KSTARR Enterprises, LLC

Digital Maritime Doctrine™: A Framework for Global Platform Accountability[i]

By Legal Theorist Katherine Starr

Inspired by the legacy of maritime law and refined through the lens of 21st-century digital harm, this doctrine establishes jurisdictional and legal responsibility for global platforms based on their structural design, server geography, and foreseeable user harm.

Introduction: The Internet as Open Sea

In the analog world, maritime law arose to govern conduct beyond the territorial waters of any one nation. In today's digital world, we face a parallel challenge: platforms operating across borders, affecting users globally, while evading accountability by docking their operations in low-duty jurisdictions. The sea, once the place of jurisdictional ambiguity and practical necessity, mirrors the internet's jurisdictional vagueness today. Maritime law's doctrines were developed to solve the accountability vacuum in unclaimed waters. So too must we now resolve the liability vacuum in cyberspace.

This Digital Maritime Doctrine is built on the foundational logic of international maritime law, product liability, and tort-based foreseeability. It asserts that global digital platforms must be held accountable not solely based on their incorporation or server location, but by the jurisdictions they intentionally serve, harm, or profit from.

Core Legal Analogies

Just as a ship is a constructed vessel navigating international waters, a platform is a designed infrastructure navigating global internet traffic. The "flag" it flies typically, the place of incorporation or server location is not enough to determine legal jurisdiction or responsibility. Hosting in jurisdictions such as the Isle of Man, Jersey, Liechtenstein, or Ireland often reflects not a technical need but a deliberate legal evasion. These are the digital equivalents of maritime flags of convenience[iiiii], where registration is chosen not for legitimacy but for immunity.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

When a platform serves users in high-regulation jurisdictions such as the United States or the European Union, it has effectively entered the ports of those countries and is thereby subject to their laws. The server may be hosted offshore, but the harm occurs domestically. The user experience, the data harvesting, the economic transactions are all docked onshore.

Foreseeable harm must override geographic placement. When a platform enables fraud, abuse, or algorithmic risk that predictably causes harm in a different jurisdiction, it has breached its duty of digital seaworthiness. In maritime law, a vessel owner cannot disclaim liability for a defective hull simply because the incident occurred in international waters[iv][v]. Likewise, a platform cannot claim immunity because its servers are in a low-liability zone. If it was foreseeable that harm would occur where it did, then liability attaches. (See Exhibit A)

The product liability doctrine strengthens this frame. If a boat sinks mid-ocean due to defective design, the manufacturer is liable wherever the loss occurs. The open sea is no refuge. In the digital realm, harm caused by product design, such as flawed recommendation algorithms, vulnerable data flows, or the facilitation of exploitation, must be treated in kind. Digital platforms are not exempt from legal logic simply because their operations lack physical form.

Integration with the Starr frameworks

To support this doctrine, we integrate the principles of Negligent Digital Access™[vi], Negligent Digital Architecture™[vii], and Negligent Dating™[viii], legal frameworks developed to assign responsibility not for content alone, but for the infrastructure that makes harm systemic and foreseeable.

Negligent Digital Access governs the jurisdictional question of who platforms choose to serve. It asserts that when access is intentional through language, currency, interface design, or regional marketing, the platform has effectively docked in that legal territory. It cannot profit from a population while disclaiming legal responsibility for foreseeable harm to that same population.

Negligent Digital Architecture addresses the design-level foreseeability baked into the structure of the platform itself. Just as a ship must be built to withstand ocean conditions, a platform must be built to prevent known forms of digital harm. Algorithms that accelerate outrage, verification processes that are toothless, or backend systems that ignore behavioral red flags are not passive oversights; they are design decisions that carry duty.

Negligent Dating brings these obligations into sharp relief by applying them to spaces of emotionally intimate contact platforms where grooming, fraud, and psychological exploitation are not anomalies but predictable features of design. These platforms often facilitate cross-border intimacy while ignoring known patterns of transnational abuse. The design is frictionless, moderation is shallow, and oversight is optional, conditions that are not only permissive of harm but profitable from it. As Katherine Starr has written, “This isn’t just emotional harm, it’s negligent dating at scale.”

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

Consider a dating app that markets trust and connection but does nothing to verify identity, block VPN access, or detect behavioral markers of coercion. It opens access to scam-heavy regions without monitoring for repeated manipulation. It requires no biometric verification and enforces no effective bans. The harm is not accidental; it is built into the structure. Under this doctrine, the platform has failed to meet the basic standard of digital seaworthiness. It has navigated directly into known storm zones without a hull, without crew, and without lifeboats—profiting from the very risk it refuses to mitigate.

Together, these three frameworks establish the core logic of the Digital Maritime Doctrine: that harm online is rarely the product of user behavior alone. It is the predictable result of architectural choices, jurisdictional reach, and access design choices that generate liability not just where harm is visible, but where it is foreseeable.

Application of Negligent Dating across Digital Borders

A real-world example of this doctrine, applying Negligent Dating, deserves closer examination within the broader framework of the Digital Maritime Doctrine. It targets a specific class of engineered vulnerability: platforms that facilitate emotionally intimate contact across borders, while failing to account for regional grooming threats. In this context, harm is not incidental; it is structurally incentivized.

The rise of romance fraud networks operating out of known hubs like Nigeria[ix] reflects a pattern of transnational grooming that platforms often enable through frictionless access, pseudonymous interaction, and engagement-driven algorithms. Under Negligent Digital Access, platforms that knowingly open these portals into high-risk regions effectively "dock" there, acquiring a duty to monitor for exploitation. Under Negligent Digital Architecture, failure to embed friction, verification, or reporting structures constitutes design-level negligence.

As Katherine Starr has written, "This isn't just emotional harm, it's negligent dating at scale." These harms demand more than content moderation; they demand jurisdictional accountability. The Digital Maritime Doctrine reframes these platforms as vessels that navigate vulnerable ports, whose failure to implement safeguards amounts to institutional failure. When a platform profits from known grooming patterns, the question is no longer whether harm occurred, but whether it was preventable, foreseeable, and allowed to persist under the guise of user freedom. In maritime terms, this is not a rogue wave; it's a poorly designed hull entering storm-prone waters without a lifeboat.

A Scenario Across Borders: Multi-Jurisdiction Accountability

To illustrate how the Digital Maritime Doctrine applies beyond the narrow lens of dating platforms, we turn to a hypothetical scenario that threads all three Starr frameworks, Negligent Digital Access™, Negligent Digital Architecture™, and Negligent Dating™, into a unified model of liability. This example underscores how structural negligence transcends content or geography, emerging instead from the interconnected failures of platform design, access intent, and regulatory

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

evasion across jurisdictions. It is not a story about one platform, but a systemic pattern that the law must learn to trace and address.

Hypothetically speaking, a rural schoolteacher in Ireland searches her own name on a popular, publicly accessible AI chatbot. The system, trained on a vast but unvetted trove of online text and hosted on servers in Liechtenstein, produces a confident, detailed assertion that she was once investigated for child-safeguarding violations. None of it is true. A curious parent takes a screenshot of the response and shares it on a local Facebook group. Within hours, the post is amplified by a large U.S.-based influencer eager for controversy, ricochets across multiple platforms, and spawns hundreds of hostile messages directed at the teacher's school. Administrators, faced with mounting pressure and fearful headlines, place her on leave while an internal review confirms no record of any misconduct. Meanwhile, the AI provider disclaims liability, pointing to user prompt wording and the offshore location of its servers.

This scenario distills the type of diffuse, design-enabled harm that the Digital Maritime Doctrine is built to navigate. Under Negligent Digital Access, the chatbot's operators chose to serve users in Ireland, effectively docking in that jurisdiction. Under Negligent Digital Architecture™, the system lacked safeguards against reputational hallucinations and an unseaworthy vessel set adrift in global discourse. The harm that followed was not an outlier but a foreseeable consequence of the platform's structure and reach. As these incidents become more common, they expose the limits of jurisdictional clarity in the digital realm and underscore the need for a cohesive framework that accounts for how access, architecture, and geography combine to produce real-world harm.

Legal and Policy Recommendations

Digital platforms must be governed by a framework that sees server geography as merely one layer of liability, not a shield. If a platform knowingly enables access to users in a jurisdiction, it must comply with that jurisdiction's safety standards. Foreseeable harm must override passive corporate form. Legal systems must treat cross-border reach as a form of digital docking. Evasion through server relocation or shell incorporation should be understood as constructive negligence or willful avoidance of the law.

As ships are required to disclose cargo and safety standards before entering port, platforms should disclose where their servers are housed, who moderates their content, and what safety mechanisms are engineered into their products. A platform sailing into global waters must be built to withstand the legal seas it enters.

Several recent decisions illustrate how traditional courts are already touching the contours of this doctrine. In Google v. Equustek Solutions Inc[x]. (Supreme Court of Canada, 2017), the Court ordered Google to deindex infringing pages worldwide, despite the company's servers and legal headquarters being outside Canada. The ruling anticipates the logic of Negligent Digital Access: once a platform docks in a jurisdiction by serving users and profiting from their data, it cannot sail away from liability simply by pointing to an offshore flag. The global delisting order also mirrors

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

the Digital Maritime Doctrine's view that a court's remedial reach should match the platform's operational reach when local harm is foreseeable and ongoing.

The tension between foreseeability and purposeful availment sits at the heart of McIntyre Machinery v. Nicastro[xi] (U.S. Supreme Court, 2011). Although the plurality hesitated to assert jurisdiction over a U.K. manufacturer whose metal-shearing machine injured a New Jersey worker, the concurrences and dissents emphasized that modern commerce makes physical presence an outdated proxy for intent. The Digital Maritime Doctrine resolves this tension by adopting the foreseeability strand: where a platform's design (the hull, under Negligent Digital Architecture) and distribution model target a global audience, harm in any port becomes legally cognizable. Nicastro therefore serves as the cautionary case that shows why a harmonized doctrine is needed.

In Lloyd v. Google[xii] (U.K. Supreme Court, 2021), a representative action alleging mass data harvesting failed on procedural grounds, yet the Court accepted in principle that a platform might owe a unified duty of care for design-level privacy violations. This resonates with Negligent Digital Architecture, which treats large-scale, design-borne data extraction as an architectural breach rather than a series of isolated user injuries. While Lloyd was dismissed, the Court's analysis signals judicial willingness to frame systemic digital harm as a single, aggregate wrong, precisely the approach the Digital Maritime Doctrine recommends.

Beyond the courtroom, the International Maritime Organization's MSCFAL.1/Circ.3 (2017) circular extended the centuries-old duty of seaworthiness to include cyber-risk management for vessels. This regulatory move affirms the Doctrine's premise that infrastructure integrity is a safety obligation. By analogy, platforms must maintain "*cyberseaworthiness*": robust code, transparent safeguards, and proactive mitigation of known threats. In doctrinal terms, the IMO circular strengthens the claim that design-level foresight is now a recognized element of duty in borderless environments[xiii].

Collectively, these authorities demonstrate that courts and regulators are inching toward a harm-centered, design-focused, and jurisdiction-agnostic mode of analysis. The Digital Maritime Doctrine™ and its supporting frameworks provide the conceptual map to complete that journey.

Legacy and Vision

Just as early maritime scholars mapped ports, shipping routes, and vessel registries to establish accountability across oceans, today's legal systems must chart a similar path in the digital world. It is no longer sufficient to rely on incorporation papers, domain registrations, or server locations. Instead, we must trace harm, design intent, and structural access mapping a vessel's digital wake across jurisdictional waters.

The Digital Maritime Doctrine reframes our legal compass: from geography to intent, from physicality to foreseeability, from national borders to infrastructural design. It demands that global platforms be treated as vessels in international waters, accountable not only where they anchor but

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

wherever they travel and cause harm. Every court that has grappled with cross-border tech harm from Canada's Equustek to the U.S. Nicastro ruling, from the U.K.'s Lloyd v. Google to the International Maritime Organization's cyber-readiness circular has touched the edges of this truth. Now, the doctrine unifies them.

Starr's frameworks, Negligent Digital Access, Negligent Digital Architecture, and Negligent Dating, give substance to this vision. They articulate the duty of platforms not simply to host, but to foresee; not merely to connect, but to protect. These principles convert abstract harm into legal obligations, bridging doctrine with digital reality.

Platforms are not neutral actors. Their infrastructure, moderation choices, algorithmic designs, and regional expansions are deliberate. When these choices foreseeably create harm, the law must step in. The doctrine's strength lies in its ability to bring together scattered legal concepts, jurisdiction, tort duty, regulatory design, and platform governance into a unified theory that responds to the true nature of digital life.

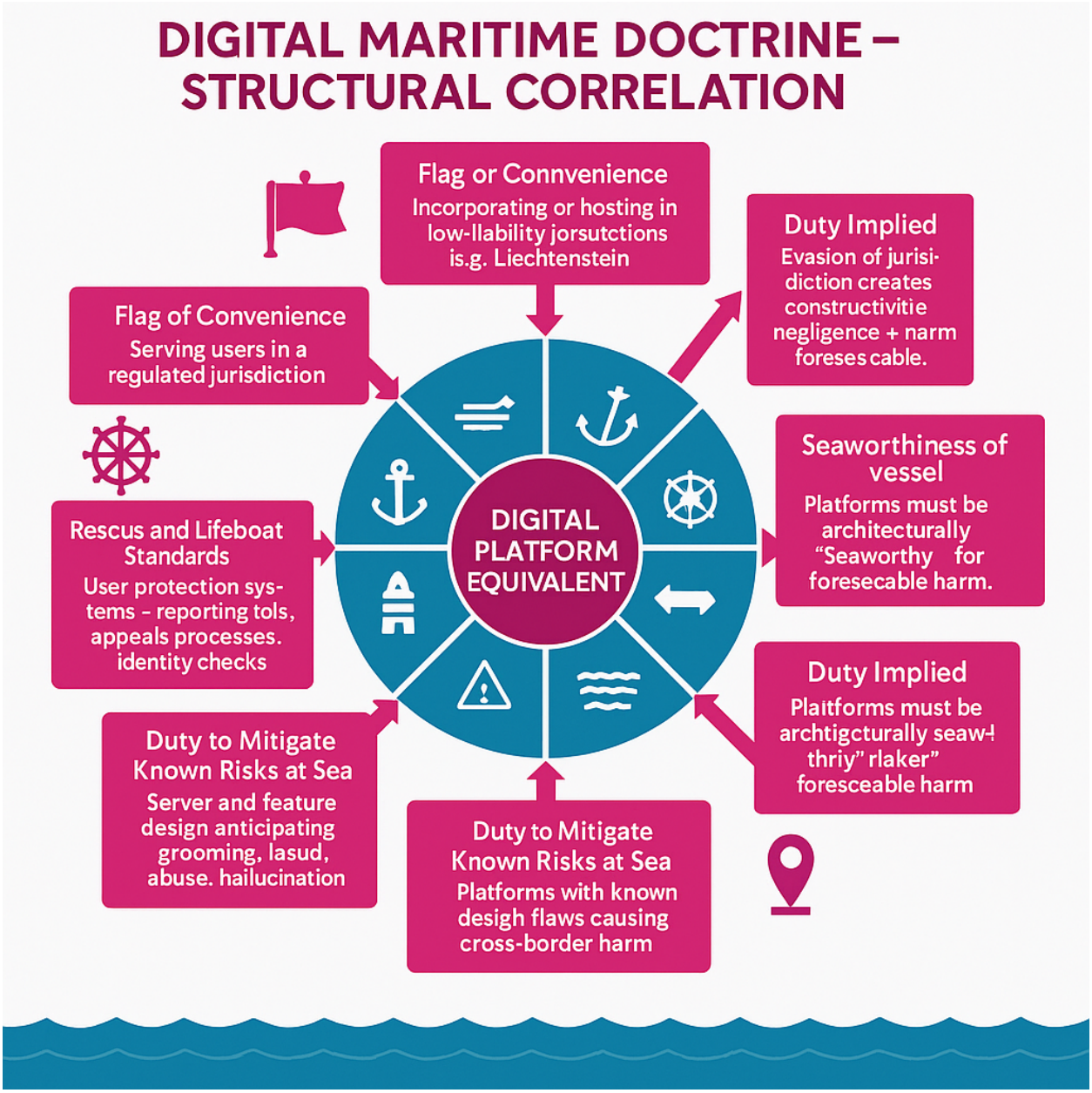
This is more than a metaphor. The cloud is not an exception. It is the evolved ocean. And just as seafarers once faced new governance to match the scale of trade and risk, so too must the internet be governed by doctrines that match its reach and consequence.

The Digital Maritime Doctrine is a call to courts and policymakers to stop asking where a server sits and start asking whom it touches, what it enables, and whether it was seaworthy when launched. It is a doctrine built not only to resolve today's jurisdictional dilemmas, but to steer legal systems through the deep waters ahead.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

Exhibit A

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED



© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

Citations and Attributes

APA (7th Edition):
Starr, K. (2025). Digital maritime doctrine™: A framework for global platform accountability. KStarr Enterprises, LLC. https://www.katherinestarr.com/digital-maritime-doctrine/

MLA (9th Edition):
Starr, Katherine. Digital Maritime Doctrine™: A Framework for Global Platform Accountability. KStarr Enterprises, LLC, 2025. www.katherinestarr.com/digital-maritime-doctrine/.

Bluebook (Legal):
Katherine Starr, Digital Maritime Doctrine™: A Framework for Global Platform Accountability, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/digital-maritime-doctrine/.

---

[i] Digital Maritime Doctrine™ is an original legal theory developed by Katherine Starr. See: Starr, K. (2025). Digital Maritime Doctrine™: A Framework for Global Platform Accountability. KStarr Enterprises, LLC.
[ii] William Tetley, Maritime Liens and Claims, 2nd ed. (Montreal: Les Éditions Yvon Blais, 1998), at ch. 2.
[iii] United Nations Conference on Trade and Development (UNCTAD), Review of Maritime Transport 2022, UN Doc. UNCTAD/RMT/2022, ch. 2 (2022).
[iv] International Convention for the Unification of Certain Rules of Law relating to Bills of Lading (Hague Rules), Art. III(1), 1924.
[v] Thomas J. Schoenbaum, Admiralty and Maritime Law, 6th ed. (St. Paul, MN: West Academic, 2018), § 5-15.
[vi] Starr, K. (2025). Negligent Digital Access™: When Platform Design Enables Harm. KStarr Enterprises, LLC. https://www.katherinestarr.com/negligent-digital-access/
[vii] Starr, K. (2025). Negligent Digital Architecture™: How Platform Design Codifies Harm. KStarr Enterprises, LLC. https://www.katherinestarr.com/negligent-digital-architecture/

[viii] Starr, K. (2025). Negligent Dating™: Exposing How a Billion-Dollar Industry Fails to Protect. KStarr Enterprises, LLC. https://www.katherinestarr.com/negligent-dating/
[ix] The Guardian (Jan. 9, 2024), https://www.theguardian.com/uk-news/2024/jan/09/if-you-think-only-lonely-middle-aged-women-fall-for-romance-scams-heres-why
[x] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (CanLII), [2017] 1 S.C.R. 824.
[xi] J. McIntyre Machinery, Ltd. v. Nicastro, 564 U.S. 873 (2011).

[xii] Lloyd v. Google LLC, [2021] UKSC 50, [2021] 3 WLR 1268.ord
[xiii] International Maritime Organization (IMO). (2017). Guidelines on Maritime Cyber Risk Management. MSC-FAL.1/Circ.3. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED