there!

I look forward to the upcoming year. I encourage each of our members to actively participate in the Section by attending an event and/or authoring an article for TranLaw. If you have an idea for a program or article that you'd like to see, please contact one of the TTSL officers. ❖

The Section Remembers our Colleague Frank Duggan

Former Section Chair Frank Duggan died at the age of 79 in Alexandria, VA, on November 1, 2017. Frank served as Chair of the Section in 2005 while he headed the National Mediation Board.

Frank was particularly regarded in the aviation community for his contribution to the victims of Pan Am Flight 103. After the 1988 terrorist bombing of Flight 103, President George H.W. Bush appointed him to the Presidential Commission on Aviation Security and Terrorism.

Frank was born in Brooklyn, NY and moved to Washington after law school. He was a graduate of St. John's University's prep, college, and law school.

He served in United States Navy prior to law school, and upon graduating from law school Frank worked in government positions for the U.S. Senate, the U.S. Department of the Treasury, and at the U.S. Department of Labor.

Frank also worked in industry spending 10 years at the Association of American Railroads.❖

Also In This Issue...

Board of Directors Slate for 2017-2018 ..... p. 2
Thrid Circuit Address Maritime Jurisdiction Involving a Brawl on a Vessel: Case Summary ..... p. 3
The Shock of the New: Blockchain Technology, Logistics, and the Building Blocks of Multi-Modulism's Not-So-Distant Future ..... p. 4
The High Stakes, High Seas Cyber Peril ..... p. 8

Who's Who

UNITED STATES DEPARTMENT OF TRANSPORTATION

OFFICE OF THE SECRETARY OF TRANSPORTATION
Elaine L. Chao
Secretary of Transportation

Maria Lefevre
Executive Director, Office of the Under Secretary for Policy

Lana Hurdle
Deputy Assistant Secretary for Budget and Programs

Audrey Farley
Executive Director, Office of Research and Technology

OFFICE OF THE GENERAL COUNSEL

Judith S. Kaleta
Deputy General Counsel

FEDERAL AVIATION ADMINISTRATION
Michael Huerta
Administrator

Pat A. McNall
Deputy Chief Counsel

FEDERAL HIGHWAY ADMINISTRATION
Walter Waidelich, Jr.
Acting Deputy Administrator

Vacant
Acting Chief Counsel

FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION
Daphne Y. Jefferson
Deputy Administrator

Charles Fromm
Deputy Chief Counsel

FEDERAL RAILROAD ADMINISTRATION
Patrick Warren
Executive Director

Brett A. Jostland
Acting Chief Counsel

FEDERAL TRANSIT ADMINISTRATION
Matt Welbes
Executive Director

Dana Nifosi
Acting Chief Counsel

MARITIME ADMINISTRATION
Joel Szabat
Executive Director

Rand Pixa
Acting Chief Counsel

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
Jack Danielson
Executive Director

Vacant
Chief Counsel

PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION
Howard ("Mac") McMillan
Executive Director

Vasiliki Tsaganos
Acting Chief Counsel

SAINT LAWRENCE SEAWAY DEVELOPMENT CORPORATION
Craig H. Middlebrook
Deputy Administrator

Carrie Mann Lavigne
Chief Counsel

OFFICE OF INSPECTOR GENERAL
Calvin Scovel III
Inspector General

Omer Poirier
Chief Counsel

SURFACE TRANSPORTATION BOARD
Ann D. Begeman
Acting Chairman

Daniel R. Elliott III
Vice Chairman

Deb Miller
Member

Craig Keats
General Counsel

TRANSPORTATION SECURITY ADMINISTRATION
Huban Gowadia
Acting Administrator

Francine J. Kerner
Chief Counsel

FEDERAL MARITIME COMMISSION

Michael Khouri
Acting Chairman

Rebecca Dye
Mario Cordero
William Doyle
Daniel Maffei
Commissioners

Tyler Wood
General Counsel

Transportation and Transportation Security Law Section Leadership

TransLaw is published by the Federal Bar Association Transportation and Transportation Security Law Section, ISSN No. 1069-157X.

Consulting Editor, FBA: Cathy Barrie

Third Circuit Address Maritime Jurisdiction Involving a Brawl on a Vessel

Case summary by Jacob Spegal and Thomas K. Lehrich

In proper maritime tradition, a day on the water ends with a drunken brawl onboard the Ben Franklin Yacht, owned by Christopher Columbus, LLC. It should be noted that the case heading misspelled "Columbus", and is titled *In the Matter of the Complaint of Christopher Columbis, LLC, (t/a BEN FRANKLIN YACHT), As the Owner of the Vessel BEN FRANKLIN YACHT, For Exoneration from or Limitation of Liability*, No. 16-1772 (3d Cir. Sept. 25, 2017).

While this decision did not address the merits of the claim, it did clarify maritime subject-matter jurisdiction, a question raised *sua sponte* by the district court despite an agreement by the parties at the outset of litigation that the district court had proper jurisdiction. Similar to a market definition in an antitrust analysis, this case was decided largely based on the court's "general features" description of the incident. By determining, inter alia, that the district court had described the incident too specifically, and subsequently broadening the description, the United States Court of Appeals for the Third Circuit found that the incident as properly described did have sufficient potential to disrupt maritime commerce and establish federal maritime jurisdiction. Consequently, the Complainant (here, Appellee), Mr. Bocchino, may not pursue his tort claim in state court and federal maritime law controls.

The Third Circuit clarified that when a party seeks to invoke federal admiralty jurisdiction over a tort claim, the claim "must satisfy conditions both of location and of connection with maritime activity." The location aspect is satisfied if "the tort occurred on navigable water" or the "injury suffered on land was caused by a vessel on navigable water." The connection aspect is a conjunctive two-part inquiry. First, the court "must 'assess the general features of the type of incident involved' to determine whether the incident has 'a potentially disruptive impact on maritime commerce.'" Second, the court "must determine whether 'the general character' of the 'activity giving rise to the incident' shows a 'substantial relationship to traditional maritime activity.'" Federal admiralty jurisdiction is only proper when the location test and both prongs of the connection test are satisfied.

Bocchino conceded that the location aspect of the jurisdictional test was satisfied because the alleged tort occurred on the Delaware River. Bocchino also conceded that the second part of the connection test is satisfied, because carrying passengers for hire on a vessel on navigable waters is substantially related to traditional maritime activity.

The analysis of whether there was admiralty jurisdiction in this case focused on the first part of the connection test: an assessment of the general features of the incident, and whether such an incident has the potential to disrupt maritime commerce. Such an assessment "turns . . . on a description of the incident at an intermediate level of possible generality."

In formulating a general features description of the case, the Supreme Court cautioned courts to avoid descriptions that are so general that they cannot be useful in comparing cases, or descriptions that are so specific that they would ignore an incident's capacity to have an effect on maritime commerce. Accordingly, courts must look at the facts of the case and formulate a description that will enable it to determine "whether the incident could be seen within a class of incidents that posed more than a fanciful risk to commercial shipping."

Applying these principles, the Third Circuit held that the incident at issue was best described as "an altercation between passengers on a boat in the process of docking." This description was more general than the district court's overly specific description as "a physical altercation among recreational passengers on board a vessel that is in the immediate process of docking." Thus, although it was not possible to ascertain the location of the vessel relative to the pier on the summary judgment record, such a precise determination was unnecessary to resolve the question of subject matter jurisdiction. For purposes of crafting a general features description to which the connection test may be applied, the court need only state that the vessel was "in the process of docking" while the altercation was occurring.

Having crafted the description of the general features of the incident involved, the court must then "ascertain 'whether the incident could be seen within a class of incidents that posed

CASE SUMMARY *continued on page 7*

Follow the Transportation and Transportation Security Law Section of the Federal Bar Association on Twitter!

@FBA_Trans

The Shock of the New: Blockchain Technology, Logistics, and the Building Blocks of Multi-Modalism's Not-So-Distant Future

Allison N. Skopec

You probably first learned about Blockchain through the cryptocurrency Bitcoin; indeed, Blockchain technology was originally developed as a means of verifying Bitcoin exchanges. Usually when someone brings up Bitcoin, people immediately think of the illicit transactions run via the darknet hidden service, SilkRoad, a site that facilitated drug deals amongst other colorful transactions. While Bitcoin's early days were undeniably steeped in this history, Blockchain technology has much broader applications and the potential to revolutionize the logistics industry.

What is Blockchain Technology?

Blockchain is a decentralized ledger technology that a network can use to exchange assets, whether physical or digital. Each party to a transaction is granted access and can draft, review, and validate transactions on the encrypted ledger, which is updated in real time. Once a transaction is validated using a unique consensus process, it is permanently stored as a "block" on a network of Peer-to-Peer nodes. Since the network is distributed (run on computers provided by logistics partners around the world) which lends itself to integrity, security breaches of confidential data are unlikely to occur. One of the many benefits provided by Blockchain is the elimination of the middle-man in any given transaction, meaning there is no need for clearance from a central bank. Each block on the Blockchain has a timestamp and a link to the previous block on the chain, ensuring that every transaction follows the specific rules of the network. After a block is created it cannot be deleted unless subsequent blocks are also changed, which requires majority approval by the network. Thus, the result is a "faster, private, confidential, auditable [networked monitoring system that facilitates] business-to-business interactions among suppliers, distributors, financial institutions, regulators or anyone wishing to make a secure exchange."[1]

What does Blockchain Technology mean for Transportation?

As freight rates plunge, shipping efficiency skyrockets, and consolidation of major players continue to affect shipping, the logistics industry continues to evolve.[2] It is clear that the highest-impacting development is technology. In recent years, logistics processes have become even more simplified with electronic data interchange (EDI). This technological speed was matched with terminal growth, service expansions, and the introduction of mega-container ships. This technology has irreversibly altered the shipping industry's infrastructure, but there is an unmet need to keep up with globalized cargo trading and commerce's substantial growth. Blockchain can fulfill this need.

For example, in transportation, a Blockchain network could potentially include every party in a transaction: the manufacturer, customs agents, sellers/buyers, banks, shippers, port authorities, government regulators, carriers, and drivers. Blockchain foreshadows a paper-free realm, by which all related parties in "each transaction have a public and private key, perform physical transactions, exchange and store information in encrypted format and perform contractual obligations, give and accept instructions, securely exchange payments, and create smart contracts."[3]

Industry Acceptance and Recent Developments

Many businesses have recognized Blockchain's potential and have embraced it through trial runs, moving Blockchain technology from theoretical to applicational. In early March 2017, Maersk partnered with IBM to conduct the first Blockchain-based cargo-tracking trial.[4] In July 2017, IBM signed up with a major port operator in Singapore, PSA Singapore Terminals, to work with a regional shipping firm to test a new Blockchain-based supply chain network. On September 6, 2017, Maersk revealed yet another collaboration with Microsoft and Guardtime (a data security firm) to build a blockchain-based marine insurance platform that will be the first truly practical use of Blockchain technology. Guardtime announced that the platform has already been built and will deploy in January 2018, "when A.P. Moller-Maersk, which was part of a 20-week trial of the new platform, would start using it for some areas of its business, along with insurers MS Amlin and XL Catlin."[5]

On September 9, 2017, Hyundai Merchant Marine (HMM), along with other members of a Blockchain consortium, announced it had completed the world's first Blockchain pilot voyage from Korea to China with reefer containers. HMM applied Blockchain technology every step of the way—from "shipment booking to cargo delivery [by] combining blockchain technology with Internet of Things (IoT) technology, [which] enabled the cargo to be monitored in real-time."[6] On October 6, 2017, the Municipality of Rotterdam and the Port of Rotterdam Authority announced that they were jointly launching a field lab for the development of Blockchain technology. The new applied research lab, christened "BlockLab," was designed to serve as a center to innovate cargo flow efficiency. One of Blocklab's first projects is a Blockchain application for stock financing in the port logistics sector, which was developed in partnership with Exact and ABN AMRO. The list of new Blockchain applications goes on, and a cursory glance at the news every day shows another company joining the Blockchain family.

Blockchain technology has even been spilling into the government sector, with the US Navy announcing plans to

implement Blockchain on a trial basis to bring added security to its manufacturing systems.[7] The trial will be led by the Naval Innovation Advisory Council to create a "data-sharing layer" for 3-D printing manufacturing.[8] Lieutenant Commander Jon McCarter strongly endorsed the new venture, saying:

> "If someone told you that the technology underpinning the cryptocurrency Bitcoin will likely revolutionize much of the way we do business in the next 10 years, you might shrug it off. I would like to tell you: it's just the beginning and that it might also revolutionize naval additive manufacturing, finance and logistics writ large, and that's only scratching the surface."[9]

Notably, the Navy is embracing this technology because it demonstrates that not only are they receptive to new manufacturing technology, but also see blockchain as a way of mitigating cyber risk.

Managing Cyber Risk

Since 90 percent of world trade is transported by sea, the need for secure logistics cannot be overstated.[10] Vessels, ports, and seamen are the arteries that sustain the global economy and strong security systems are necessary to manage risk and keep up with new cyber threats. In the past few years, ports have become increasingly reliant on digital communications systems, albeit often outdated or unsecure, to keep their internal operations running smoothly. Any IT issues create major disruptions that cripple complex logistic supply chains.

The supply chain's worst nightmare came true on June 27, 2017, when A.P. Møller - Mærsk A/S confirmed via press release that their security was breached during a global cyberattack named Petya.[11] Beyond delaying operations and leaving the status of cargo unaccounted for, Maersk said they expected "$200 million to $300 million" for costs in remediating the damage caused by the cyberattack.[12] If the Blockchain technology Maersk developed had been in place at the time of the cyberattack, it would have prevented the Petya malware from disrupting Maersk's communications and operations IT systems.[13] As the largest container shipping line and the operator of 76 ports' APM Terminals, the Maersk Petya cyberattack showed "the scale of the damage a computer virus can unleash on the technology dependent and inter-connected [logistics] industry."[14] Fortunately, no data was lost in this attack, though the malware's creators intended for the cyberattack to delete such information.

In the wake of a major cyber security attack, also caused by Petya malware, that disabled the largest terminal at the Port of Los Angeles, legislators are recognizing the need for a strong cybersecurity measures to protect U.S. industry. On November 7, 2017, U.S. Senators Kamala D. Harris (D-CA), a member of the Senate Homeland Security and Governmental Affairs Committee, and Dan Sullivan (R-AK) introduced S. 2083, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017.[15] The proposed legislation is intended to "incorporate best practices in cybersecurity policy into the Department of Homeland Security and Coast Guard maritime protective missions."[16]

Increased governmental and business interest in Blockchain paired with exasperation with outdated systems and increased cyber risk has led to broader acceptance of Blockchain-based platforms. While no security system is impervious to breaches, the combination of Blockchain's encryption and its decentralized security system makes it extremely difficult to hack. The main takeaway from recent security breaches is investing in security will prevent cyberattacks and will also strengthen and synergize the entire flow of supply chains.

Smart Contracts

If distributed ledgers such as Bitcoin defined Blockchain's nascent days, Smart Contracts will define its adolescence. In 1994, Nick Szabo coined the term Smart Contracts with the goal of creating an "electronic commerce protocol, which would facilitate business transactions between strangers on the internet without the need for trusted intermediaries" (very similar to the idea behind Blockchain).[17] Smart Contracts are written in various code languages that define "how and when an agreement" can be enforced.[18] Similar to other Blockchain platforms mentioned previously, a Smart Contract is recorded on the Blockchain ledger.[19]

According to Jerry Cuomo, vice president for Blockchain technologies at IBM, Smart Contracts will be "useful across industries, from financial services to logistics to the insurance industry." Just like other Blockchain-based platforms, Smart Contracts eliminate the need for an intermediary when exchanging anything of value. Another benefit of Smart Contracts is that they are inherently transparent and conflict-free. Smart Contracts define "the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations."[20]

Some legal practitioners have raised concerns about Smart Contracts and their potential to make transactional lawyers obsolete. Nick Szabo addressed these concerns at a Smart Contracts Symposium in 2016, saying he does not believe this will be the case for lawyers.[21] He went as far to say Smart Contracts will lead to new legal possibilities previously unimagined since "traditional law is manual, local and often uncertain [whereas] public blockchains are automated, global and [predictable] in their operations."[22] Since Smart Contracts explicitly lay out the rights and obligations of parties in a contract, there will be no need for litigation if a dispute arises.

Unmanned Vessels

Unmanned vessels and autonomous logistics operations are picking up steam worldwide—setting the stage for total transformation of the way the shipping industry operates. While autonomous technology, such as flying cars, may seem like something from Back to the Future, the reality is autonomous drone ships have left the realm of science fiction. With Norway[23] leading the charge, the number of projects funding unmanned vessel research and development is

steadily rising, with 2017 showing the highest numbers yet. So far, 2017 showed us the world's first designated test area for autonomous ships and European Union-funded research,[24] Japanese shipbuilders and shipping firms announced a plan to fully-functional remote-controlled cargo vessels,[25] and Rolls-Royce and tug operator, Svitzer, demonstrated the world's first remote-controlled unmanned commercial ship earlier this year.[26] Following an international proposal to include autonomous ships on its agenda, the IMO Maritime Safety Committee announced it will "establish a new international legal framework for the safe operation of these vessels" addressing unresolved safety and legal issues surrounding autonomous vessels.

What exactly is an unmanned vessel? Simply put: they are vehicles, called either unmanned surface vehicles (USV) or autonomous surface vessels (ASV), which operate without a crew. They function in one of two ways: by way of a remote operator or via completely autonomous operation. When a vessel is completely autonomous, the vessel operator "input[s] a final destination into a USVs onboard computer and the vessel will then navigate to the destination with no further human interaction."[27] The US Navy tried out the completely autonomous route, launching the $20 million "Sea Hunter" in late 2016, and has been implementing self-driving technology for over a year now.[28] Therefore, it makes sense companies are starting to recognize the commercial value in investing in unmanned vessel and autonomous logistics.

Conclusion

An oversupply of vessels, plunging freight rates, and worries over global demand have pushed the logistics industry to find greater cost efficiencies while maintaining secure technology systems. Given the global nature of the shipping business, the interconnectedness of the different parts of logistics operations and the common problems shared by most operators, the most obvious solution is the further application of Blockchain. Time will tell if an international Blockchain consortium between ports and shippers will arise; in the meantime, it is up to the United States to find cost-effective and secure methods to keep business afloat. It is time for the logistics industry to embrace and develop practical applications of Blockchain. ❖

Endnotes

[1]MarEx, *Blockchain Taking Hold in Shipping, Insurance* (Sept. 9, 2017), https://www.maritime-executive.com/article/blockchain-taking-hold-in-shipping-insurance.

[2]The OW Bunker and Hanjin bankruptcies are the two most notable examples of these issues conglomerated. *To read more see*: http://www.latimes.com/business/la-fi-hanjin-shipping-industry-crisis-20160913-snap-story.html.

[3]*How Can the Shipping Industry Take Advantage of the Blockchain Technology?* (last accessed Nov. 14, 2017), https://opensea.pro/blog/blockchain-for-shipping-industry.

[4]*Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain* (March 4, 2017), https://www-03.ibm.com/press/us/en/pressrelease/51712.wss.

[5]Jemima Kelly, *EY Teams up with Maersk, Microsoft on Blockchain-Based Marine Insurance*, (Sept. 5, 2017), https://www.reuters.com/article/us-blockchain-insurance-marine/ey-teams-up-with-maersk-microsoft-on-blockchain-based-marine-insurance-idUSKCN1BG3B6.

[6]*See supra* note 1.

[7]LCDR Jon McCarter, DON *Innovator Embraces a New Disruptive Technology: Blockchain* (last accessed Nov. 13, 2017), http://www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx.

[8]*Id*.

[9]*Id.*

[10]*IMO Profile, UN- Business Action Hub* (last accessed Nov. 12, 2017), https://business.un.org/en/entities/13.

[11]*A.P. Møller - Mærsk A/S – cyber attack update Press Release* (Aug. 16, 2017), https://globenewswire.com/news-release/2017/06/28/1029815/0/en/Cyber-attack-update.html.

[12]Reuters, *Maersk Upbeat Despite Hefty Cyber Attack Bill, Impairment Charges* (Aug. 16, 2017), http://gcaptain.com/maersk-upbeat-despite-hefty-cyber-attack-bill-impairment-charges/.

[13]http://www.marinemec.com/news/view,blockchain-would-have-prevented-maersk-cyber-attack_48287.htm. Cyence, a firm that helps insurers measure cyber risk, said economic costs from the attack would total $850 million. Jacob Gronholt-Pederson, *Maersk Upbeat on Shipping Outlook, Faces Hefty Cyber Attack Bill* (Aug. 16, 2017), https://www.reuters.com/article/us-maersk-results/maersk-upbeat-on-shipping-outlook-faces-hefty-cyber-attack-bill-idUSKCN1AW0FQ.

[14]Jonathan Saul, *Global Shipping Feels Fallout from Maersk Cyber Attack* (June 29, 2017), https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE.

[15]*US Port Cybersecurity Bill Advances* (Nov. 13, 2017), https://www.harris.senate.gov/content/harris-sullivan-introduce-legislation-upgrade-cybersecurity-us-ports.

[16]*Id.* The bill would "additionally ensure that the maritime sector is represented on the NCCIC's 24/7 watch floor and would require the Coast Guard to integrate cybersecurity into its maritime security assessments and plans." Id.

[17]Seema Lal Gulabrani, *Blockchain Beyond Bitcoin: Smart Contracts* (April 13,2017), https://blog.soprasteria.com/blockchain-smart-contracts/.

[18]*Smart Contracts: the Blockchain Technology that will Replace Lawyers* (last accessed Nov. 14, 2017), https://blockgeeks.com/guides/smart-contracts/.

[19]*Id.*

[20]*Id.*

[21]Michael del Castillo, *Relax Lawyers, Nick Szabo Says Smart Contracts Won't Kill Jobs*, (Dec. 8, 2016), https://www.coindesk.com/nick-szabo-lawyers-jobs-safe-in-smart-contract-era/.

[22]*Id.*

[23]Christian Matthews, Unmanned Ships are Coming—but they could cost the industry dearly (Sept. 4, 2017), https://phys.org/news/2017-09-unmanned-ships-cargo-industry-dearly.html.

[24]Gary Peters, *Is 2017 the Breakthrough Year for Unmanned Vessels?* (Dec. 12, 2016), http://www.ship-technology.com/features/featureis-2017-the-breakthrough-year-for-unmanned-vessels-5692723/.

[25]Justin McCurry, *Japanese Firms Plan to Launch Self-Driving Cargo Ships Within Decade* (June 8, 2017), https://www.theguardian.com/world/2017/jun/08/japanese-self-driving-cargo-ships-within-decade.

[26]*Rolls-Royce Demonstrates World's First Remotely Operated Commercial Vessel* (June 20, 2017), https://www.rolls-royce.com/media/press-releases/yr-2017/20-06-2017-rr-demonstrates-worlds-first-remotely-operated-commercial-vessel.aspx.

[27]Paul W. Pritchett, *Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology,* 40 TUL. MAR. L.J. 197, 199 (2015).

[28]Mark Prigg, The Self-Driving Warship: US Navy's 132 ft-long "Sea Hunter" Drone that will Scout Oceans for Enemy Subs Takes to the Seas (Dec. 16, 2016), http://www.dailymail.co.uk/sciencetech/article-4042298/The-self-driving-warship-Navy-s-132ft-long-Sea-Hunter-drone-scour-oceans-enemy-subs-takes-seas.html. The US Navy launched the $20 million, 132-foot 'Sea Hunter' last year. It can travel thousands of nautical miles at sea without needing a single crewmember. *Id.*

Allison N. Skopec is a third-year law student at Tulane University in New Orleans, LA, specializing in maritime & admiralty law. Feedback/Questions: askopec@tulane.edu.

CASE SUMMARY *continued from page 3*

more than a fanciful risk to commercial shipping.'" Assessments in this case lead the court to conclude that an altercation between passengers on a boat in the process of docking has the potential to disrupt maritime commerce.

Although the record is unclear about the location of the vessel when the fight broke out, the number of people involved in the fight, and the crew's involvement, if any, in stopping the fight, there are numerous scenarios that could result from a passenger altercation, each of which poses more than a fanciful risk to maritime commerce.

First, this type of incident had the potential to distract the captain or crew during docking, which could have resulted in the vessel crashing into or in some way colliding with the pier, causing damage to the vessel or to the pier. Depending on the degree of damage to the pier, it could be rendered unusable.

Second, a mishap during docking also had the potential to cause injuries to passengers or the crew, the latter of which could leave the vessel unable to dock at the pier. Such injuries could require a rescue of those on board, which might then lead to a Coast Guard investigation.

Finally, if the crew was sufficiently sidetracked by the altercation and unable to dock safely, the vessel could be forced back out on the waterway with a passenger riot underway. That would certainly be distracting to the captain and crew, and also pose a risk to nearby vessels. Any of these outcomes were possible, and all have the potential to disrupt maritime commerce.

Bocchino's arguments to the contrary failed because he relied on the overly specific general features described by the district court and because he focused on what did not actually happen as opposed to what could have happened.

This case serves as a reminder to lower courts in the Third Circuit to not craft descriptions of incidents occurring on the water so narrowly that they obscure the potential effect on maritime commerce.❖

Jacob Spegal and Thomas K. Lehrich both work in the Office of Inspector General at the Committee for Purchase From People Who Are Blind or Severely Disabled (AbilityOne Program) in Washington D.C.

The High Stakes, High Seas Cyber Peril

Michael Bahar, Trevor J. Satnick, and Brownwyn McDermott

Those who work in shipping are accustomed to the perils of the high seas, whether from storms, pirates, floods or fires. But now, a new danger is lurking—the possibility of a cyberattack.

Despite the growing prevalence and severity of cyberattacks across industries, the shipping industry as a whole has been slow to react, and many are less than optimally prepared. To help improve the state of the industry's cybersecurity, international advisory organizations, industry associations, the United States Coast Guard and private industry are all working to provide practical advice, best practices and even minimum standards, just as hackers are increasingly turning their focus to the shipping industry.

The Approaching Cyber Storm

The term "cyberattack" covers a broad array of possible evils, and it is no longer confined to just the theft of data. Perpetrators have already launched successful attacks. One attack against a shipping company involved malware that allowed the attackers to monitor incoming and outgoing emails from the company's finance department, and then change account numbers in order to reroute funds into the accounts of bad actors instead of proper payees.[1] In another instance, a larger shipping company based in Singapore had its computer systems infiltrated. The company declined to release full details of the extent of this attack, but its internet and intranet systems were temporarily shut down.[2]

One of the more notorious forms of cyberattack is a "ransomware" attack, which essentially locks up (or encrypts) the operations of ships and shipping companies, as well as port facilities, until ransom is paid. Even then, there is no guarantee that the bad guys will keep to their end of the bargain. Shipping giant A.P. Moller-Maersk fell victim to a ransomware attack this past summer, and temporarily lost access to its internal systems and lost its ability to take new orders.[3] It is estimated to have cost Maersk $300 million. This attack not only impacted Maersk, but also the suppliers that were counting on the company to deliver their products to markets around the world, and those that were relying on deliveries of supplies such as food and materials.

As the shipping industry becomes more automated and more dependent on computer systems for onshore office and offshore navigation systems, the risk of harm to individual ships, companies and major shipping ports from a cyberattack increases substantially—with the growing potential for attacks which cause injury, loss of life and environmental disasters.

Keeping Systems Ship-Shape and Bristol Fashion

As cyberattacks on the maritime industry continue to become more prevalent and sophisticated, international organizations, government agencies and industry associations are beginning to set expectations and provide crucial guidance for the industry before it's too late.

For example, in June 2017, the International Maritime Organization (IMO), a specialized agency within the United Nations responsible for the safety and security of shipping, adopted Resolution MSC.428 (98) "Maritime Cyber Risk Management in Safety Management Systems" (the IMO Resolution). The IMO Resolution recommends that ship owners and operators appropriately address cyber risks in a Safety Management System no later than January 2021. In fact, by 2021, some of these regulations will require full compliance. In the interim, BIMCO, a Denmark-based international shipping organization, recently produced its version 2.0 of "The Guidelines on Cyber Security Onboard Ships," which are "aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety."

The U.S. Coast Guard and the U.S. Department of Homeland Security also released draft cybersecurity guidelines for maritime facilities, which closely adhere to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and which aim to mitigate the effect of cyberattacks against port facilities.

Furthermore, the Oil Companies International Marine Forum (OCIMF), a voluntary association of oil companies that has been granted consultative status at the IMO, recently published the third version of its Tanker Management and Self-Assessment (TMSA) guide, which, for the first time ever, includes cybersecurity provisions. As of January 1, 2018, those ship owner companies that wish to ship oil may find that they lose out on the business if they do not comply with the cyber provisions. More specifically, the vessel vetting rider clauses often included with the SHELLTIME 4 form charter party, a standard form in the shipping industry, usually provide a cure period of only four weeks before a ship is placed off-hire. This means that if an oil company decides to undertake a cybersecurity review of its shipping provider, and the shipping company fails the vetting process, that company will have only four weeks to implement proper cybersecurity policies and procedures, which realistically is not nearly enough time to successfully establish and implement a coherent and effective policy.

All of this guidance, however, is principles-based and high level. It lacks specificity on exactly how to comply because each ship, port, or shipping company has different risks and different risk appetites. There is no one-size-fits-all solution to cyber issues, and no 100% technological solution.

In fact, the cornerstone of an effective cybersecurity strategy starts with a risk assessment. Knowing your valuable data, your key vulnerabilities and who holds your data or touches your network allows you to design the right

***CYBER PERIL** continued on page 11*

Federal Bar Association Application for Membership

The Federal Bar Association offers an unmatched array of opportunities and services to enhance your connections to the judiciary, the legal profession, and your peers within the legal community. Our mission is to strengthen the federal legal system and administration of justice by serving the interests and the needs of the federal practitioner, both public and private, the federal judiciary, and the public they serve.

Advocacy
The opportunity to make a change and improve the federal legal system through grassroots work in over 90 FBA chapters and a strong national advocacy.

Networking
Connect with a network of federal practitioners extending across all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands.

Leadership
Governance positions within the association help shape the FBA's future and make an impact on the growth of the federal legal community.

Learning
Explore best practices and new ideas at the many Continuing Legal Education programs offered throughout the year—at both the national and chapter levels.

Expand your connections, advance your career

THREE WAYS TO APPLY TODAY: Join online at www.fedbar.org; Fax application to (571) 481-9090; or Mail application to FBA, PO Box 79395, Baltimore, MD 21279-0395. For more information, contact the FBA membership department at (571) 481-9100 or membership@fedbar.org.

Applicant Information

First Name M.I. Last Name Suffix (e.g. Jr.) Title (e.g. Attorney At Law, Partner, Assistant U.S. Attorney)

❍ Male ❍ Female Have you been an FBA member in the past? ❍ yes ❍ no Which do you prefer as your primary address? ❍ business ❍ home

Business

Firm/Company/Agency Number of Attorneys

Address Suite/Floor

City State Zip Country

( )

Phone Email Address

Home

Address Apt. #

City State Zip Country

( ) / /

Phone Date of Birth

Email Address

Bar Admission and Law School Information (required)

U.S.
Court of Record: _____
State/District: _____ Original Admission: / /

Foreign
Court/Tribunal of Record: _____
Country: _____ Original Admission: / /

Tribal
Court of Record: _____
State: _____ Original Admission: / /

Students
Law School: _____
State/District: _____ Expected Graduation: / /

***Court of Record:** Name of **first court** in which you were admitted to practice.*

Authorization Statement

By signing this application, I hereby apply for membership in the Federal Bar Association and agree to conform to its Constitution and Bylaws and to the rules and regulations prescribed by its Board of Directors. I declare that the information contained herein is true and complete. I understand that any false statements made on this application will lead to rejection of my application or the immediate termination of my membership. I also understand that by providing my fax number and e-mail address, I hereby consent to receive faxes and e-mail messages sent by or on behalf of the Federal Bar Association, the Foundation of the Federal Bar Association, and the Federal Bar Building Corporation.

Signature of Applicant ***Date***

(Signature must be included for membership to be activated)

*Contributions and dues to the FBA may be deductible by members under provisions of the IRS Code, such as an ordinary and necessary business expense, except 4.5 percent which is used for congressional lobbying and is not deductible. Your FBA dues include $15 for a yearly subscription to the FBA's professional magazine.

Application continued on the back

Federal Bar Association

Membership Categories and Optional Section, Division, and Chapter Affiliations

Membership Levels

Sustaining Membership

Members of the association distinguish themselves when becoming sustaining members of the FBA. Sixty dollars of the sustaining dues are used to support educational programs and publications of the FBA. Sustaining members receive a 5 percent discount on the registration fees for all national meetings and national CLE events.

	Private Sector	Public Sector
Member Admitted to Practice 0-5 Years	❍ $170	❍ $150
Member Admitted to Practice 6-10 Years	❍ $235	❍ $215
Member Admitted to Practice 11+ Years	❍ $285	❍ $245
Retired (Fully Retired from the Practice of Law)	❍ $170	❍ $170

Active Membership

Open to any person admitted to the practice of law before a federal court or a court of record in any of the several states, commonwealths, territories, or possessions of the United States or in the District of Columbia.

	Private Sector	Public Sector
Member Admitted to Practice 0-5 Years	❍ $110	❍ $85
Member Admitted to Practice 6-10 Years	❍ $170	❍ $145
Member Admitted to Practice 11+ Years	❍ $215	❍ $175
Retired (Fully Retired from the Practice of Law)	❍ $110	❍ $110

Associate Membership

Foreign Associate

Admitted to practice law outside the U.S. ❍ $215

Law Student Associate

First year student (includes four years of membership) ❍ $50
Second year student (includes three years of membership) ❍ $30
Third year student (includes two years of membership) ❍ $20
One year only option ❍ $20

All first, second and third year student memberships include an additional free year of membership starting from your date of graduation.

Dues Total: _____

Practice Area Sections

- ❍ Admiralty Law $25
- ❍ Alternative Dispute Resolution $15
- ❍ Antitrust and Trade Regulation $15
- ❍ Banking Law $20
- ❍ Bankruptcy Law $25
- ❍ Civil Rights Law $15
- ❍ Criminal Law $10
- ❍ Environment, Energy, and Natural Resources $15
- ❍ Federal Litigation $20
- ❍ Government Contracts $20
- ❍ Health Law $15
- ❍ Immigration Law $10
- ❍ Indian Law $15
- ❍ Intellectual Property Law $10
- ❍ International Law $10
- ❍ Labor and Employment Law $15
- ❍ LGBT Law $15
- ❍ Qui Tam Section $15
- ❍ Securities Law Section $0
- ❍ Social Security $10
- ❍ State and Local Government Relations $15
- ❍ Taxation $15
- ❍ Transportation and Transportation Security Law $20
- ❍ Veterans and Military Law $20

Career Divisions

- ❍ Corporate & Association Counsel (in-house counsel and/or corporate law practice) $20
- ❍ Federal Career Service (past/present employee of federal government) N/C
- ❍ Judiciary (past/present member or staff of a judiciary) N/C
- ❍ Senior Lawyers* (age 55 or over) $10
- ❍ Younger Lawyers* (age 40 or younger or admitted less than 10 years) N/C
- ❍ Law Student Division N/C

For eligibility, date of birth must be provided.

Sections and Divisions Total: _____

Chapter Affiliation

Your FBA membership entitles you to a chapter membership. Local chapter dues are indicated next to the chapter name (if applicable). If no chapter is selected, you will be assigned a chapter based on geographic location. *No chapter currently located in this state or location.

Alabama
- ❍ Birmingham
- ❍ Montgomery
- ❍ North Alabama

Alaska
- ❍ Alaska

Arizona
- ❍ Phoenix
- ❍ William D. Browning/ Tucson

Arkansas
- ❍ Arkansas

California
- ❍ Inland Empire
- ❍ Los Angeles
- ❍ Northern District of California
- ❍ Orange County
- ❍ Sacramento
- ❍ San Diego
- ❍ San Joaquin Valley

Colorado
- ❍ Colorado

Connecticut
- ❍ District of Connecticut

Delaware
- ❍ Delaware

District of Columbia
- ❍ Capitol Hill
- ❍ D.C.
- ❍ Pentagon

Florida
- ❍ Broward County
- ❍ Jacksonville
- ❍ North Central Florida–$25
- ❍ Orlando
- ❍ Palm Beach County
- ❍ South Florida
- ❍ Southwest Florida
- ❍ Tallahassee
- ❍ Tampa Bay

Georgia
- ❍ Atlanta–$10
- ❍ Southern District of Georgia Chapter

Hawaii
- ❍ Hawaii

Idaho
- ❍ Idaho

Illinois
- ❍ Central District of Illinois–$25
- ❍ Chicago
- ❍ P. Michael Mahoney (Rockford, Illinois) Chapter
- ❍ Southern District of Illinois

Indiana
- ❍ Indianapolis
- ❍ Northern District of Indiana

Iowa
- ❍ Iowa–$10

Kansas
- ❍ Kansas and Western District of Missouri

Kentucky
- ❍ Kentucky

Louisiana
- ❍ Baton Rouge
- ❍ Lafayette/ Acadiana
- ❍ New Orleans–$10
- ❍ North Louisiana

Maine
- ❍ Maine

Maryland
- ❍ Maryland

Massachusetts
- ❍ Massachusetts –$10

Michigan
- ❍ Eastern District of Michigan
- ❍ Western District of Michigan

Minnesota
- ❍ Minnesota

Mississippi
- ❍ Mississippi

Missouri
- ❍ St. Louis
- ❍ Kansas and Western District of Missouri

Montana
- ❍ Montana

Nebraska
- ❍ Nebraska

Nevada
- ❍ Nevada

New Hampshire
- ❍ New Hampshire–$10

New Jersey
- ❍ New Jersey

New Mexico
- ❍ New Mexico

New York
- ❍ Eastern District of New York
- ❍ Southern District of New York
- ❍ Western District of New York

North Carolina
- ❍ Eastern District of North Carolina
- ❍ Middle District of North Carolina
- ❍ Western District of North Carolina

North Dakota
- ❍ North Dakota

Ohio
- ❍ Cincinnati/ Northern Kentucky-John W. Peck
- ❍ Columbus
- ❍ Dayton
- ❍ Northern District of Ohio–$10

Oklahoma
- ❍ Oklahoma City
- ❍ Northern/ Eastern Oklahoma

Oregon
- ❍ Oregon

Pennsylvania
- ❍ Eastern District of Pennsylvania
- ❍ Middle District of Pennsylvania
- ❍ Western District of Pennsylvania

Puerto Rico
- ❍ Hon. Raymond L. Acosta/ Puerto Rico–$10

Rhode Island
- ❍ Rhode Island

South Carolina
- ❍ South Carolina

South Dakota
- ❍ South Dakota

Tennessee
- ❍ Chattanooga
- ❍ Knoxville Chapter
- ❍ Memphis Mid-South
- ❍ Nashville
- ❍ Northeast Tennessee

Texas
- ❍ Austin
- ❍ Dallas–$10
- ❍ El Paso
- ❍ Fort Worth
- ❍ San Antonio
- ❍ Southern District of Texas–$25
- ❍ Waco

Utah
- ❍ Utah

Vermont
- ❍ Vermont

Virgin Islands
- ❍ Virgin Islands

Virginia
- ❍ Northern Virginia
- ❍ Richmond
- ❍ Roanoke
- ❍ Hampton Roads Chapter

Washington*
- ❍ At Large

West Virginia
- ❍ Northern District of West Virginia–$20

Wisconsin
- ❍ Wisconsin

Wyoming
- ❍ Wyoming

Chapter Total: _____

Payment Information

TOTAL DUES TO BE CHARGED
(membership, section/division, and chapter dues): $ _____

❍ Check enclosed, payable to Federal Bar Association
Credit: ❍ American Express ❍ MasterCard ❍ Visa

_____
Name on card (please print)

_____
Card No. Exp. Date

_____
Signature Date

CYBER PERIL *continued from page 8*

protections.

Based on this knowledge, the next step is to have a detailed incident response plan. Ships already know what to do in the event of floods and fires. Now they need to know what to do in the event of a cyber incident.

It's also not just enough to know what to do. Crews and, in fact, all employees from ship to shore (and not just IT employees) need to train on what to do in the event of a cyber incident. Even the most advanced cybersecurity systems are thwarted by an employee who clicks on a link he or she shouldn't. While we often think of "hacking" as a highly advanced act involving lines of computer code and technical know-how, one of the most common hacker methods is to simply trick an employee into entering in personal information via an email form or website that is disguised to look like a legitimate website or email correspondence. In essence, hackers gain access to vessel systems by duping employees into giving them the credentials they need to log into those very systems. This kind of attack is called "phishing," and proper training on how to spot and avoid falling victim to phishing attacks can decrease the likelihood of a breach.

The industry also needs to look out for single points of failure and low-tech solutions. For example, with the growing reality of GPS spoofing, whereby hackers subtly manipulate GPS data to cause ships to go off course, it is more important than ever to return to old-fashioned seamanship, to ensure that mariners do not lose vital skills and rely solely on computers that could be leading them astray.

Conclusion

When it comes to cybersecurity, the dangers faced by the shipping industry are real and growing. Helpful guidance, best practices and minimum standards are available, and soon may become mandatory, so the time to act is now to better prepare against the coming cyber storms.❖

Endnotes

[1]http://www.bbc.com/news/technology-40685821.

[2]https://www.platts.com/latest-news/shipping/singapore/shipping-bw-groups-computer-systems-hacked-steps-26820691.

[3]http://fortune.com/2017/06/28/petya-ransomware-cyber-attack-maersk-delays/.

Michael Bahar is a partner at Eversheds Sutherland (US) LLP in Washington D.C. and Trevor J. Satnick is a Staff Attorney at Eversheds Sutherland (US) LLP in New York. Brownwyn McDermott is Special Counsel at Eversheds Sutherland (US) LLP in Rhode Island.

Notes from the Section's "Cybersecurity Issues in Transportation" brown-bag panel discussion

Alison Graab and Mike Higgins, Surface Transportation Board

On September 20, 2017, the Transportation and Transportation Security Law section of the Federal Bar Association held a panel discussion on "Cybersecurity Issues in Transportation." The panel consisted of Lee Allen, Cybersecurity Lead - Surface Division, Office of Security Policy and Industry Engagement (OSPIE), Transportation Security Administration, Thomas Farmer, Assistant Vice President – Security, Association of American Railroads (AAR), and Sean C. Griffin, Member, Dykema Gossett PLLC. It was moderated by John E. Anderson, Member, Dickinson Wright PLLC.

Mr. Griffin discussed cybersecurity issues related to practicing law, focusing on an attorney's ethical obligations to protect client confidentiality. Mr. Griffin noted that many standard rules of conduct could be interpreted to cover electronic records and communications, such as email. For example, a lawyer's duty of competency could impose on the attorney a basic obligation to be familiar with cyber risks and to take appropriate steps to protect against those risks, such as having up-to-date antivirus protection. Additionally, an attorney could be required to adhere to the client's instructions with respect to handling electronic information.

Mr. Farmer discussed cybersecurity from the freight railroad perspective. He noted that railroads have been active in the area of cybersecurity since Y2K when the AAR established a committee to address cyber issues. In approaching cybersecurity, Mr. Farmer emphasized the need to focus on how breaches happen rather than seeking to explore every potential consequence of a breach. He observed that approximately 85% of incidents can be safeguarded by implementing and adhering to relatively simple security measures, such as utilizing strong passwords and training to recognize phishing. With respect to the rail industry, he observed that AAR has recommendations on preferred capabilities as to electronic infrastructure, which can drive suppliers to reduce vulnerabilities.

Mr. Allen reviewed a number of cybersecurity resources that the Department of Homeland Security and the Transportation Security Administration (TSA) make available for purposes of protecting against threats to surface transportation. In particular, he highlighted the TSA Surface Transportation Cybersecurity Resource Toolkit and the Surface Transportation Cybersecurity "Pocket" Awareness Guide as key resources for industry. ❖

Published by the Federal Bar Association Transportation and Transportation Security Law Section

Federal Bar Association
1220 N. Fillmore St.
Suite 444
Arlington, VA 22201