Northwestern Journal of International Law & Business

Volume 42
Issue 2 *Winter*

Article 2

Winter 2022

Monitoring Sanctions Compliance at Sea

Richard L. Kilpatrick Jr.

Vol. 42, No. 2
Northwestern Journal of International Law & Business

Monitoring Sanctions Compliance at Sea

Richard L. Kilpatrick, Jr.*

TABLE OF CONTENTS

* Assistant Professor of Business Law, College of Charleston, School of Business, Charleston, South Carolina.

I. INTRODUCTION

Vessel tracking technology is currently in the vanguard of global economic sanctions enforcement and compliance initiatives. As multilateral actors and governmental authorities focus on maritime activities as a key component of sanctions strategy, the shipping industry is in the crosshairs of intense regulatory scrutiny.[1] Since the consequences of running afoul of sanctions are severe—civil penalties, blacklisting, and even vessel or cargo seizure and forfeiture—commercial maritime actors have been forced to quickly adapt as trade rules evolve under the pressures of mercurial geopolitical developments.

Risking the consequences, some nefarious actors continue to utilize maritime assets for illicit sanctions-busting trades.[2] To circumvent sanctions, these vessel operators engage in deceptive practices designed to conceal their activities.[3] Through a technique known as "going dark," they deactivate or manipulate their vessels' mandatory tracking systems to disguise their locations, launder their identities, and obfuscate the nature of the transactions they perform.[4] Law enforcement entities have monitored the world's oceans for such violations, citing suspicious vessel tracking transmissions as evidence of malfeasance.[5] Sanctioning authorities have also advised the private sector to implement technology-driven compliance tools and risk mitigation processes to avoid inadvertently violating sanctions.[6] This is requiring the shipping industry to examine the details of their business dealings more forensically through vessel vetting and counterparty due diligence.[7]

The international vessel monitoring framework finds its origins in

---

[1] Sanctioning authorities include multilateral institutions, such as the United Nations and European Union, or national governments willing to act on their own. The maritime aspects of contemporary sanctions are discussed *infra* in Part III.

[2] For a review of recent maritime sanctions circumvention tactics linked to North Korea, *see generally* Final Rep. of the Panel of Experts Established Pursuant to Security Council Resolution 1874 (2009), transmitted by Letter dated 2 March 2021 addressed to the President of the Security Council, ¶¶ 17-40, U.N. Doc. S/2021/211 (Mar. 4, 2021) [hereinafter Final Rep. of Experts], https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf (Mar. 4, 2021).

[3] *Id.*

[4] *Id*.

[5] *See infra* Part III(A).

[6] *See infra* Part III(B). *See, e.g.*, U.S. Dep't of Treasury, Dep't of State, and Coast Guard, *Sanctions Advisory for the Maritime Industry, Energy and Metal Sectors, and Related Communities* (May 14, 2020) [hereinafter U.S. Sanctions Advisory].

[7] These vetting requirements are akin to the "know your customer" (KYC) inquiries that have become common in the banking and finance sector for compliance with laws relating to sanctions, terrorism financing, and money laundering. *See, e.g.*, *The KYC Process Explained*, SOC'Y FOR WORLDWIDE INTERBANK FIN. TELECOMM. (SWIFT), https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/kyc-process (last visited Feb. 15, 2022).

efforts to ensure navigational safety, but the recent pivot to enhance maritime sanctions has transformed this infrastructure into a transparency apparatus. To examine this phenomenon, this paper first describes the regulatory background that led to mandatory vessel tracking under international law, and analyzes its transformation into a sanctions tool. The paper then explores the ways in which vessel tracking data analytics and artificial intelligence are fueling innovative surveillance-focused commercial compliance products and risk mitigation efforts. Finally, it evaluates the viability of the current approach and, looking ahead, calls into question the reliance on voluntarily transmitted vessel tracking data subject to manual switch-off.

II. VESSEL TRACKING IN INTERNATIONAL LAW

Contemporary vessel tracking flows from treaties designed to protect life at sea. The invention of the radio in the late nineteenth century created the technical capabilities for ships to wirelessly relay distress signals across relatively long distances.[8] After the tragic sinking of the *RMS Titanic* in 1912, major seafaring nations soon mobilized to incorporate these tools into a comprehensive navigational safety framework reflected in the International Convention for the Safety of Life at Sea (SOLAS) 1914.[9] SOLAS 1914 codified processes for the merchant shipmaster to relay danger and distress alerts to other ships and to shore "by all the means of communication at his disposal."[10] This treaty, however, only required ships to be fitted with a "radiotelegraphic installation" if they carried at least fifty people on board.[11] Other ships were only required to carry rudimentary tools for distress alerts, such as "a Morse signaling lamp of sufficient range."[12]

Bolstered by further innovations developed during the two world wars and the creation of multilateral institutions in their aftermath, the international community eventually formed a more complete regulatory structure operationalizing new technologies for coordination on maritime safety.[13] The establishment of the Inter-Governmental Maritime Consultative Organization—the predecessor to the International Maritime Organization (IMO)—also provided the shipping community a platform for further

[8] Prior to the widespread use of radio technology, ships depended on visual signals such as flags and lights, or audible devices such as fog horns, whistles, and bells.

[9] International Convention for the Safety of Life at Sea 1914, Jan. 20, 1914 [hereinafter SOLAS 1914].

[10] *Id.* art. 8.

[11] *Id.* art. 31. Article 35 requires that these radiographic installations be capable of transmitting "clearly perceptible signals from ship to ship over a range of at least 100 sea miles."

[12] *Id.* art. 9.

[13] Even in the interwar period, SOLAS was updated to better facilitate radio-based alert signals. SOLAS 1929 requires all ships engaged on international voyages to carry radiographic installations, except those less than 1,600 gross tonnages. *See* International Convention for the Safety of Life at Sea 1929, UKTS 43, May 31, 1929, Chapter IV, Article 27.

harmonized regulation. Through these auspices, SOLAS was updated in 1960, and once again in 1974, producing a treaty text designed to promote maritime safety through detailed provisions articulating minimum standards for vessel construction and operation, as well as safety equipment that must be carried on ships at sea.[14]

The original text of SOLAS 1974 contains explicit carriage requirements, including maritime monitoring tools relying on enhanced communication and data exchange between ships and shore. Among these is a requirement that qualifying vessels be fitted with a Very High Frequency (VHF) "radiographic station" and "radiotelephone station" capable of sending and receiving danger and distress communications across designated channels.[15] The original SOLAS 1974 also requires certain "shipborne navigational equipment" to be carried on vessels, including radar systems, echo sounding devices, and various other technologies of the era.[16] Some of these items referenced in the SOLAS 1974 text are now technologically obsolete, but in the decades following its entry into force, amendments have been added by way of the IMO Maritime Safety Committee in accordance with the procedures laid out in Article VIII.[17] Through this flexible amendment process, the IMO has repeatedly updated SOLAS 1974 to fulfill maritime safety goals through increasingly sophisticated vessel tracking processes as new technologies have emerged.

A. Global Maritime Distress Safety System (GMDSS)

Under the original SOLAS 1974 text, along with corresponding language found in the International Convention on Maritime Search and Rescue 1979 (SAR Convention), both national coast guards and private commercial vessel operators are obliged to observe designated radio frequencies for distress signals relayed by other ships.[18] But since conventional radio transmissions have limited working range in part due to the curvature of the earth's surface, vessels operating at sea often filled the role of tracking distress signals and providing assistance.[19] The advancement

[14] *See* International Convention for the Safety of Life at Sea 1960, UKTS 60, May 31, 1960; International Convention for the Safety of Life at Sea 1974, 1184 UNTS 3, Nov. 1, 1974, [hereinafter SOLAS 1974].

[15] SOLAS 1974, Chapter IV.

[16] *Id.* Chapter V.

[17] Article VIII directs amendments proposed by a contracting government to be "referred to the Maritime Safety Committee of the Organization for consideration." Contracting governments may participate in the proceedings considering the adoption of amendments, which requires a two-thirds majority of the contracting governments present and voting. *Id*.

[18] *See* International Convention on Maritime Search and Rescue, 1405 UNTS 97, adopted April 27, 1979, entered into force June 22, 1985 [hereinafter SAR Convention]; *see also* IMO Maritime Safety Committee, *Guidelines on the Treatment of Persons Rescued at Sea*, MSC.167 (78) (May 20, 2004).

[19] *See* Denise Brehaut, GMDSS: A USER'S HANDBOOK 11 (5th ed., Bloomsbury Publishing 2013).

of telecommunications capabilities through satellite technology altered this dynamic, and ultimately led to SOLAS updates.[20] In 1988, the IMO adopted a revised SOLAS chapter to establish a Global Maritime Distress and Safety System (GMDSS), which reimagined maritime safety responses utilizing new technology.[21] These GMDSS provisions mandate that every qualifying ship carry radio equipment capable of performing enumerated functions including transmitting and receiving ship-to-ship and ship-to-shore distress alerts, signals for determining location, and other maritime safety information.[22] Relying on a combination of satellite and terrestrial technologies, this new SOLAS regime transformed distress communications from being primarily dependent on ship-to-ship radio transmissions to instead extensively facilitate ship-to-shore messaging.[23]

From its inception, the technological operability of GMDSS has depended on three types of equipment: transmitters carried on vessels operating at sea, receivers housed in shore-based facilities, and geostationary satellites moving in synchronous orbits more than twenty-thousand miles above the earth.[24] The GMDSS regulations require that vessels carry emergency position indicating radio beacons (EPIRBs) which relay homing signals for location detection, navigational telex devices capable of automatically receiving safety messages such as emergency meteorological forecasts, and search and rescue transponders used to enhance tracking through more precise location signals on a radar band.[25]

The GMDSS satellites are primarily monitored and controlled by the London-based International Maritime Satellite Organization (INMARSAT).[26] INMARSAT satellites are assigned ocean region footprints, and within the coverage of these overlapping sea areas distress communications may be conveyed nearly anywhere in the world (with

---

[20] *Id.* at 27-29; *See also* Arthur Alan Severance, *The Duty to Render Assistance in the Satellite Age*, 36 CAL. W. INT'L L. J. 377 (2006) (discussing the role of technology in the development of GMDSS).

[21] *See* SOLAS 1974, *supra* note 14, as amended, Chapter IV, Reg. 4. These GMDSS requirements came into force on February 1, 1992.

[22] *Id.* The SOLAS GMDSS provisions also require contracting governments to "ensure that suitable arrangements are made for registering [GMDSS] identities and for making information on these identities available to rescue co-ordination centers on a 24-hour basis."

[23] *See* U.S. Coast Guard, *Global Maritime Distress and Safety System* https://www.navcen.uscg.gov/?pageName=GMDSS.

[24] *See* Brehaut, GMDSS: A USER'S HANDBOOK, *supra* note 19, at 12.

[25] *Id.* at 98. Search and rescue transponders can be especially helpful to locate survivors who have abandoned a sinking vessel.

[26] *Id.* at 81. INMARSAT was originally established in conjunction with the International Mobile Satellite Organization. It was later privatized but continues to provide infrastructure for the operation of GMDSS. *See* David Sagar, *INMARSAT*, 14 INT'L J. OF MARINE AND COASTAL L. 423 (1999). Note that EPIRBs interact with a different group of COSPAS-SARSAT satellites designed to provide broader coverage that include the polar regions. *See* U.S. Coast Guard, *Emergency Position Indicating Radiobeacon*, https://www.navcen.uscg.gov/?pageName=mtEpirb.

certain parts of the polar regions being the possible exception).[27] Recent efforts to modernize GMDSS have also included the use of new satellites managed by entities beyond INMARSAT. In 2018, the IMO Maritime Safety Committee approved a new service provider called Iridium.[28] Iridium has described its satellites as offering more comprehensive GMDSS services with "full coverage at even extreme latitudes."[29]

In practice, GMDSS has allowed vessel operators to relay distress signals to state-operated Rescue Coordination Centers (RCCs), which the SAR Convention tasks with the responsibility of coordinating rescue responses.[30] To fulfill this purpose, GMDSS data is collected by the IMO-authorized service providers and is then passed on to state authorities.[31] GMDSS does not transmit vessel location information automatically; rather it is subject to human operation through the initiation of a distress signal.[32] This involves a vessel operator activating the system using the red push-button on the shipborne GMDSS equipment to relay a pre-formatted distress alert, which transmits the message to the service providers.[33] One problem with this reliance on manual operation is that GMDSS has commonly been subject to false positive signals.[34] In the early years following its implementation, the prevalence of false positives threatened to strain search and rescue resources, although this problem has reportedly diminished with modifications to newer equipment.[35] Despite any shortcomings, the GMDSS implementation represents a critical first wave in globally mobilizing

---

[27] *See* Brehaut, GMDSS: A USER'S HANDBOOK, *supra* note 19, at 81; *see also* S.E. Doyle, *INMARSAT: The International Maritime Satellite Organization—Origins and Structure*, 5 J. OF SPACE L. 45 (1977).

[28] *See* IMO Maritime Safety Committee, *Statement of Recognition of Maritime Mobile Satellite Services Provided by Iridium Satellite LLC, MSC.451(99)* (May 24, 2018).

[29] *Ten Things to Know About GMDSS*, IRIDIUM (July 12, 2018), https://www.iridium.com/blog/2018/07/12/ten-things-know-gmdss/.

[30] *See* SAR Convention, *supra* note 18, para 2; *see also* IMO Maritime Safety Committee, *Guidelines on the Treatment of Persons Rescued at Sea*, MSC.167(78) (May 20, 2004).

[31] Note that GMDSS data is designed for government use to facilitate search and rescue, and it is not designed to be made publicly accessible like AIS discussed *infra* in Part II(B).

[32] EPIRBs are designed to activate automatically when immersed in water, but they can be made inoperable by simply removing the battery or even wrapping the transponder in tin foil—a possibility mentioned in IMO documents as necessary when a ship is scrapped after the end of its useful life. *See* IMO General Assembly, *IMO Guidelines for the Avoidance of False Distress Alerts*, Res A.814(19) (Nov. 23, 1995).

[33] *See* Brehaut, GMDSS: A USER'S HANDBOOK, *supra* note 19, at 49. The GMDSS equipment is capable of automatically transmitting the distress message, including vessel location, via a Digital Select Calling (DSC) framework. To prevent false positive signals, new equipment houses the distress button under a spring-loaded cover and requires the user to hold the button for five seconds. *Id.* at 55.

[34] *See* IMO Sub-Committee on Navigation, Communications and Search and Rescue, *Completion of the Detailed Review of the Global Maritime Distress and Safety System*, NCSR 3/14 (Dec. 11, 2015) Annex 1, at 15.

[35] *See IMO Guidelines for the Avoidance of False Distress Alerts*, *supra* note 32.

satellite-based technology to promote maritime safety through enhanced vessel location tracking.

B. Automatic Identification System (AIS)

The international harmonization of GMDSS technical requirements set the stage for further vessel monitoring capacity. In 2000, the IMO Maritime Safety Committee again adopted SOLAS amendments—this time updating system and equipment carriage requirements for the purpose of aiding navigation through automatic information exchanges.[36] These provisions require qualifying vessels to be "fitted with an automatic identification system (AIS)."[37] The amendments mandate that the AIS "provide automatically" real-time information, including the vessel's "identity, type, position, course, speed, navigational status and other safety-related information" which must be made accessible to other ships, aircraft, and equipped shore-based facilities through transponders carried on board.[38] The AIS equipment must also be capable of automatically receiving such information from other ships for the purpose of monitoring and tracking their movements.[39]

The new SOLAS provisions also explain that AIS "shall be operated taking into account the guidelines adopted by the [IMO]."[40] Less than a year after the IMO adopted the amendments, the IMO General Assembly issued Guidelines for the Onboard Operational Use of Ship-borne Automatic Identification Systems (AIS).[41] These Guidelines were developed to promote the efficacy of AIS and also to "inform the mariner about the operational use, limits and potential uses of AIS."[42] They also clarify the objective of AIS is "to enhance: safety of life at sea; the safety and efficiency of navigation; and the protection of the marine environment" through vessel identification, tracking, and information exchange.[43]

The AIS Guidelines, which were revised slightly in 2015, clarify its technical requirements. The AIS should relay fixed information including the

---

[36] Maritime Safety Committee*, Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended*, MSC.99(73) (Dec. 5, 2000).

[37] This provision requires, "all ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size be fitted with an automatic identification system (AIS)." SOLAS 1974, *supra* note 14, as amended, Chapter V, Reg. 19, para. 2.4.

[38] SOLAS 1974, *supra* note 14, as amended, Chapter V, Reg. 19, para. 2.4.5; *see also* International Maritime Organization, *AIS Transponders*, https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx.

[39] *AIS Transponders*, *supra* note 38.

[40] SOLAS 1974, *supra* note 14, as amended, Chapter V, Reg. 19, para. 2.4.5.7.

[41] Int'l Maritime Org. Res. A.917(22), annex, U.N. Doc. A 22/Res17 (Nov. 29, 2001) [hereinafter Original AIS Guidelines].

[42] *Id.* para. 1.

[43] *Id*. para. 4.

IMO number, Maritime Mobile Service Identity (MMSI) number, and vessel type and size; dynamic information such as vessel position and speed; and voyage information such as the vessel draught and intended destination.[44] The Guidelines explain that AIS utilizes radio waves sent through VHF broadcasts to transmit messages in the maritime band.[45] Some of these messages, such as the vessel's position and speed, are updated automatically from the ship sensors, while other data is entered manually.[46] Manual inputs into the system may be entered by the vessel operator at the start of the voyage or "whenever changes occur.[47]" This manually entered data includes the draught, departure time, expected destination arrival time, route plan, and other information such as whether hazardous cargo is carried onboard.[48] To ensure the accuracy of the AIS data, the vessel operator is encouraged to "carry out regular routine checks during a voyage to validate the accuracy of the information being transmitted."[49]

The AIS Guidelines also provide operational instructions. They emphasize that some ships, such as leisure craft, warships, naval auxiliary vessels, and small fishing boats do not carry AIS.[50] For those vessels that are subject to the AIS requirement, "AIS should always be in operation when ships are underway or at anchor."[51] However, the AIS Guidelines also indicate a limited exception to the continuous nature of the AIS requirement: "[i]f the master believes that the continual operation of AIS might compromise the safety or security of his/her ship or where security incidents are imminent, the AIS may be switched off."[52] As an elaborating point, the original AIS Guidelines note that "[t]his might be the case in sea areas where pirates and armed robbers are known to operate," although this illustrative language is excluded in the revised AIS Guidelines.[53] In any event, if the AIS is switched off, the revised Guidelines highlight, "[t]he master should however restart the AIS as soon as the source of danger has disappeared."[54]

Due to this possibility of AIS switch-off, the AIS Guidelines also caution vessel operators to "always be aware that other ships fitted with AIS as a mandatory carriage requirement might switch off AIS under certain circumstances" and, consequently, "the information given by the AIS may

---

[44] Int'l Maritime Org. Res. A.1106(29), annex, U.N. Doc. A 29/Res.1106, paras. 12–13 (Dec. 2, 2015) [hereinafter AIS Guidelines].

[45] *Id*. para. 8*; see also* United States Coast Guard, *Automatic Identification System Overview*, (Apr. 17, 2020), https://www.navcen.uscg.gov/?pageName=AISmain.

[46] AIS Guidelines, *supra* note 44, paras. 12-13.

[47] *Id.* para. 23.

[48] *Id.*

[49] *Id*. para. 27.

[50] *Id*. para. 3.

[51] *Id.* para. 22.

[52] *Id.*

[53] *See* Original AIS Guidelines, *supra* note 41, para. 21.

[54] AIS Guidelines, *supra* note 44, para. 22.

not be a complete picture of the situation around the ship."[55] While the reasons for this inaccurate transmission may be based on the "professional judgment of the master," the Guidelines also note that it is possible that "poorly configured or calibrated ship sensors" might lead to faulty transmissions that are "dangerously confusing."[56]

Shipping industry organizations with IMO consultative status, including the International Chamber of Shipping (ICS) and the International Association of Independent Tanker Owners (INTERTANKO), appear to have played a significant role in the development of the AIS Guidelines with its AIS switch-off exception.[57] Their submissions to the Maritime Safety Committee support the adoption of provisions in the SOLAS amendments and the corresponding AIS Guidelines allowing for AIS to be deactivated at the shipmaster's discretion. INTERTANKO argued in its submission that "[d]ue to the type of information contained within a broadcast, by an AIS Transponder, a Master should have the authority to turn off the transponder when the Master thinks the safety of the ship could be affected by its transmission."[58] INTERTANKO proposed that the Maritime Safety Committee, "make a provision in the Guidelines for AIS Transponders indicating that a Master is allowed to switch off the AIS transponder should he consider the safety of the ship could be affected."[59] In a document submitted on the same day, ICS, which proposed the original draft AIS Guidelines for consideration by the Maritime Safety Committee Sub-Committee on Safety of Navigation, also described the following as one of the principles of its proposal: "if the master believes that the continual operation of AIS might compromise the safety of his ship, he may switch the AIS off at any time."[60]

---

[55] *Id.* paras. 33-34.

[56] *Id.* para. 37.

[57] *See* Maritime Safety Committee, *Report of the Maritime Safety Committee on its Seventy-Second Session*, MSC 72/73 (May 31, 2000) paras. 10.21, 10.65-10.68; The International Chamber of Shipping is a non-profit trade association made up of shipowners and operators, describing itself as "the collective voice of the international shipping industry." It represents its membership as an advocate for "high operational standards and a regulatory environment embracing safety, environment, open markets and fair competition." *See* International Chamber of Shipping, *About ICS,* https://www.ics-shipping.org/about-ics/; INTERTANKO is a trade association representing the interest of its members who are independent tanker owners. Its work is devoted to "a wide range of operational, technical, legal and commercial issues affecting tanker owners and operators around the world." *See* INTERTANKO, *About Us,* https://www.intertanko.com/About-Us/.

[58] *See* Maritime Safety Committee, *Revision of Chapter V of SOLAS—Transponders: Submitted by INTERTANKO*, MSC 72/10/8 (Mar. 14, 2000), para. 5.

[59] *Id.* para. 7.

[60] *See* Maritime Safety Committee, *Guidelines on Automatic Identification System (AIS) Operational Matters: Note by the International Chamber of Shipping (ICS)*, MSC 72/10/12 (Mar. 14, 2000); *see also* Navigation Committee, *Guidelines on Automatic Identification System (AIS) Operational Matters: Note By the International Chamber of Shipping (ICS)*, NAV, 46/10, (Mar. 20, 2000).

AIS data has been utilized for research and regulatory purposes beyond the original navigation-focused scope articulated in the text of the SOLAS amendments. State actors have employed AIS data to surveil traffic for maritime domain awareness purposes, including pollution prevention and response, ballast water exchange, noise regulation, and protection of aquatic life and vulnerable sea areas.[61] In the years following the 9/11 attacks, AIS was also re-directed as a tool to respond to maritime security vulnerabilities, such as enhancing compliance with the new International Ship and Port Facility Security (ISPS) code.[62]

AIS capabilities have also been enhanced through the use of satellite technology by which space-based AIS receivers collect and report vessel identification information in real time.[63] This has broadened the possibilities of vessel tracking for disaster response such as alerting vessels in the path dangerous weather, enhancing search and rescue efforts in conjunction with GMDSS equipment, and collecting evidence for the purpose of identifying vessels responsible for incidents of ship-source marine pollution.[64] Some observers see this wide-ranging use of AIS data optimistically, while others view its application through a more skeptical lens.[65]

But even as AIS has become a fundamental tool for maritime monitoring, regulators, industry participants, and technical researchers alike continue to recognize that AIS is not always reliable. As a self-reporting system dependent on manual inputs, AIS remains notoriously susceptible to unintentional human error and jamming.[66] Since AIS relies on unencrypted

---

[61] For an overview of these initiatives, *see generally* Melanie Fournier et al., *Past, Present, and Future of the Satellite-based Automatic Identification System: Areas of Applications* (2004-2016), 17 WMU J. OF MAR. AFFAIRS 311, 311-45 (2018); *see also* Martin Svanberg, et al., *AIS in Maritime Research*, 106 MARINE POL'Y 103520 (2019).

[62] *See generally* William R. Cairns, *AIS and Long Range Identification & Tracking*, 58 J. OF NAVIGATION 181 (2005); Jay A. Creech & Joseph F. Ryan, *AIS The Cornerstone of National Security*, 56 J. OF NAVIGATION 31, 31-44 (2003).

[63] *See* J. Carson-Jackson, *Satellite AIS—Developing Technology or Existing Capability?*, 65 J. OF NAVIGATION 303, 304-07 (2012) (noting AIS was "never intended to be received by satellites" and that authorities noticed that AIS carried "potential to support a wide range of maritime regulatory and traffic monitoring activities and assist with maritime security"); *see also* Athanassios Goudossis & Sokratis K Katsikas, *Towards a Secure Automatic Identification System (AIS)*, 24 J. OF MARINE SCIENCE & TECH. 410, 410-23 (2019) (discussing new technologies that could reduce some of the security vulnerabilities of AIS).

[64] *See* EunSu Lee et al., *The Maturity of Automatic Identification Systems (AIS) and Its Implications for Innovation*, 7 J. OF MARINE SCI. & INNOVATION 287 (2019).

[65] For an optimistic view *see, e.g.*, Elizabeth Nyman, *Techno-optimism and Ocean Governance: New Trends in Maritime Monitoring*, 99 MARINE POL'Y 30, 30-33 (2019). For a more skeptical discussion, see, for example, Lorenzo Pezzani & Charles Heller, *AIS Politics: The Contested Use of Vessel Tracking at the EU's Maritime Frontier* 44 SCI., TECH., & HUM. VALUES 881, 881-89 (2019).

[66] *See, e.g.*, Abbas Harait-Mokhtariet et al., *Automatic Identification Systems (AIS): Data Reliability and Human Error Implications*, 60(3) J. OF NAVIGATION 373, 373-89 (2007); Jay A. Creech & Joseph F. Ryan, *supra* note 62.

VHF channels, it is also vulnerable to hacking, manipulation, and spoofing.[67] Despite this evidence that the AIS-based information cannot be fully trusted, its application continues to expand into new contexts.[68]

C. Long-Range Identification and Tracking (LRIT)

International maritime regulators have also expanded vessel tracking requirements beyond AIS through a separate Long-Range Identification and Tracking (LRIT) system. In 2006, the IMO Maritime Safety Committee once again amended SOLAS to require qualifying vessels to "be fitted with a system to automatically transmit" information including the ship's identity, its position, and the date and time of the message.[69] This LRIT framework is designed to provide for the global identification and tracking of ships, whereby transmitting equipment carried on ships relays information to be collected in an international LRIT data exchange accessible by flag states, port states, coastal states, and search and rescue authorities.[70]

Unlike AIS, LRIT data is not relayed on a VHF band; instead, LRIT utilizes the same equipment required to be carried on ships for the purpose of the GMDSS (although this equipment must be slightly reconfigured).[71] Due to this satellite-linked technology, LRIT is capable of automatically transmitting the necessary information "without human intervention" at 6-hour intervals.[72] Although the data is automatically transmitted, LRIT still relies on shipborne equipment and is therefore not "passive" like radar or optical satellite-driven observation tools that might be able to track vessels without the vessel operator's participation.[73] Instead, LRIT is described as a "cooperative" system requiring interaction with the equipment carried on vessels, the orbiting satellites, and designated shore-based data collection

---

[67] The US Coast Guard also acknowledges this on its FAQ website: "AIS by design is an open, non-proprietary, unencrypted, unprotected radio system, intended to operate on non-secure VHF-FM channels. So technically it can be spoofed—*so trust, but verify*. Should you encounter ghost or fake AIS targets, please report them to us." *See* United States Coast Guard, *AIS Frequently Asked Questions* https://www.navcen.uscg.gov/?pageName=AISFAQ#1 (emphasis in original).

[68] To address this informational integrity problem, researchers have attempted to measure AIS signals to determine whether a gap in AIS indicates intentional manipulation or unintentional technical failure. *See* Fabio Mazzarella et al., *A Novel Anomaly Detection Approach to Identify Intentional AIS On-Off Switching*, 78 EXPERT SYS. WITH APPLICATIONS 110, 110-23 (2017).

[69] *See* Maritime Safety Committee, *Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended*, MSC.202(81) (May 19, 2006), paras. 4-5.

[70] *Id.*

[71] *Id.* para. 4.

[72] *Id.*

[73] For an overview of the policy rationale driving the LRIT framework, *see* Jason M. Krajewski, *Out of Sight, Out of Mind? A Case for Long Range Identification and Tracking of Vessels on the High Seas*, 56 NAVAL L. REV. 219, 223 (2008).

centers.[74]

One of the critical distinctions between LRIT and AIS is that the information transmitted via LRIT is not intended to be relayed to other ships or to the broader public. Instead, LRIT data is designed to be for government use only, which may include various state actors such as the vessel flag state administration, the port state the vessel operator has indicated as the intended destination, or other coastal states within close range of the vessel. As these authorized governmental entities access LRIT information, they are obliged to "recognize and respect the commercial confidentiality and sensitivity of any long-range identification and tracking information they may receive."[75]

Despite their technical differences, LRIT is intentionally subject to some of the same limitations as AIS. Even prior to its adoption, the IMO determined that LRIT systems and equipment "shall be capable of being switched off on board or be capable of ceasing the distribution of long-range identification and tracking information" in certain circumstances.[76] These include "in exceptional circumstances and for the shortest duration possible where the operation is considered by the master to compromise the safety or security of the ship."[77] This LRIT switch-off possibility is a surprising choice from a regulatory perspective, as the confidential nature of the LRIT data exchange limits the scenarios where a shipmaster would need to deactivate LRIT to avoid tracking by dangerous non-state actors such as pirates who in theory should not have access to such data in the first place.[78]

The original purposes of LRIT are limited to maritime safety and security issues, including enhancing search and rescue by improving the GMDSS.[79] But even during its development, there was an apparent intention to utilize LRIT data to improve maritime domain awareness more generally.[80] After its adoption, the United States, for instance, immediately implemented domestic regulations requiring a wide range of ships either bound for a US port or traveling within 1,000 nautical miles from the US

---

[74] *Id.* at 223.

[75] *See* Maritime Safety Committee, *Adoption of Amendments to the International Convention for the Safety of Life at Sea*, *1974, as Amended*, MSC.202(81) (May 19, 2006), 10.2.

[76] *Id.* para. 7.

[77] *Id.*

[78] A counterpoint is that hostile state-affiliated actors may utilize access to confidential LRIT data to target merchant ships. Such politically motivated attacks have unfortunately occurred in recent years, which supports the position that merchant shipmasters should retain some level of discretion to deactivate LRIT to avoid security risks. *See, e.g.*, Patrick Kingsley et al., *Israel's Shadow War with Iran Moves Out to Sea*, N.Y. TIMES, Mar. 26, 2021; Courtney McBride, *U.S. Says Drone Fragments Recovered From Israeli-Linked Tanker Point to Iran's Role in Attack*, WALL STREET J., Aug. 6, 2021.

[79] *See* Maritime Safety Committee, *Guidance to Search and Rescue Services in Relation to Requesting and Receiving LRIT Information*, MSC.1/Circ.1338 (Mar. 1, 2011).

[80] *See* Krajewski, *supra* note 73, at 229.

coast to relay LRIT data for security surveillance.[81] But LRIT, like AIS, has also been used for the purpose of broadly enhancing maritime law enforcement.[82] In response to a significant uptick in maritime piracy occurring off the coast of Somalia, the IMO Maritime Safety Committee established a "distribution center" in 2010 for security forces operating in the waters of the Western Indian Ocean, noting that "LRIT information could provide a very useful source of data" for the security forces to build a "holistic picture."[83] In establishing this new distribution center, the Maritime Safety Committee recognized that although it is not part of the original LRIT framework, the center is designed to "leverage the LRIT technical architecture in order to accomplish its goal, without any prejudicial impact" on the system.[84]

III. VESSEL TRACKING AND MARITIME SANCTIONS

Although mandatory vessel tracking processes imposed by the international legal framework were built to facilitate safe and secure navigation, over the years these tools—particularly AIS—have also been used for intelligence gathering. This includes law enforcement efforts attempting to address illegal fishing, environmental crimes, contraband smuggling, piracy, and human trafficking.[85] As sanctioning authorities have increasingly zeroed-in on maritime transport as a means of strengthening the impact of economic sanctions, they have also begun utilizing vessel tracking tools for enforcement actions and referencing them in regulatory guidance. The redirection of vessel tracking tools in the sanctions context has also forced the shipping industry to bear a compliance burden that includes vessel tracking to facilitate counterparty due diligence and contractual risk mitigation efforts.

A. Enforcement Actions

Contemporary multilateral sanctions, such as UN-level trade restrictions targeting North Korea, reflect a focused pivot to maritime transport regulation. This technique is evident in the language of recent U.N. Security Council Resolutions imposing maritime trade restrictions, such as prohibitions on the export of coal out of North Korea and quotas limiting its

---

[81] *See* 33 CFR Part 169; United States Coast Guard, *Long Range Identification and Tracking (LRIT) Overview*, https://www.navcen.uscg.gov/?pageName=lritMain (last visited Aug. 4, 2021).

[82] *See* Maritime Safety Committee Res. 87/26/Add.1/Annex 15 (May 21, 2010).

[83] *Id.*

[84] *Id.*; *see also* Maritime Safety Committee Res. 83/28/Add.2/Annex 6 (Oct. 12, 2007) ("Contracting Governments may request, receive, and use LRIT information for safety and marine environment protection purposes.").

[85] *See, e.g.*, Fournier et al., *supra* note 61; Svanberg et al., *supra* note 61; Creech & Ryan, *supra* note 62.

access to the import of petroleum.[86] The dependence of these sanctions on maritime industry participation is also reflected by compliance monitoring initiatives administered under U.N. auspices. Recent reports of the U.N. Panel of Experts tasked with tracking the effectiveness of North Korea sanctions have described a series of deceptive maritime practices used to conduct prohibited trades.[87] Among these tactics are sophisticated ship identity laundering techniques accomplished by disguising participating vessels with fraudulent profiles involving the deactivation, manipulation, and spoofing of AIS transmissions.[88]

Unilateral sanctions, especially those promulgated by the United States, have also recently emphasized a strategy of regulating maritime transport to pressure actors linked to North Korea, Iran, Syria, Venezuela, and now also Russia.[89] These trade restrictions have been paired with the threat of civil penalties, blacklisting, and secondary sanctions against those who do business with Specially Designated Nations (SDNs). Enforcement measures of this kind are primarily administered by the US Department of Treasury Office of Foreign Assets Control (OFAC), which keeps a list of SDNs, including vessels, that the international trade community must consult for sanctions compliance purposes, or otherwise risk the prospect of serious fines.[90] Press releases describing these enforcement actions have indicated OFAC's reliance on intelligence gathering that utilizes vessel tracking technology for the purpose of discovering deceptive sanctions circumvention

---

[86] *See, e.g.,* S.C. Res. 2397 (Dec. 22, 2017); S.C. Res. 2375 (Sept. 11, 2017).

[87] *See* Final Rep. of Experts, *supra* note 2, ¶¶ 17-40; *see also* Midterm Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009), transmitted by Note by the President of the Security Council, ¶¶ 13–42, U.N. Doc. S/2021/777 (Sept. 8, 2021).

[88] *See* Midterm Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009), transmitted by Note by the President of the Security Council, ¶¶ 13-42, U.N. Doc. S/2021/777 (Sept. 8, 2021).

[89] *See, e.g.*, OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, OFAC ADVISORY TO THE MARITIME PETROLEUM SHIPPING COMMUNITY: SANCTIONS RISKS RELATED TO PETROLEUM SHIPMENTS INVOLVING IRAN AND SYRIA (2019); *Treasury Targets Maritime Entities for Supporting Illegitimate Maduro Regime in the Venezuela Oil Trade*, U.S. DEP'T OF THE TREASURY, (June 2, 2020), https://home.treasury.gov/news/press-releases/sm1022. At the time of this writing, less than one month after the Russian invasion of Ukraine, sanctions applied to Russia-linked economic activities are evolving rapidly. The United States and other governments have imposed wide-ranging sanctions impacting maritime activities; however, multilateral sanctions from the U.N. Security Council are unlikely to materialize since Russia is a permanent member with veto power. *See e.g.*, Office of Foreign Assets Control, *Issuance of New Russia-related Executive Order and Related License 16* (Mar. 8, 2022), U.S. DEP'T OF THE TREASURY https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220308; *Fact Sheet: United States Bans Imports of Russian Oil, Liquified Natural Gas, and Coal*, (Mar. 8, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/08/fact-sheet-united-states-bans-imports-of-russian-oil-liquefied-natural-gas-and-coal/.

[90] *See* Office of Foreign Asset Control, *Specially Designated Nationals and Blocked Persons Lists (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

practices.[91]

The US Department of Justice (DOJ) has also increasingly played a role in enforcing maritime sanctions, including the coordination of vessel and cargo seizure and forfeiture.[92] Intelligence gathering related to these actions has focused on monitoring vessel movements primarily relying on AIS data. In May 2019, the DOJ took the extraordinary step of seizing North Korea's second-largest bulk carrier, the *M/V Wise Honest,* in the territorial waters of Indonesia.[93] Indonesian authorities had detained the *Wise Honest* when it was discovered drifting off its coast with deactivated AIS shortly after it had been photographed loading illicit coal at a North Korean port. DOJ officials secured a warrant from a U.S. magistrate judge to seize the vessel.[94] After executing the seizure with the aid of Indonesian authorities, DOJ officials filed a civil complaint in the U.S. Southern District of New York alleging that the *Wise Honest* was property subject to forfeiture under U.S. law.[95] In the complaint, the DOJ highlighted deactivated AIS as a red flag, describing that "the fact that a vessel has turned off its AIS transmissions is typically evidence of an attempt to avoid detection."[96] On these grounds, the complaint alleged the *Wise Honest* "attempted to conceal information about its location, course, speed, or other navigational status while in the course of transporting

---

[91] *See, e.g.*, Office of Foreign Assets Control, *Press Release: Treasury Announces Largest North Korean Sanctions Package Targeting 56 Shipping and Trading Companies and Vessels to Further Isolate Rogue State*, U.S. DEP'T OF THE TREASURY (Feb. 23, 2018), https://home.treasury.gov/news/press-releases/sm0297; *see also* U.S. DEP'T OF TREASURY OFF. OF FOREIGN ASSETS CONTROL, *Press Release: Treasury Sanctions Shipping Companies Transporting North Korean Coal,* U.S. DEP'T OF THE TREASURY (Dec. 8, 2020), https://home.treasury.gov/news/press-releases/sm0297; OFF. OF FOREIGN ASSETS CONTROL, *Press Release: Treasury Designates Vast Iranian Petroleum Shipping Network that Supports IRGC-QF and Terror Proxies*, U.S. DEP'T OF THE TREASURY (Sept. 4, 2019), https://home.treasury.gov/news/press-releases/sm767.

[92] Other governments have engaged in similar enforcement measures when sanctions-busting vessels have operated in their waters. *See, e.g.*, Edna Tarigan, *Indonesia Says It Has Seized Iranian and Panamanian Tankers,* ASSOCIATED PRESS, Jan. 24, 2021, https://apnews.com/article/indonesia-iran-f8f4b6889418e3ad9ef798bc52a80774; Yuna Park & Hyunjoo Jin, *South Korea Seizes Second Ship Suspected of Providing Oil to North Korea*, REUTERS, Dec. 31, 2017. Sanctioning authorities have already begun seizing Russia-linked vessels, including merchant ships and private yachts. *See, e.g.*, Pascal Rossignol, *France, Enforcing Sanctions on Russia, Seizes Ship in Channel*, REUTERS, Feb. 26, 2022, https://www.reuters.com/world/europe/france-seizes-ship-suspected-violating-russia-sanctions-official-2022-02-26/.

[93] *See* U.S. DEP'T OF JUSTICE, *Press Release: North Korean Cargo Vessel Connected to Sanctions Violations Seized by U.S. Government*, May 9, 2019, https://www.justice.gov/opa/pr/north-korean-cargo-vessel-connected-sanctions-violations-seized-us-government.

[94] Verified Complaint for Forfeiture para. 45, *United States of America v. The Bulk Cargo Carrier Known as the "Wise Honest," Bearing International Maritime Organization Number 8905490*, No. 1:19-cv-04210 (S.D.N.Y. 2019) (asserting that warrant authorizing seizure was issued July 17, 2018), https://www.justice.gov/opa/press-release/file/1161356/download.

[95] *Id.*

[96] *Id.* para. 34.

coal from North Korea to Indonesia."[97] Subsequently, U.S. officials worked with Indonesian authorities to tow the *Wise Honest* to American Samoa, where it was eventually sold.[98]

In a similar move in April 2021, the DOJ filed an action to enforce the forfeiture of the tanker *M/T Courageous* on grounds that the vessel had been involved in trades that violate North Korea sanctions.[99] In its complaint, the DOJ argued that the *Courageous* attempted to circumvent the sanctions by concealing the nature of its activities. Under the heading, "M/T Courageous Goes Dark," the DOJ complaint read, "the fact that a vessel has turned off its AIS transmissions is typically evidence of an attempt to avoid detection."[100] Since the *Courageous* turned off its AIS signal for a period of four months, the DOJ argued, "[t]he disabling of AIS is consistent with other DPRK-related efforts to avoid sanctions."[101]

A slightly more complex case brought by the DOJ in 2021 involves crude oil carried on the *M/T Achilleas*, which allegedly originated from oil terminals in Iran to facilitate transactions involving sanctioned entities linked to the Iran Revolutionary Guard Corps.[102] In the complaint, the DOJ cited intelligence demonstrating a complex web of ship-to-ship transfers and AIS manipulation leading to the sanctioned cargo being carried by the *Achilleas*. The complaint alleged a tanker linked to Iran's national tanker company, the *M/T Humanity,* "spoofed" another vessel called the *M/T Lubov* by "assuming [its AIS] parameters."[103] "Based on satellite imagery," the DOJ alleged that the *Humanity* "shut off her AIS transponder" and sailed along the Persian

---

[97] *Id*. para. 36.

[98] *See* U.S. DEP'T OF JUSTICE, *Press Release: Department of Justice Announces Forfeiture of North Korean Cargo Vessel*, Oct. 21, 2019, https://www.justice.gov/opa/pr/department-justice-announces-forfeiture-north-korean-cargo-vessel. The proceeds from the sale were reportedly transferred to the family of Otto Warmbier, an American college student who suffered a fatal injury while in North Korean custody. This arrangement was made after the Warmbier family filed an action in rem against the vessel to satisfy a judgment of $500 million issued by the US DC District Court. *See Seized North Korean Cargo Ship sold to Compensate Parents of Otto Warmbier, Others*, NAVY TIMES, Oct. 9, 2019, https://www.navytimes.com/news/your-navy/2019/10/09/seized-north-korean-cargo-ship-sold-to-compensate-parents-of-otto-warmbier-others; Marisa Iati, *Otto Warmbier's Family is Suing for North Korean Coal Ship Seized by U.S. Officials*, WASHINGTON POST, July 6, 2019, https://www.washingtonpost.com/world/2019/07/06/otto-warmbiers-family-is-suing-north-korean-coal-ship-seized-by-us-officials.

[99] Complaint, *United States of America v. The Tanker Vessel Known as the "Courageous," Bearing International Maritime Organization Number 8617524*, No. 1:21-CV-03636 (SDNY 2021).

[100] *Id.* at 13.

[101] *Id.* at 14.

[102] United States' Verified Complaint for Forfeiture *In Rem*, *United States v. All Petroleum-Product Cargo Aboard the Achilleas with International Maritime Organization Number 9398072*, No. 1:21-CV-00305 (D.D.C. 2021), 2021 WL 386496.

[103] The complaint defined AIS spoofing as "a technique where a ship manipulates its AIS transponder to transmit false data such as a ship's location or name." *Id.* at 7.

Gulf to "temporarily assume her new identity" as the *Lubov*.[104] Meanwhile, the real *Lubov* conducted a series of ship-to-ship transfers with other vessels to load petroleum-product cargo "with her AIS transponder switched off."[105] Then the real *Lubov* engaged in a five day ship-to-ship transfer with the *Trident Liberty*, which subsequently indicated via AIS data that it was fully laden with two million barrels of oil.[106] Several months later, the complaint contended, the *Trident Liberty* transferred the illicit crude to the *Achilleas* via ship-to-ship transfer in the Gulf of Oman.[107] By tracking the cargo transfers from the *Lubov* to the *Trident Liberty* and finally to the *Achilleas*, the DOJ asserted that the cargo was sanctionable and subject to seizure.

Flag state registries around the world have also recently engaged in sanctions enforcement by de-flagging ships that have performed sanctions-evading trades. In 2019, Panama, among the most popular flag registries in the world, announced that it would withdraw its flag from any vessel that violates sanctions.[108] Other less-popular flag registries, including the Cook Islands, Gabon, St. Kitts and Nevis, and Tanzania, have also de-flagged vessels for isolated, sanctions-related offenses.[109] These decisions were also reportedly based on suspicious gaps in AIS transmission or AIS data indicating participation in illicit ship-to-ship transfers.[110] It is important to recall, however, that certain flag states—namely open registries—are sometimes managed by private business entities based in offices thousands of miles from the geographic territory of the flags they represent.[111]

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *See* Marianna Parraga & Elida Moreno, *Exclusive: Panama to Withdraw Flags from More Vessels that Violate Sanctions*, REUTERS, July 12, 2019, https://www.reuters.com/article/mideast-iran-tanker-panama-exclusive-idINKCN1U72E9; Alonso Illueca, *On Sanctions and Deregistration of Vessels: The Recent Practice of Panama*, OPINIO JURIS, July 24, 2019, http://opiniojuris.org/2019/07/24/on-sanctions-and-deregistration-of-vessels-the-recent-practice-of-panama.

[109] *See*, *e.g.*, Michelle Wiese Bockmann, *Gabon Deflags Iranian Tanker*, LLOYD'S LIST, Feb. 11, 2020; Michelle Wiese Bockmann, *Tanzania De-flags Tankers for 'Illicit Transfers" of Iranian Crude*, LLOYD'S LIST, Oct. 27, 2020.

[110] *Id*. These actions serve as counterpoint to criticism that "flags of convenience" are complicit in sanctions circumvention. *See, e.g.*, Christopher J. Watterson, Stephen Osborn, & Samuel Grant, *Open Registries as Enabler of Maritime Sanctions Evasion*, 119 MARINE POL'Y 104090 (2020). Cameroon, Togo, Djibouti, and Sierra Leone are thought to be some of the open registries allowing "subterfuge tankers" to operate under their flags. *See* Michelle Wiese Bockmann, *An Inconvenient Truth: Flags Failing*, LLOYD'S LIST, Feb. 5, 2021.

[111] For instance, the popular registries of Liberia and the Marshall Islands, are both based in Virginia. *See* Liberian Registry, *About the Liberian Registry*, https://www.liscr.com/about-liberian-registry (last visited Feb. 17, 2022); International Registries, Inc., *About IRI*, https://www.register-iri.com/about-iri/ (last visited Feb. 17, 2022) (The flag registry of Gabon is based in Amjan, United Arab Emirates). *See* Intership Services, LLC, *About Intership Services*, http://www.intershippingservices.com/about-intershippingservices.php.

Consequently, these actors could have little connection to state intelligence agencies and may need to rely on information from external investigations.[112]

In these monitoring and enforcement actions, authorities have substantially relied on AIS data to track vessel movements and discover illicit transactions at sea. By scrutinizing vessel tracking data for irregularities, such as deactivation, manipulation, or spoofing, these authorities have utilized information originally designed for navigational safety purposes to facilitate sanctions surveillance and intelligence gathering. Remarkably, however, in the publicly available documents describing these efforts, there is scant reference to other data subject to the international legal framework governing vessel tracking, such as data flowing from LRIT or GMDSS-compliant equipment. While court documents do occasionally reference satellite imagery to justify enforcement, details are limited regarding the technical source of this data and whether it is open-source, commercially available, or military grade.[113]

B. Regulatory Guidance

Recent maritime sanctions have generated nervous energy across the shipping industry. Much of this buzz is driven by what industry participants view as an uncomfortable call to action from regulators to shore up sanctions compliance.[114] During the last decade, U.N. Member States began sounding the alarm that more shipping industry participation in sanctions monitoring was necessary to verify the identities and activities of at-risk actors through technology-driven screening.[115] After the U.N. Security Council imposed new rounds of economic sanctions pressure on North Korea in 2017 through updated Resolutions adopting maritime restrictions, a subsequent U.N. Panel of Experts Report urged shipping industry participants to engage in vessel

[112] *See* Bockmann, *Tanzania De-flags Tankers for 'Illicit Transfers" of Iranian Crude*, *supra* note 109 (discussing letters sent to flag registries by NGO United Against a Nuclear Iran indicating the findings of its own vessel tracking investigations).

[113] Conventional law enforcement methods such as naval patrols continue to play a role in sanctions compliance monitoring as well. *See, e.g.*, United Kingdom Ministry of Defense, *Press Release: UK Conducts U.N. Sanctions Enforcement to Counter North Korea's Weapons Programmes* (Sept. 26, 2021), https://www.gov.uk/government/news/uk-conducts-un-sanctions-enforcement-to-counter-north-koreas-weapons-programmes (describing the use of UK Navy frigates to track suspected vessels and collect video and photographic evidence of ships breaching sanctions).

[114] *See* Lloyd's List, *Shipping's Compliance Risk Conundrum*, May 21, 2021; Sebastian Villyn, *A Message to the Marine Insurance Market: Conduct Your KYC or Risk Fines*, LLOYD'S LIST, July 28, 2021.

[115] *See*, *e.g.*, U.N. SCOR., *Letter Dated 15 January 2015 from the Permanent Representatives of Australia and Singapore to the United Nations Addressed to the President of the Security Council*, U.N. Doc. S/2015/28 (2015) at paras. 50-53 (recommending increased due diligence efforts to ensure private sector sanctions compliance, including the commercial use of vessel tracking via AIS-dependent monitoring, and the flag state use of INMARSAT satellite-dependent tracking).

tracking to support "far greater private sector due diligence, information-sharing and self-policing."[116] The U.N. Panel of Experts also recommended that private shipping industry actors, including insurers, commodity traders, and other members of the international trade community implement AIS monitoring tools and verification measures.[117]

Since 2018, U.S. officials have also recommended shipping industry participants, including shipowners, charterers, insurers, and others to carefully examine the identity of counterparties and even track their vessel movements.[118] An already infamous May 2020 Sanctions Advisory, issued jointly by the Department of Treasury, Department of State, and Coast Guard, directs the private sector to bolster its compliance using technology.[119] This Sanctions Advisory urges the shipping community to "adopt business practices addressing red flags and other anomalies that may indicate illicit or sanctionable behavior."[120] These include the implementation of "AIS best practices" such as, "researching a ship's history to identify previous AIS manipulation and monitoring AIS manipulation and disablement when cargo is in transit" and also to "promote continuous broadcasting of AIS throughout the life of the transaction."[121] The Sanctions Advisory even suggests private industry participants "consider amending contracts to make disabling or manipulating AIS for illegitimate reasons, grounds for termination . . . if illicit sanctionable activity is identified." [122]

The Annex to the Sanctions Advisory is even more explicit on recommendations for private sector vessel tracking. It urges marine insurance companies to engage in compliance practices such as "[m]onitoring [AIS] transmissions" to determine whether an insured vessel has "a pattern of turning off AIS in a manner inconsistent with SOLAS" or "engaging in trade to or from vessels that are not transmitting AIS consistent with SOLAS."[123]

---

[116] *See Rep. of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, U.N. Doc. S/2018/171, at 4 (Mar. 5, 2018). For an overview of these recommendations and the impact on merchant shipping, *see* Richard L. Kilpatrick, Jr. *North Korea's Sanctions-Busting Maritime Practices: Implications for Commercial Shipping*, 37 CHINESE (TAIWAN) Y.B. INT'L L. & AFF. 199 (2019).

[117] *Id.*

[118] *See, e.g.*, *OFAC North Korea Sanctions Advisory: Sanctions Risks Related to North Korea's Shipping Practices*, U.S. DEP'T TREASURY (Feb. 23, 2018); *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Shipping Petroleum to Syria*, U.S. DEP'T TREASURY (Nov. 20, 2018); *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risks Related to Petroleum Shipments Involving Iran and Syria*, U.S. DEP'T TREASURY (Mar. 25, 2019); *North Korea Sanctions Advisory: Updated Guidance on Addressing North Korea's Illicit Shipping Practices* (Mar. 21, 2019); *OFAC Advisory to the Maritime Petroleum Shipping Community*, U.S. DEP'T TREASURY (Mar. 4, 2019).

[119] U.S. Sanctions Advisory, *supra* note 6.

[120] *Id*. at 3.

[121] *Id.* at 4.

[122] *Id.*

[123] *Id.* at 9.

It also recommends insurers engage in "pre-coverage" due diligence, assessing the "AIS history of vessels that engage in potentially illegal activities and operate in areas determined to be high-risk areas for sanctions evasion."[124] It further recommends that commodity traders, suppliers, brokers, vessel captains, and even crewing companies engage in at least some form of AIS vetting, and advises shipowners, operators, and charterers adopt an "AIS switch-off clause" that would allow them to terminate contracts if a counterparty "demonstrates multiple instances of AIS manipulation that is inconsistent with SOLAS."[125]

Controversially, the Sanctions Advisory also encourages shipowners, managers, and charterers, to continuously monitor vessels through means that "include supplementing AIS with [LRIT] and receiving periodic LRIT signals."[126] The Annex also goes further in recommending private actors "consider using LRIT in addition to AIS and receiving LRIT signals every 3 hours."[127] Remarkably, the Sanctions Advisory and the Annex make no mention of the confidential nature of LRIT data and do not explain how private entities would be able to evaluate data that is designed for government access only.[128]

A UK Guidance issued by the HM Treasury Office of Financial Sanctions Implementation in December 2020 largely aligns with the U.S. recommendations in citing AIS manipulation as a red flag for sanctions violations and encouraging private sector participation in compliance tracking.[129] Although less comprehensive (and arguably softer in tone) than the U.S. Sanctions Advisory on the issue of vessel tracking, the UK Guidance provides that shipowners, charterers, insurers, flag registries, and port state control entities "may wish to consider any benefits in AIS screening and the inclusion of 'AIS switch off' clauses in contracts" for the purpose of due diligence.[130] The UK Guidance, however, is careful to emphasize that there could be "legitimate reasons for AIS to be turned off or go dark" such as to avoid the risk of piracy or due to technical connectivity problems.[131] It also diverges from the U.S. Advisory in that the UK Guidance does not mention a private sector role in monitoring LRIT or other forms of vessel tracking.

---

[124] *Id*.

[125] *Id*. at 18. The Advisory and Annex further encourage public authorities, including flag state registries and port state control authorities, to utilize AIS monitoring. *Id.* at 11-14.

[126] *Id*. at 5.

[127] *Id*. at 18.

[128] *Id*. LRIT monitoring is also encouraged for flag registry managers. *Id.* at 11-15.

[129] *See* UK HM Treasury Office of Financial Sanctions Implementation, *Maritime Guidance: Financial Sanctions Guidance for Entities and Individuals Operating within the Maritime Shipping Sector* (Dec. 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948299/OFSI_Guidance_-_Maritime_.pdf.

[130] *Id.* at 8.

[131] *Id*. at 3.

C. Compliance Initiatives

These regulatory advisories demonstrate a current dependance on private sector sanctions due diligence. But to accomplish this task, commercial actors must have the tools. Ship monitoring websites such as fleetmon.com, marinetraffic.com, and vesseltracker.com, which collect and display AIS data, have long been popular for hobbyist ship watchers and industry participants wishing to keep tabs on the movements of cargo.[132] Although these tools were developed with broad transparency interests in mind, the information that they display is not suited for the level of sanctions due diligence required by regulators. Instead, the recent regulatory demands have led to an impressive proliferation of new vessel tracking products designed to help shipping industry participants track vessels for the purpose of sanctions compliance through data collection, artificial intelligence, and machine-learning analysis, re-packaged in user-friendly platforms.

Among these tracking products is the Lloyd's List Intelligence Seasearcher Advanced Risk & Compliance product.[133] This platform is marketed as utilizing machine learning to gain insight into vessel behavior and detect "dark" port callings, ship-to-ship transfers, and AIS manipulation.[134] It is described as tracking AIS transmissions to look for gaps, and then using artificial intelligence, it evaluates other relevant variables such as high risk locations, distance traveled, and changes in the vessel draught which might demonstrate undeclared loading or unloading.[135] A recent Lloyd's List report utilized this tool to help uncover deceptive practices performed by a "subterfuge fleet" of more than 160 tankers used to evade U.S. sanctions on petroleum products shipped out of Iran and Venezuela.[136]

The Israeli company Windward is another provider selling digital products for maritime sanctions compliance.[137] Windward markets itself as a

---

[132] *See* Fleetmon, *About Fleetmon*, https://www.fleetmon.com/company/our-story/; Marine Traffic, *About U*s, https://www.marinetraffic.com/en/p/company; Vessel Tracker, *Innovation Since 2006*, https://www.vesseltracker.com/en/static/about_vesseltracker.html.

[133] *See* Lloyd's List, *Lloyd's List Intelligence Unveils AIS Risk Analysis Platform*, July 5, 2021, https://lloydslist.maritimeintelligence.informa.com/LL1137446/Lloyds-List-Intelligence-unveils-AI-risk-analysis-platform.

[134] Lloyd's List Intelligence Seasercher Advanced Risk & Compliance, https://www.lloydslistintelligence.com/services/data-and-analytics/advanced-risk-and-compliance.

[135] *Id*.

[136] Richard Meade & Michelle Wiese Bockmann, *The Sanctions-Skirting Secrets of Shipping*, LLOYD'S LIST INTELLIGENCE, July 2021, https://images.intelligence.informa.com/Web/InformaUKLimited/%7Bc86d2824-6198-4660-85d0-2b7df5469ab3%7D_Sanctions_Skirting_of_Shipping_Whitepaper.pdf; These tools have also uncovered similar tactics adopted by actors seeking to circumvent the new Russia-related sanctions. See Michelle Wiese Bockmann, *Tankers Shipping Venezuela and Iranian Crude Switch to Russian Trade,* LLOYD'S LIST, June 8, 2022.

[137] *See* Windward, *About Us*, https://windward.ai/company/about-us/.

maritime risk management and intelligence company offering programs for counterparty due diligence, including analysis of ownership structures and vessel behaviors using AIS data and artificial intelligence.[138] Its website describes a "Know Your Vessel" product for sanctions compliance vessel-vetting, using processes that "go beyond compliance risk" and "stay ahead of emerging typologies and evolving trends with [] predictive insights."[139] This is accomplished using machine learning to scrutinize vessel movements for red flags.[140] Although commercially available, Windward is also cited in recent U.N. Panel of Experts Reports as one of its resources for investigating North Korea sanctions circumvention.[141]

Some companies are offering products that focus on satellite imagery to facilitate commercial intelligence for compliance purposes. Planet Labs utilizes satellites to capture imagery that can be used to monitor maritime spaces, detect vessels, and search for behavioral anomalies.[142] It can also be used along with AIS monitoring to observe sea areas where a vessel has deactivated its AIS signal.[143] Maxar Technologies offers a similar product, although it is described as being less dependent on AIS transmissions.[144] In its marketing materials, Maxar Technologies has described its maritime monitoring capabilities as providing "near-real-time" surveillance relying on "space-based optical and radar imagery and advanced machine learning."[145] This includes the use of synthetic aperture radar technology, which has been touted as having the capacity to recognize ships even in cloudy conditions.[146]

One of the more controversial approaches in maritime compliance data mining is the potential private marketability of LRIT data. Although IMO documents indicate LRIT data is designed to be accessible only by

---

[138] *Id*.

[139] *See* Windward, *Know Your Vessel*, https://windward.ai/solutions/know-your-vessel/.

[140] Windward's vessel-tracking technology has also received a patent from the U.S. Patent and Trademark Office. *See* USPTO Patent Number 10,922,981, *Risk Event Identification in Maritime Data and Usage Thereof* (Feb. 16, 2021), https://uspto.report/patent/grant/10,922,981.

[141] *See, e.g.,* Final Rep. of Experts, *supra* n. 2, at 17. IHS Markit is another company that offers similar AIS screening products for sanctions compliance purposes utilizing data collection and artificial intelligence. *See* IHS Markit, *Risk & Compliance: Intelligent Solutions for Trade Compliance*, https://cdn.ihsmarkit.com/www/pdf/1021/705690708_RNC_Intelligent-Solutions-for-Trade-Compliance_Oct-2021_Brochure_U1-lores.pdf.

[142] Planet Labs, *Maritime and Coastal Monitoring from Planet,* https://www.planet.com/markets/maritime/; *see also* Robin Kraft, *Experimenting with the Deep Data Stack: Ship Counting*, PLANET LABS, May 4, 2017, https://www.planet.com/pulse/experimenting-with-the-deep-data-stack-ship-counting/.

[143] *Id.*; *See also* Planet Labs*, Planet Partners with SynMax to Provide Energy Intellegence and Monitor Dark Vessels*, April 18, 2022, https://www.planet.com/pulse/planet-partners-with-synmax-to-provide-energy-intelligence-and-monitor-dark-vessels/.

[144] *See* Maxar, *Crow's Nest Maritime Monitoring and Security*, https://resources.maxar.com/on-demand-intelligence/crows-nest-maritime-monitoring-and-security.

[145] *Id.*

[146] *Id.*

governments, such as flag states or coastal states, the recent recommendation from U.S. officials that private actors could use LRIT data to supplement AIS tracking has challenged this interpretation.[147] Shortly after the 2020 U.S. Sanctions Advisory published such recommendations, representatives of UK company Pole Star, which has managed LRIT data for major flag states such as Panama, Liberia, and the Marshall Islands, suggested that commercial maritime actors may be able to purchase its data to ensure compliance with maritime sanctions.[148] In an interview with Lloyd's List, the CEO of Pole Star explained that its ship position reporting technology is "parallel" to the LRIT data collection it performs for flag states.[149] He also clarified that its system, "is technically the same as LRIT but set up separately by Pole Star using INMARSAT or Iridium [satellites] and therefore billed separately to the commercial entity" that purchases the data.[150] On Pole Star's website, its products are also described as utilizing INMARSAT satellite data capable of providing ship location "even when its AIS is unavailable."[151] This practice of distributing LRIT (or LRIT-parallel) data runs counter to the underlying confidentiality concerns raised when LRIT amendments were added to SOLAS, but at the same time it appears to facilitate the recommendations contained in recent US regulatory guidance.[152]

Non-governmental organizations (NGOs) and think tanks have also engaged in their own vessel tracking analysis using commercially available intelligence gathering tools to support investigations on sanctions compliance. Organizations such as the Washington D.C.-based Center for Advanced Defense Studies (C4ADS) and the London-based Royal United Services Institute (RUSI) have issued multiple reports describing North Korea sanctions evasion tactics with a focus on deceptive maritime activities.[153] In its most recent report, C4ADS described a sophisticated

---

[147] *See* discussion *supra* Part III(B).

[148] *See* Michelle Wiese Bockmann, *Government-only Vessel-tracking Data Up for Sale 'with US Approval,'* LLOYD'S LIST, June 19, 2020, https://lloydslist.maritimeintelligence.informa.com/LL1132749/Government-only-vessel-tracking-data-up-for-sale-with-US-approval.

[149] *Id.*

[150] *Id*. In response to the cited Lloyd's List reporting, Pole Star CEO Julian Longson published a right-of-reply highlighting "a number of serious inferences and regrettable choice of words" that were used when describing the Pole Star products and protection of LRIT and other similar data using the same technology. While Longson alleged the Lloyd's List story was "fake news," he did not directly dispute any of the quotations contained in the story. It appears that the point of contention is that Longson believes that Pole Star does not sell privileged government data because the data sold to commercial entities is collected separately.

[151] *See* Pole Star, *PurpleTRAC Update: Extending Your Sanctions Screening & Vessel Tracking Capabilities* (May, 26, 2021), https://www.polestarglobal.com/resources/purpletrac-update-extending-your-sanctions-screening-vessel-tracking-capabilities (last visited Nov. 3, 2021).

[152] *See* discussion *supra* Part II(C) and Part III(B).

[153] *See, e.g.*, Lucas Kuo & Jason Arterburn, *Lux & Loaded: Exposing North Korea's*

process of vessel identity laundering demonstrated through analysis depending on data collected by Windward, Planet Labs, Pole Star, and other vessel tracking technology companies.[154]

Another NGO that has dabbled in sanctions compliance vessel tracking in recent years is the group United Against a Nuclear Iran (UANI), which describes itself as a "nonprofit and non-partisan policy organization."[155] To fulfill its namesake agenda in pressuring Iran, UANI has tracked vessels engaged in Iran-related sanctions circumvention, and describes its methodology as using "AIS, satellite imagery, vessel comparison and tanker classification, and cargo datasets."[156] UANI has used this information to advocate for flag states and even private shipping industry participants to avoid doing business with sanctions-busters. After reportedly receiving a letter from UANI, which showed "satellite imagery" indicating Tanzania-registered vessels engaged in sanctions circumvention activities, Tanzania de-flagged the tankers involved.[157] Multiple P&I clubs also reportedly cancelled membership of Iran-linked vessels after receiving similar letters from UANI suggesting the vessels had spoofed AIS signals to circumvent sanctions.[158]

D. Contractual Risk Allocation

Vessel tracking for commercial purposes has also moved beyond counterparty vetting as shipping industry participants have also reacted to regulatory guidance recommending the incorporation of monitoring measures into commercial agreements. During the last decade, sanctions risk in the maritime sector has already led hull insurers, P&I clubs, shipowners, charterers, and financial institutions to develop sanctions clauses designed to allocate the risk of sanctions exposure.[159] But the recent regulatory push to

Strategic Procurement Networks, C4ADS (2019); Jason Byrne et al., *Black Gold: Exposing North Korea's Oil Procurement Networks*, C4ADS & RUSI (2021).

[154] Andrew Boling, *Unmasked: Vessel Identity Laundering and North Korea's Sanctions Evasion*, C4ADS 2021; *see also* Anne Pellegrino, *Planet's Data Used to Reveal Illicit Shipping Networks Delivering Fuel to North Korea in Violation of U.N. Sanctions*, PLANET LABS (last visited Sept. 9, 2021), https://www.planet.com/pulse/planets-data-used-to-reveal-illicit-shipping-networks-delivering-fuel-to-north-korea-in-violation-of-un-sanctions/; *see also* Natalia Dinsmore & Dror Salzman, *North Korean Sanctions Evasion: Identity Laundering Explained*, https://windward.ai/blog/north-korean-sanctions-evasion-identity-laundering-explained/ (last visited Sept. 13, 2021).

[155] *See About UANI*, UNITED AGAINST A NUCLEAR IRAN, https://www.unitedagainst nucleariran.com/about (last visited Feb. 18, 2022).

[156] *See Iran Tanker Tracking*, UNITED AGAINST A NUCLEAR IRAN, https://www.unitedagainstnucleariran.com/tanker-tracker (last visited Feb. 18, 2022).

[157] *Id.*

[158] *See* Michelle Wiese Bockmann, *Marine Insurers Cancel 'Spoofing' Iran-linked Ships*, LLOYD'S LIST, Oct. 4, 2021.

[159] For a comprehensive discussion of these clauses, *see generally* Richard L. Kilpatrick, Jr. "Maritime Sanctions Clauses" LLOYD'S MARITIME AND COMMERCIAL LAW QUARTERLY

track vessels for sanctions compliance has further mobilized the development of AIS switch-off clauses for the purpose of contractually addressing rights and responsibilities relating to sanctions evasion red flags such as gaps in AIS transmission or suspicious ship-to-ship transfers.

In July 2021, the Baltic and International Maritime Council (BIMCO) published an AIS Switch Off Clause for Time and Voyage Charter Parties.[160] The BIMCO background note to the clause explains that the reason for its development flows from the publication of the U.S. and UK regulatory guidance recommending that shipping industry participants utilize contract clauses that provide grounds for termination when AIS has been deactivated or manipulated. After consultation with industry actors attempting to comply with these recommendations, BIMCO recognized that "ad hoc" AIS switch-off clauses were materializing on the market. While BIMCO has expressed the opinion that "AIS as such is not a sanctions tool" and is instead designed for navigational safety, concern about the "shortcomings of such 'ad hoc' clauses" led the BIMCO Documentary Committee to create its own standard AIS switch off clause.[161] This clause now adds to its growing menu of BIMCO-endorsed sanctions clauses.[162]

The BIMCO AIS Switch Off Clause assigns warranties from both the shipowner and charterer, which depend on compliance with the IMO AIS Guidelines.[163] The shipowner's warranty provides in relevant part:

> (b) Owners warrant that for the six (6) months prior to the arrival of the Vessel at the first or sole loading port under this Charter Party and throughout its duration they have not knowingly operated and will not knowingly operate the Vessel's AIS other than in accordance with the Guidelines. This includes, but is not limited to, not manipulating, knowingly switching off or otherwise disabling the Vessel's AIS other than in accordance with the Guidelines.[164]

The charterer's warranty is relayed as follows:

565, 565-83 (2020).

[160] BIMCO, *AIS Switch Off Clause 2021*, https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/ais_switch_off_clause_2021 [hereinafter BIMCO AIS Switch Off Clause].

[161] *Id.*; *see also* Mett Kronholm Fraende, BIMCO, *The Severe Risks and Repercussions of Switching Off the AIS*, http://portfolio.cpl.co.uk/BIMCO/202106/security/ (quoting Grant Hunter, then Head of Contracts and Clauses at BIMCO: "[t]he problem we have seen emerging is that the AIS clauses that many have started adding to the contracts are badly drafted").

[162] *See*, *e.g.*, BIMCO, *Sanctions Clause for Time Charter Parties 2020*; BIMCO, *Sanctions Clause for Voyage Charter Parties 2020*; BIMCO, *Sanctions Clause for Container Vessel Time Charter Parties 2021*.

[163] The Clause clarifies the "'Guidelines' means the IMO Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems, Resolution A.1106(29) or any subsequent amendment thereto." BIMCO AIS Switch Off Clause, *supra* note 160.

[164] *Id.*

> (e) Charterers warrant that throughout the duration of this Charter Party they shall not:
>
> (i) request Owners to operate the Vessel's AIS other than in accordance with the Guidelines. This includes, but is not limited to, manipulating, switching off or otherwise disabling the Vessel's AIS other than in accordance with the Guidelines; or
>
> (ii) give orders to conduct a ship-to-ship cargo transfer (STS) with a vessel whose AIS has not been operated in accordance with the Guidelines throughout the last six (6) months prior to the orders.[165]

If the charterer "reasonably believes" the shipowner has breached its warranty, the charterer "shall request" the shipowner explain the apparent breach, which triggers 72 hours to respond.[166] If indeed the shipowner has breached the warranty, the charterer has the right to terminate the charterparty.[167] At the same time, in the case of a charterer warranty breach, the shipowner may reject the request, terminate the charterparty, and claim damages resulting from the breach.[168]

The BIMCO Guidance Notes to the clause explain that if the AIS is not transmitting, this does not necessarily mean that the shipowner is in breach of its warranty.[169] For instance, if the AIS is switched off for purposes consistent with the IMO AIS Guidelines, such as to protect against the threat of piracy, there is no breach.[170] Likewise, there is no breach if the AIS is switched off for a legitimate purpose and accidently left deactivated after departing a high-risk area, if the AIS is switched off when the ship operator wrongfully believes it is permitted to do so under the IMO AIS Guidelines, or if the AIS equipment malfunctions.[171] Instead, to establish a breach, the charterer must demonstrate that the AIS was switched off "knowingly" for the purpose of evading sanctions.[172]

To facilitate information gathering about a possible breach, the charterer is granted the right to request information from the shipowner. The purpose of this part of the clause is to facilitate communication in certain situations, such as when the charterer receives information from a third-party vessel tracking company that there has been a suspicious AIS switch off.[173] But the Guidance Notes clarify that this does not grant the charterer the right to demand information from the shipowner each time AIS is not transmitted

---

165 *Id*.
166 *Id*. at subclause (c).
167 *Id.* at subclause (d).
168 *Id.* at subclause (f).
169 BIMCO AIS Switch Off Clause, *supra* note 160.
170 *Id.* at guidance note to subclause (b).
171 *Id.*
172 *Id.*
173 *Id.* at guidance note to subclause (c).

because it would be "too cumbersome."[174] Nevertheless, if a third-party service provider reports that the vessel operator has engaged in AIS manipulation, the charterer has a contractual right to request compliance assurance. In asserting a breach, the charterer does not have to establish a pattern of AIS manipulation or deactivation since even a singular violation could expose the charterer to sanctions liability.[175]

Since the charterer's warranty also includes an obligation to ensure it does not give vessel orders to engage in ship-to-ship operations involving other vessels that have failed to properly maintain AIS transmission in the six months prior to the transaction, this places a substantial burden on the charterer to investigate the AIS backgrounds of STS counterparty vessels prior to any transaction. In a nod to contemporary tracking products available for this purpose, the BIMCO Guidance Notes also emphasize that "[v]arious AIS tracking providers and sanctions screening services offer reports on the AIS activity of vessels."[176]

Outside of the vessel chartering context, other maritime industry actors have also addressed the contractual implications of AIS switch-off. The International Group of P&I Clubs, representing thirteen of the most well-regarded P&I insurers around the world, has issued a circular to its members describing efforts to introduce a common vessel tracking approach utilizing "commercial providers to track the movements of their entered vessels" to ensure compliance with regulatory guidance.[177] The circular also acknowledges the limitations associated with AIS-based tracking, highlighting that "routine monitoring of a vessel's AIS transmissions is not a complete answer when it comes to identifying potential evasion activity."[178] Some of these P&I clubs have also issued separate circulars addressing the contractual consequences of AIS switch-off by explaining to their members that deactivating AIS without a legitimate reason could lead to a breach of P&I club rules.[179]

---

[174] *Id.*

[175] *Id.* at guidance note to subclause (d).

[176] *Id.* at background note.

[177] *See* International Group of P&I Clubs, *Vessel Monitoring and P&I Insurance—Ship's Automated Information System (AIS)* (May 20, 2020), https://www.igpandi.org/article/the-international-group-clubs-discuss-the-importance-of-ships-complying-with-the-requirement-to-use-a-ships-automated-information-system-ais; International Group of P&I Clubs, *Sanctions—Recent Deceptive Practices* (Feb. 2, 2022), https://static.igpandi.org/igpi_website/media/adminfiles/Sanctions_Recent_Deceptive_Practices.pdf.

[178] *Id.*

[179] This could be based on an explicit sanctions clause contained in the P&I club rules or on broad provisions prohibiting imprudent and unlawful trading. *See, e.g.*, *North of England P&I Club, Sanctions: A Guide for Owners and Charterers*, at 17 (May 2021); Irene Anastassiou, *Going Dark is a Red Flag—AIS Tracking and Sanctions Compliance*, GARD, May 29, 2019.

E. Looking Ahead

Vessel tracking data is currently being used as a regulatory weapon and a compliance shield in the sanctions space. These efforts, however, are heavily dependent on AIS data, which belies its well-known technical vulnerability and dependance on the human element in the form of voluntarily transmitted information amenable to manual switch-off. As AIS fills this improvised role as the fulcrum of various maritime sanctions-related initiatives, this is leading to a search for other options that would be better suited in the push for vessel location transparency.

One possibility is the further utilization of LRIT data or other information that could be relayed from GMDSS-compliant equipment already carried on vessels.[180] While more secure than AIS, LRIT data is not regularly cited in law enforcement documents as a basis for demonstrating sanctions-busting trades, suggesting it may be underutilized by the regulators authorized to access this information. Remarkably, however, as U.S. officials have instead encouraged private sector actors to examine LRIT data for sanctions due diligence, this has opened the door to the potential of new possibilities for analytics that could enhance privately administered vessel tracking. As these options are evaluated, LRIT's current dependance on human operation could still limit its effectiveness. As with AIS, vessel operators maintain both the technical capability and legal authority to deactivate LRIT transmissions at their discretion to avoid maritime security risk. Consequently, even though LRIT is technically less vulnerable than AIS, the possibility of LRIT switch-off dampens the prospect that it is equipped for sanctions monitoring in its current iteration.

The LRIT technical and legal architecture, however, does not have to remain static. The international community, under IMO auspices, already managed to modify GMDSS equipment to facilitate the original LRIT system, which suggests additional upgrades might be possible. For instance, if LRIT equipment is converted to perpetually relay vessel location data, and perhaps even preclude the possibility of manual switch-off, this could potentially enhance vessel tracking without the need for major infrastructure reform. If such options are pursued, the SOLAS framework would also need to be reimagined in the interest of transparency, which might limit vessel operators' flexibility in deactivating LRIT transmissions. Changes of this kind would require buy-in from corners of the maritime community that have previously voiced concerns about the confidentiality interests and security vulnerabilities related to continuous LRIT data transmissions.[181]

---

[180] Others have also advocated for more focus on LRIT data for sanctions monitoring. *See* Anastassios Adamopoulous, *States Must Do More on Sanctions Compliance,* LLOYD'S LIST, Sept. 9, 2019.

[181] One solution could be for regulators to re-affirm that LRIT data is for governments only, which would preclude the possibility of LRIT or LRIT-parallel distribution through commercially available platforms. If the concern about perpetual LRIT transmission is that this could cause a vessel to be exposed to threats such as piracy, maintaining a bar on public

Other recently proposed vessel tracking solutions include methods utilizing satellite images and artificial intelligence analysis with less dependance on data relayed by equipment carried on vessels.[182] One team of product developers described their process as follows: after detecting ships from the skies using optical satellite imagery, or more advanced cloud-piercing synthetic aperture radar imagery, with the aid of machine learning, metadata from these images is then analyzed using complex geospatial analysis to pinpoint vessel locations.[183] Ships detected through this process are then cross-referenced with AIS data to create a database pairing their physical characteristics with this identifying information.[184] While the accurate identifying data must be relayed at some point, either before or after the images are analyzed, the image-based vessel tracking process does not depend on a continuous AIS feed.[185] The product developers have described this process as "facial recognition" or "fingerprinting" for ships that could one day function for various enforcement or compliance purposes, including sanctions monitoring.[186] At present, however, such products have not yet come to market due in part to limited access to real-time high-resolution satellite imagery.[187] Although the technological capabilities exist to perform this imagery-based vessel tracking analysis, the data access necessary for product functionality is not yet available, or at least is not feasible from a cost perspective.[188]

An additional variable to consider for the future of vessel tracking discourse is the ongoing development of vessel automation and its dependance on improved navigational technology. Currently, vessels with varying degrees of autonomy, including remotely controlled and even fully autonomous unmanned vessels are being tested. These vessels are expected to utilize cutting-edge navigation, vessel monitoring, and collision avoidance systems.[189] If autonomous vessels are to one day become a viable part of

---

access to LRIT data could help allay this fear. That said, if LRIT data remains for government eyes only, this might limit its usefulness for the type of private sector self-policing and sanctions due diligence currently recommended by sanctioning authorities.

[182] *See, e.g.*, Michael S. Treacy & Mitchell B. Mikinski, Presentation: Ship Identification and AI, Disruptive Technologies in International Law Conference, held by the Stockton Cennter for International Law at U.S. Naval War College (Dec. 10, 2020).

[183] *Id*.

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] *Id.* Other similar possibilities based on technological advancements in synthetic aperture radar have been raised in academic literature. *See, e.g.*, Zhi Zhao et al., *Ship Surveillance by Integration of Space-borne SAR and AIS—Review of Current Research*, 67 J. OF NAVIGATION 177-189 (2014); Sudhir Kumar Chaturvedi et al., *Ship Recognition by Integration of SAR and AIS*, 65 J. OF NAVIGATION 323, 323-37 (2012).

[189] Some observers have argued that autonomous shipping could significantly enhance maritime safety. *See, e.g.*, Jiri de Vos et al., *The Impact of Autonomous Ships on Safety at*

international maritime operations, this is likely to require that at some stage vessel tracking improve well beyond the current processes that rely on unstable voluntarily transmitted data transmission that can be switched off at the whim of the shipmaster.[190] As the regulatory framework surrounding maritime automation evolves parallel to emerging technologies, this could offer an opportunity to create a new vessel location transparency standard, and perhaps even eventually retire today's concept of AIS or LRIT switch-off monitoring.[191]

With maritime sanctions in vogue as a geopolitical tool, regulators interested in sanctions enforcement, along with the commercial actors tasked with compliance, will need to adapt with these new technologies. Although currently available tools include helpful AIS-dependent surveillance platforms, this could be a temporary phenomenon as more reliable options come onto the scene. As they do, this could translate into updated regulatory guidance potentially citing new vessel tracking tools as necessary for sanctions due diligence purposes, which may then be mirrored by commercial agreements reflecting contractual risk allocation beyond the AIS switch-off clauses that have recently circulated.

IV. CONCLUSION

Although driven by policy underpinnings to promote safe and secure navigation, the tools built under the international legal framework governing vessel tracking have been funneled into a new purpose of effectuating sanctions enforcement and compliance. At present, AIS, even with its well-known vulnerabilities, is the primary mechanism being used by regulators and compliance-attuned commercial actors. As sanctioning authorities push for more private sector coordination on vessel-vetting and counterparty due diligence in the sanctions space, technology-driven compliance products are attracting widespread attention as they attempt to promote transparency in a shipping industry that has long been criticized as opaque. But even as vessel tracking improves with data layering, machine learning, and artificial intelligence, the continued dependance on AIS challenges the notion that the

Sea—A Statistical Analysis, 210 RELIABILITY ENG'G & SYS. SAFETY 107558 (2021); for an overview of new technological developments impacting the shipping industry more generally, *see* Baris Soyer & Andrew Tettenborn, NEW TECHNOLOGIES, ARTIFICIAL INTELLIGENCE AND SHIPPING LAW IN THE 21ST CENTURY (2020).

[190] This may include vessel data capture, recording, and storage to aid incident and accident investigations. For a discussion on these possibilities, *see* Maritime UK, MARITIME AUTONOMOUS SHIP SYSTEMS, *MASS UK Industry Conduct Principles and Code of Practice*, Volume 5, at 88 (Nov. 2021), https://www.maritimeuk.org/priorities/innovation/maritime-uk-autonomous-systems-regulatory-working-group/mass-uk-industry-conduct-principles-and-code-practice-2021-v5/.

[191] The IMO has already recognized the implications that autonomous shipping may have on SOLAS and other maritime conventions. *See, e.g.*, Maritime Safety Comm., *Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)*, MSC.1/Circ.1638 (June 3, 2021).

transparency revolution has already arrived. Instead, it is the next wave of technologies including those driven by satellite imagery recognition and vessel automation that are more likely to illuminate the dark side of the shipping industry. These emerging tools may support efforts to monitor sanctionable activity in the current geopolitical climate—with the new Russia-related restrictions representing an extraordinary inflection point—and perhaps also offer opportunities to track compliance with other regulatory obligations looming on the horizon.[192]

[192] These forthcoming regulatory developments include shipping decarbonization efforts. For a discussion on this trend and its connection to transparency initiatives, *see* LLOYD'S LIST, TRANSPARENCY IN SHIPPING: A SPECIAL (2021), https://lloydslist.maritimeintelligence.informa.com/Special-report-Transparency-in-shipping. Maritime analytics companies have already begun marketing their products as a means to track compliance with environmental commitments. *See, e.g.*, THE WINDWARD BLOG, *Introducing Windward's Data for Decarbonization Program* (Sept. 14, 2021), https://windward.ai/blog/introducing-windwards-data-for-decarbonization-program/.