AN A.S. PRATT PUBLICATION
JUNE 2022
VOL. 8 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: UTAH MAKES FOUR
Victoria Prussen Spears

AND NOW THERE ARE FOUR: UTAH ENACTS CONSUMER PRIVACY LAW
Marian A. Waldmann Agarwal, Mary Race and Robert N. Famigletti

HEIGHTENED CYBER THREATS HIGHLIGHT THE NEED TO BE READY
Daniel K. Alvarez, Laura E. Jehl, Richard M. Borden, Kari Prochaska and Amelia Putnam

COPPA SAFE HARBORS: A NEW COURSE FOR INDUSTRY SELF-REGULATORY GROUPS
Sarah L. Bruno, John P. Feldman and Stuart D. Cobb

SENSOR SHIPS: MANAGING BIG DATA GENERATED IN THE MARITIME WORLD
Sharon R. Klein, Vanessa C. DiDomenico and Karen H. Shin

SEC PROPOSES SUBSTANTIAL NEW CYBERSECURITY REQUIREMENTS FOR INVESTMENT ADVISERS AND COMPANIES
Scott F. Mascianica and Shardul Desai

EUROPEAN COMMISSION PUBLISHES DRAFT DATA ACT
Daniel Cooper and Anna Oberschelp de Meneses

CHINA ISSUES DRAFT MEASURES ON DATA SECURITY IN THE INDUSTRY AND INFORMATION TECHNOLOGY SECTORS
Lester Ross, Kenneth Zhou and Tingting Liu

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 5** **June 2022**

Editor's Note: Utah Makes Four
Victoria Prussen Spears 149

And Now There Are Four: Utah Enacts Consumer Privacy Law
Marian A. Waldmann Agarwal, Mary Race and Robert N. Famigletti 151

Heightened Cyber Threats Highlight the Need to Be Ready
Daniel K. Alvarez, Laura E. Jehl, Richard M. Borden, Kari Prochaska and Amelia Putnam 157

COPPA Safe Harbors: A New Course for Industry Self-Regulatory Groups
Sarah L. Bruno, John P. Feldman and Stuart D. Cobb 162

Sensor Ships: Managing Big Data Generated in the Maritime World
Sharon R. Klein, Vanessa C. DiDomenico and Karen H. Shin 165

SEC Proposes Substantial New Cybersecurity Requirements for Investment Advisers and Companies
Scott F. Mascianica and Shardul Desai 170

European Commission Publishes Draft Data Act
Daniel Cooper and Anna Oberschelp de Meneses 179

China Issues Draft Measures on Data Security in the Industry and Information Technology Sectors
Lester Ross, Kenneth Zhou and Tingting Liu 184

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [149] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Sensor Ships: Managing Big Data Generated in the Maritime World

By Sharon R. Klein, Vanessa C. DiDomenico and Karen H. Shin*

The authors recommend that vessel operators make strategic security investments in implementing incident monitoring and response software and other appropriate security controls, making continued updates, timely installing patches to the technology on board, and training crew on cybersecurity.

Big data is not a "trend" or fad; big data is a concept of gathering, deciphering, and analyzing massive quantities of information to ultimately reveal patterns and associations, and it is here to stay. Companies have proven how useful it can be to interpret performance trends to expose areas of vulnerability or underperformance within a company. Big data can be used to make strategic decisions within a company's operating profile. In particular, the maritime industry is using big data to revolutionize the way engine performance and maintenance is carried out aboard vessels. Understanding how to effectively capture data – and the risks involved – will enable users to apply big data in ways never considered before.

THE VALUE OF BIG DATA

The maritime industry has progressed at a moderately stable speed with various innovations to proven mechanical systems, such as energy reducing pumps and updated models of equipment; however, compared to other industries it is decades behind digitally. To capitalize on the benefits of big-data technology, maritime companies must define the goals they will achieve, such as reducing fuel consumption. By clearly defining a goal, systems can be constructed to deliver the required data points.

Once the goals are defined, sensors and instruments can be installed onboard to capture new data points that, when spliced with existing readings already extracted from the vessel's automation, such as weather patterns and engine load signals, create interconnected data ecosystems that can be used to examine performance.

This combined data set is sent to an onboard personal logic controller ("plc") and downloaded in a readable format to an onboard server, where it can be uploaded at four-to-five second frequencies to a cloud server via the vessels' satellite at sea or LAN connection in port. The data is then downloaded from the cloud to the designated

* Sharon R. Klein, a partner in the Orange County office of Blank Rome LLP, is chair of the firm's Privacy, Security and Data Protection Practice. Vanessa C. DiDomenico, an associate in the firm's office in Washington, D.C., concentrates her practice in the area of maritime law. Karen H. Shin, an associate in the firm's office in Orange County, focuses her practice on a diverse range of data privacy and information security matters. The authors may be contacted at sharon.klein@blankrome.com, vanessa.didomenico@blankrome.com and karen.shin@blankrome.com, respectively.

monitoring center, where programs will scrub the data and further process it by using algorithms.

After collecting and processing the data, it can be shown on a platform or user-friendly dashboard designed to match the company's needs. Viewing multiple layers of information on one screen is one of the many appealing factors encouraging companies to invest in big data. Analysis of the data generated onboard can guide crew operation and assist in identifying abnormal states of energy efficiency or trim optimization and can enable the company to make informed decisions with planned maintenance or hull fouling treatment. Different departments within the same organization can examine and extract information specific to their needs. For example, environmental departments can use the dashboard fed with big data in real time to understand the vessel's location, fuel type, and engine usage all together to ensure compliance within certain emission control areas that may require the use of low sulphur fuel. Marketing departments can compare costs of adding additional ports by understanding vessel performance. Technical departments can filter data to see engine measurements after an overhaul or dry docking and view monthly and yearly reports to better plan fuel and spare-part budgets.

Maritime companies can tailor the platforms toward their specific needs; they can start small by compiling data from past voyages and move into real time continuous-based monitoring and even predictive analytics. Furthermore, engine manufacturers can enter into data sharing agreements to partner with vessel owners to share in research and development. Partnerships with manufacturers can also help to offset some of the upfront costs of developing the system and installing the required sensors.

Other companies are using tools onboard to gather and share metrics with outside organizations. For example, Maersk, as part of its environmental, sustainability, and governance (commonly referred to as "ESG") plan, is sharing ocean-weather-observation data generated onboard its vessels with the National Meteorological Service of Germany. Maersk announced that it will collect and share ocean-weather observations for climate science and various inputs for weather forecasts.[1] The ever-growing pool of data generated onboard vessels may serve to cross-pollinate ideas and generate new solutions to industry and global challenges.

CYBER RISKS AND CONCERNS

Big data has many advantages that may offset various risks, but with enormous amounts of data being sent, there are increased concerns from industry. There are no clear channel markers or buoys set up in the cyber world. Navigating through complex

[1] *See* Maersk Vessels Live Feed Meteorologists around the Globe with Weather Data, available at https://www.maersk.com/news/articles/2022/02/07/maersk-vessels-live-feed-meteorologists-around-the-globe-with-weather-data.

security concerns and privacy issues are hazards associated with the gathering, transmittal, and usage of the data. Maritime transportation companies are concerned with firewall protections to ensure that hackers cannot access their automated systems to gain control or take over a vessel at sea. Vessel owners are also concerned about the storage of this data and the access of other competitors to the sensitive operating measurements. There are also concerns about costs in relation to pilot programs, installation, data transmission through satellites, and continuous monitoring.

Officers onboard also have raised their own concerns as it relates to the daily vessel operations. Captains and chief engineers are already consumed with tasks to ensure safe day-to-day operations, and crew members are concerned that additional work is created by the new sensors, and if the system goes offline, it can jeopardize other work priorities.

These concerns are well-founded – in 2017, an ocean container carrier fell victim to a ransomware attack destroying all end-user devices, including 49,000 laptops and print capability, making 1,200 applications inaccessible and destroying approximately 1,000 more and destroying around 3,500 of its 6,200 servers, costing the company between $250 million and $300 million; again in 2017, the GPS systems of 20 ships sailing in the Black Sea were altered in such a way that the position displayed on the GPS device of the ships did not match the actual position; in 2019, a spoofing incident caused the transponders on multiple ships in the port of Shanghai to show various erroneous positions that formed odd ring-like patterns.

CYBERSECURITY POLICY MEASURES

With the rise in cybersecurity attacks on the supply chain, there has been a heightened focus on incident response procedures and security standards. For instance, the United States, using the purchasing power of the government through President Biden's Executive Order on Improving the Nation's Cybersecurity,[2] has attempted to strengthen its cybersecurity practices by requiring government-information-technology-service providers to notify the government agencies with which they contract of cyber incidents and establishing new cybersecurity standards through amendments to the Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS").[3]

President Biden also issued the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries,[4] which requires the U.S. Department of Commerce to evaluate transactions involving connected software applications that may pose

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[3] Exec. Order No. 14028 86 C.F.R. 26633 (2021).

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

an unacceptable risk to U.S. information and communications technology, critical infrastructure, the digital economy, or national security, and to take appropriate action based on its evaluation.[5]

On January 24, 2022, the Port of Los Angeles debuted[6] its Cyber Resilience Center ("CRC"), a cyber-defense solution created to improve the cybersecurity readiness of the Port by enabling participating stakeholders to automatically share cyber-threat indicators and potential defensive measures with each other.

SAILING AHEAD: MARITIME CYBERSECURITY AWARENESS

Maritime transportation companies should pay close attention to and monitor developments in the privacy and security landscape to ensure that they and their service providers, who provide sensors and automation programs, are compliant with the applicable security standards to not only protect data, but also protect the vessel's enterprise systems that receive inputs from sensors and automation programs. Cybersecurity in the maritime industry is especially problematic with ocean transits exposing the vessel's systems to a higher number of unknown networks and across international lines and with usually outdated legacy hardware on board (as vessels are designed and built to last for decades). Thus, it will be important for vessel operators to make strategic security investments in implementing incident monitoring and response software and other appropriate security controls, making continued updates, timely installing patches to the technology on board, and training crew on cybersecurity (especially during crew turnover at various points on a voyage).

There are also misunderstood motives behind the big-data push in the maritime world. Companies are reluctant to share data that may expose legal liabilities to regulators or provide a competitive advantage to other market participants. However, the EU, for instance, unveiled[7] new proposed rules on February 23, 2022, to make it easier for the sharing and transferring of non-personal data (i.e., data that does not contain any information that can or does identify an individual). The European Commission's Data Act, among other things, includes measures to allow users of connected devices to gain access to data generated by them and to share such data with third parties to provide aftermarket or other data-driven innovative services, and clarifies that databases containing data from Internet-of-Things ("IoT") devices and objects are not subject to separate legal protection, thereby allowing end users to more easily access data generated by IoT devices.

---

[5] Exec. Order No. 14034 86 C.F.R. 31423 (2021).

[6] https://www.portoflosangeles.org/references/2022-news-releases/news_012422_csc_ibm.

[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

Nevertheless, companies should evaluate any cybersecurity vulnerabilities and perform due diligence on the service providers that provide sensors and automation programs for the reasons described above. Maritime transportation companies should also ensure that they (and not their service providers) own the data being collected via sensors and automation programs for intellectual property purposes, so that the service provider cannot freely use the data for its own purposes or to monetize outside of performing its obligations under the agreement with the company.

Additionally, some officers and crew members may view continuous monitoring as a "big brother" watching over from the office critiquing every decision made at sea. However, vessel operators can address the misconceptions behind data measuring by explaining the benefits of improving performance and providing more in-depth trends to those serving afloat, including reducing paperwork and presenting helpful data onboard to assist in decision making and maintenance.

CONCLUSION

Big data may prove incredibly useful to maritime companies if specific goals are created, data is captured correctly, appropriate cybersecurity and data protection safeguards are implemented, and utilization is optimized. Data privacy concerns should be addressed from the industry as a whole to seek assistance from policy makers and regulatory bodies. Employing big data within the maritime industry can create new jobs and opportunities for technology companies to market to the world fleet, generating tremendous opportunities for companies to revolutionize and propel the industry forward.

Data storage costs and concerns with transmission should not stop the industry from advancing and should not deter innovation. Big data will not only allow companies more insight into their current assets, it may also open doors to new companies, greater research, visibility within the supply chain, and collaboration. The data generated onboard vessels may also assist informed decision making onboard and ashore while also providing necessary aid to support decarbonization and autonomous shipping.