Data Governance For On-Demand Fishing

On-Demand Data Governance Working Group

Photo: @edgetech_marine via Instagram

Erica Fuller (Conservation Law Foundation), chair
Amy Knowlton (New England Aquarium)
Elizabeth Vézina (Canadian Wildlife Federation)
Hannah Drake (Canadian Wildlife Federation)
Heather Pettis (New England Aquarium)
Mark Baumgartner (Woods Hole Oceanographic Institution)
Michael Moore (Woods Hole Oceanographic Institution)
Regina Asmutis-Silvia (Whale and Dolphin Conservation)

How to cite this report:

Fuller, E., A. Knowlton, E. Vézina, H. Drake, H. Pettis, M. Baumgartner, M. Moore, R. Asmutis-Silvia. 2025. Data governance for on-demand fishing. A report to the Ropeless Consortium. Available at ropeless.org.

The working group acknowledges and is grateful for the input of the following subject matter experts:

Christin Khan (NOAA Fisheries)
Brett Alger (NOAA Fisheries)
Kate Wing (Intertidal Agency)
Doug Poirier (Ai2)

SUMMARY OF RECOMMENDATIONS

To minimize gear conflict and enable enforcement of on-demand fishing, we recommend the following:

- On-demand fishing data should be housed outside of government by an independent cloud service provider
- A single centralized cloud database should be used to accept, store and disseminate gear location data for all of North America
- On-demand data collected at sea should be transmitted directly from the vessel to the centralized cloud database, and it should be available for access by enforcement and other nearby fishers in real time
- Data sharing should be mandatory and a condition of the permit to fish on-demand gear
- Rules for data access by fishers and enforcement should be determined by appropriate regulatory authorities for their jurisdictions
- Each regulatory authority should have an administrator who is responsible for verifying and registering fishers in the system
- Regulatory authorities should be responsible for bearing the costs of the cloud service

INTRODUCTION

Significant progress has been achieved to date on many technical aspects of on-demand fishing, such as gear retrieval by stowed rope or lift bag, global positioning system (GPS) marking of gear deployment locations, and sharing of those gear deployment locations via manufacturer or data integrator (e.g., EarthRanger) cloud databases. Prototype systems have been trialed extensively by U.S. and Canadian fishers over the past several years, which has yielded vital performance information and generated questions and ideas about how actual commercial fishing may be conducted with these systems. It has become clear to all stakeholders that to address gear conflict with on-demand gear, the location of buoyless fixed fishing gear must be shared with other nearby fixed and mobile fishers; likewise, enforcement agencies need access to this same data to be able to find and inspect the gear. While conceptually simple, the mechanisms, security, legality and governance of this data sharing is complex and challenging. Who owns these data? Where should the data reside? How should the data get from a fishing vessel to the cloud? How should the data get from the cloud to authorized users? Who decides who gets permission to access those data? What should the rules of access be and who decides on those? And what data, exactly, are required? This document is intended to explore the possible answers to these questions, and to make recommendations about data governance for on-demand fishing. It is organized such that the recommendations are presented first, and the supplemental sections that follow are presented as rationale for the recommendations.

This working group is comprised of people who have been working to advance on-demand fishing since 2017. None of the members have a commercial interest in on-demand fishing; all work for non-profit organizations (some advocacy organizations, others research/ technology organizations). Two invited subject matter experts work for the U.S. federal government. Members have worked in Canada and/or the U.S. to organize and conduct gear trials, assemble and operate gear libraries, make on-demand data accessible in the cloud, convene on-demand stakeholders, assess and report on the needs of fishers, enforcement and regulators, and address issues of interoperability.

EVOLUTION

October 21, 2024

Discussion of need among working group members at the Ropeless Consortium in Providence, RI

November 1, 2024

Meeting of subset of working group members and NOAA Fisheries representatives (Erica Fuller, Michael Moore, Brett Alger, Christin Khan) to discuss data governance questions

November 14, 2024

Meeting of working group members to discuss challenges and scope

November 20, 2024

Meeting of working group members and NOAA Fisheries (Caroline Potter, Jennifer Goebel, Colleen Cogan, Sam Duggan, Eric Matzen, Brett Alger, Allison Murphy, Jay Hermsen, Henry Milliken) to discuss challenges NOAA is facing with on-demand data governance issues

November 21, 2024

Meeting of working group with Kate Wing and Rachel Blake of Intertidal Agency to discuss tackling data governance issues in the fisheries space; working group decided to work independent of agency authority because of Federal Advisory Committee Act (FACA) concerns and to ensure that our recommendations can be considered as weighted evidence

December 3, 2024

Draft of version 1 begun

December 6, 2024

Draft of version 1 disseminated to working group members for comment

January 10, 2025

Meeting of working group with Invited Experts Brett Alger and Christin Khan as well as Doug Poirier and Kate Wing to discuss Draft version 1

February 25, 2025

Need for data governance discussed at Fisheries and Oceans Canada's Second Gear Innovation Summit

May 2, 2025

Draft of version 2 circulated

May 12, 2025

Version 2 of draft discussed, draft edited and version 3 circulated

May 13, 2025

Draft document finalized

WORKING GROUP RECOMMENDATIONS

We recommend the development and use of a single centralized cloud database that resides outside of government to receive, store and disseminate on-demand fishing data for the purposes of minimizing gear conflict and enabling enforcement. Fishing vessels should transmit on-demand data directly to this centralized cloud database to maximize security and minimize latency. These data should be available in real time to enforcement agencies as well as other fixed or mobile fishers that are near the on-demand gear at sea. The specific data access rules governing who has access and when they have access should be decided in consultation with fisheries by regulatory authorities and required as a permit condition. For example, U.S. fishers would be required to provide written authorization/consent/waivers allowing their data to be shared with other fishers and enforcement under the several statutes or agreements that might otherwise restrict such sharing, including the Magnuson-Stevens Fishery Conservation and Management Act (MSA), Atlantic Coastal Cooperative Fisheries Management Act, The Privacy Act, Uniform Trade Secrets Act, and Federal Records Act. Processes should be in place to delete business information such as gear locations as quickly as practicable. Database administrators for each jurisdiction would be responsible for communicating to the cloud service provider the data access rules for their region, as well as verifying and registering users (primarily fishers and enforcement personnel) in the cloud database (Figure 1). Funding for the cloud service could be split between regulatory authorities based on the number of fishers and/or units of on-demand gear being used in each jurisdiction.

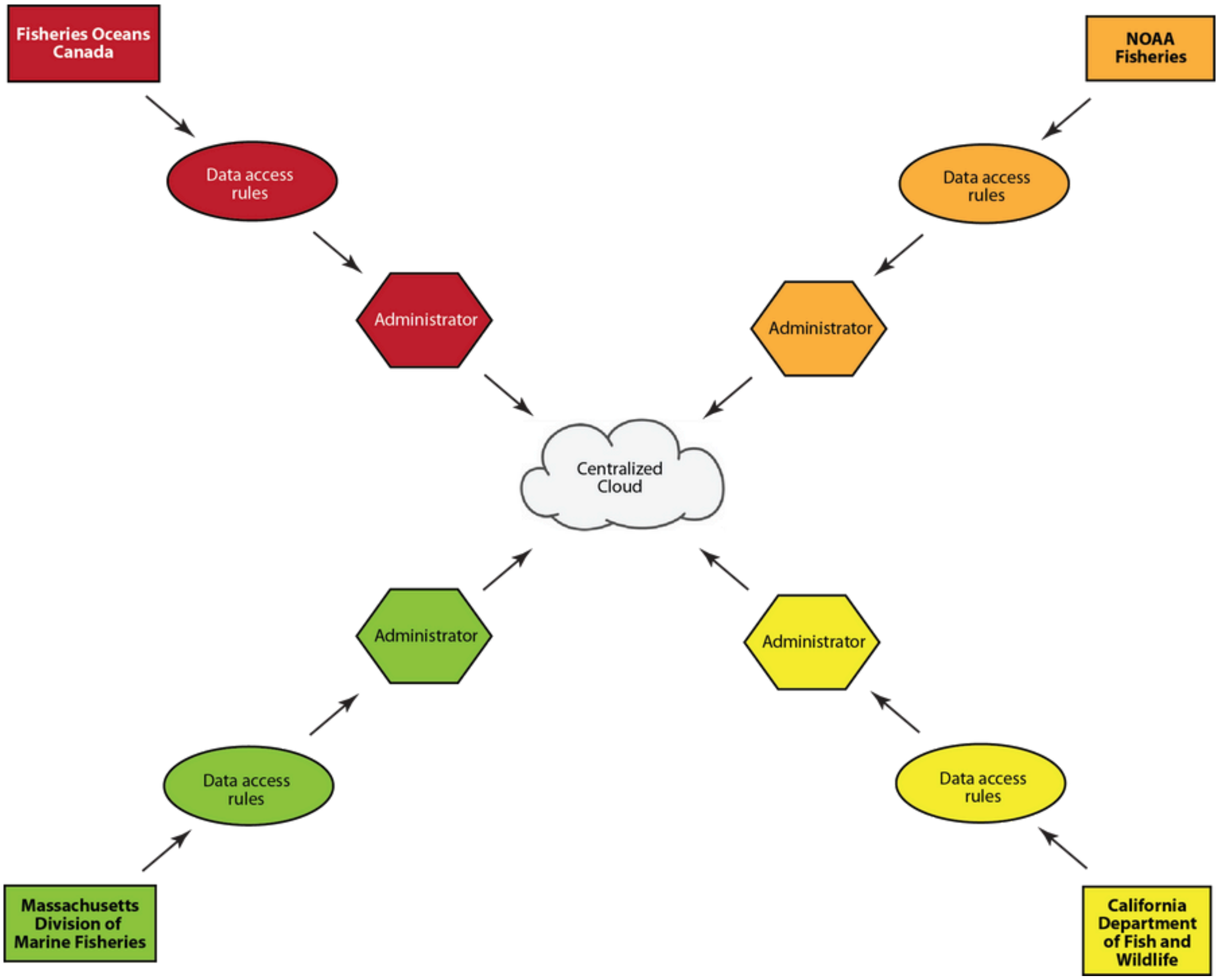


Figure 1. Example of several different jurisdictions, each with their own data access rules and administrator, establishing and maintaining users from their respective jurisdictions in the centralized cloud database. In the example here, Fisheries and Oceans Canada would regulate access by Canadian fishers and DFO Conservation & Protection (enforcement), NOAA Fisheries would regulate access by U.S. fishers with federal licenses as well as Coast Guard and NOAA Office of Law Enforcement (federal enforcement agencies), the Massachusetts Division of Marine Fisheries would regulate access by Massachusetts license holders and Massachusetts Environmental Police (enforcement), and the California Department of Fish and Wildlife (CDFW) would regulate access by California license holders and CDFW Law Enforcement Division. In reality, there would be many jurisdictions that regulate access to data in the cloud database, not just the four depicted here.

HOW WOULD IT WORK?

If a fisher wishes to begin using on-demand gear, they would contact the regulatory authority under whose jurisdiction they currently fish to register themselves for on-demand fishing. The on-demand administrator for that authority would (1) have the fisher report basic information (e.g., name, contact information, registration number) and sign any required documents that indicate the fisher's explicit authorization to share the location of their own on-demand gear for the purposes of minimizing gear conflict and enabling enforcement (e.g., permission to satisfy the MSA), (2) verify that the fisher is legitimately permitted to fish in that jurisdiction, (3) share with the fisher information about the data access rules for their jurisdiction, and (4) issue a special permit for the fisher to fish commercially with on-demand gear in an area that is closed to fishing with persistent vertical lines. The on-demand administrator would then share with the cloud service provider information about the fisher, and the cloud service provider would establish an account for the fisher. The fisher would then be provided credentials to access their account in the cloud database, and they would be free to purchase on-demand gear that is certified for use in that jurisdiction and register device identification information for their newly purchased gear in the cloud database. When the fisher uses the on-demand gear, data about the location of their gear would be shared with other users and enforcement according to that jurisdiction's data access rules.

The role of a regulatory authority's on-demand administrator is to (1) collect information from fishers that wish to use on-demand gear, (2) inform the fisher of data access rules, (3) issue a permit for on-demand fishing, and (4) provide information about new fishers to the cloud service provider for the establishment of fisher accounts. Each on-demand administrator also plays an active role in the development of the data access rules for their jurisdiction in consultation with fishers, enforcement and the cloud service provider.

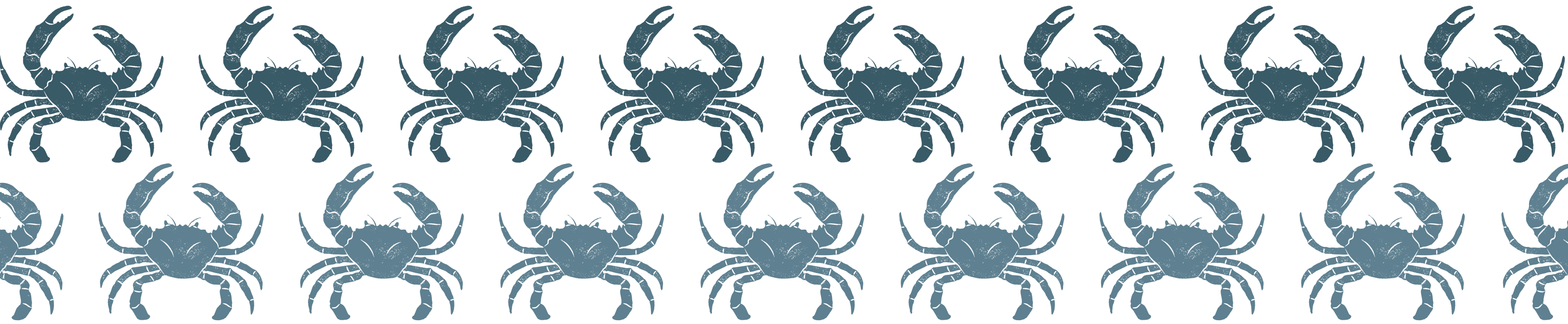
The role of the cloud service provider is to provide all of the technical infrastructure of the cloud database, including secure storage of and access to gear location data and fisher personal information from authorized users. The cloud service provider does not make any decisions about who is allowed access to these data; these decisions are made by each regulatory authority's on-demand administrator in consultation with fishers and enforcement.

MECHANICS OF DATA SHARING

When a fisher sets a traditional trawl, the buoys (and perhaps high-flyers and/or radar reflectors) atop the end lines of the trawl are visible at the sea surface and are used by other fishers (both fixed and mobile) to help avoid laying over or dragging dredges or nets through that trawl. In the same sense that buoys help to localize the gear on the sea floor to minimize this gear conflict, location data for the terminal ends of on-demand trawls without end lines and buoys must be made available to other fishers to minimize gear conflict. Moreover, the end lines and surface buoys as well as the markings on the surface buoys allow enforcement to discover, identify, haul and inspect gear. Both the location of on-demand fishing gear, its owner's identity, and any information required to facilitate hauling the gear (e.g., a private passkey to enable remote release) must similarly be accessible to enforcement.

In areas where both the density of fixed fishing gear is low (e.g., hundreds of meters or more between trawls) and the chance of gear moving (either because of gear conflict or storms) is low, location data may consist only of surface deployment positions collected via GPS (i.e., the location of the ship when the gear left the deck). However, in areas where the density of fixed fishing gear is high (e.g., tens of meters or less between trawls) or there is a high chance of unattended gear moving, underwater acoustic detection and localization of on-demand gear may be needed (i.e., localization of where the gear rests on the sea floor). In such cases, the location of gear can be estimated locally (with directional ranging technology) or computed in the cloud using acoustic localization information contributed by numerous passing fishing vessels in a process called "community localization" that relies on acoustic interoperability.

Hence, to minimize gear conflict and enable enforcement, a fisher must share (1) any information required by enforcement to identify, locate and haul their on-demand gear, (2) surface deployment location data of their on-demand gear, and (3) acoustic localization information for their on-demand gear as well as other fishers' on-demand gear if in a region/jurisdiction that uses acoustic localization. Additionally, a user may wish to share the status of their on-demand gear with a manufacturer to improve customer support.



Photos: @aketchify via Canva.com

USERS AND PRIVACY

There are multiple end users that could potentially benefit from access to data shared by the fisher, but it is important to stress that **on-demand data must only be shared with appropriate users.** Some data sharing will be mandatory for the purposes of minimizing gear conflict and enabling enforcement (Table 1). For example, sharing identification and hauling information with relevant enforcement agencies would be mandatory, as would sharing gear location information with fishers that are currently close to one's gear. However, some data sharing could be at the discretion of the fisher (i.e., voluntary), such as sharing status information with a gear manufacturer or sharing gear location and hauling information with a business partner, trusted friend or family member. A data governance policy for on-demand fishing must specify access rules, including what data are shareable, with whom it can be shared, when and where it can be shared, and for what purposes it is to be shared. Some data access rules may differ between fisheries, such as the distance from one's gear another fisher must be within to have access to gear location information, or whether a regulatory body tasked with monitoring the target stock can access summarized gear location information to quantify fishing effort.

THE CLOUD

Data collected by a fisher must be made easily and readily accessible to enforcement agencies and other nearby fishers to enable enforcement and minimize gear conflict. Many fishers involved in on-demand gear trials have expressed the wish to have gear location data available in real time on chartplotters in their vessel's wheelhouse. Fishers may also wish to be able to interrogate and visualize their own gear locations from shore for research or planning purposes. Enforcement agencies have expressed a desire to have access to gear location and ownership information for their jurisdictions from shore to plan at-sea and covert activities. Enforcement will also need access to these data in real time at sea to facilitate locating, identifying, hauling and inspecting on-demand gear. To make these data accessible in all of these use cases, they must be transmitted to and stored in a database that is capable of disseminating those same data to all authorized users either on shore or at sea.This database is frequently referred to as "the cloud," since it is largely invisible to users. The concept of the cloud is ubiquitous in our lives and the many apps we access on a daily basis, including texts, emails, Wi-fi enabled thermostats, Facebook and Instagram, which are all examples of systems that accept, store, and disseminate data to authorized users using application-specific data access rules.

Table 1. Examples of data access rules for different users.

End user	Accessible information	Sharing
Gear owner	all information	N/A
Enforcement	fisher identification, information required to haul gear, gear location	Mandatory
Other fishers	gear location only when within certain distance	Mandatory
Manufacturer	gear status	Voluntary
Owner-authorized third party	hauling information, gear location	Voluntary
Regulator	gear location summary only	Fishery dependent

MOVING DATA FROM VESSEL TO CLOUD

The on-demand community has articulated a few visions for how data would be transmitted from a fishing vessel to the cloud. There is general agreement that data should be relayed to shore via a full-time, real-time, at-sea Internet connection provided by a cellular or satellite provider, although if data volume is very low, other satellite connectivity solutions (e.g., Iridium) may be possible. An Internet connection can take advantage of all the security features that we regularly depend on for reliable and private network traffic.

One vision of transmitting the data to a centralized cloud database is to have each manufacturer create their own cloud database to which the data are transmitted from the fishing vessel (Figure 2a).Using a standardized application programming interface (API), the manufacturer's cloud database would then transmit the data to a centralized cloud database where the data can be accessed by other authorized users, including those that use other manufacturers' gear. When disseminating data, the centralized cloud would transmit data directly to the user (e.g., another fisher on a vessel at sea).

The benefits of such a system are that gear manufacturers would have access to their customers' gear location and status information to (1) help them improve their products and (2) allow them to provide better service to their customers should they have problems. However, there are several drawbacks to this approach. Having the data pass through a manufacturer's cloud service has potential confidentiality and security implications, as the manufacturer must store and transmit the data in a way that ensures privacy. Security and privacy procedures may vary between manufacturers unless there are agreed-upon minimum standards. There are also concerns over latency, which is the elapsed time between a fisher transmitting the data to the cloud and another authorized user receiving that same data from the cloud. For example, in circumstances where two fishers are fishing in the same area and are recovering and deploying on-demand gear close to one another, real-time updates with very low latency (e.g., tens of seconds or less) are essential to avoid gear conflict. Including a manufacturer's cloud database between the fishing vessel and the centralized cloud has the potential to increase latency, particularly if there are any problems with the manufacturers cloud database. Using manufacturer clouds also forces the fisher to opt-in to data sharing with the manufacturer to have their gear location information shared with other users, and it forces manufacturers to provide cloud databases, which could be a barrier to entry for new gear manufacturers with no expertise in developing cloud databases.

Alternatively, data can be transmitted directly from a fishing vessel to the centralized cloud database via the Internet in the same way data are disseminated from the centralized cloud to users directly (Figure 2b). This has the advantage of maximizing data security by transmitting it just once and storing it in only one location, keeping latency as low as possible, and freeing gear manufacturers from having to provide cloud services. If fishers wish to share their data with manufacturers, the centralized cloud database can be built in such a way to allow fishers to authorize manufacturers to access their gear location and status data. Provisions can be made to allow vendor-specific gear status information to be transmitted to the cloud for access and use by manufacturers if granted permission by fishers. This allows the fisher to opt-out by default or actively opt-in to data sharing with the manufacturer without having any effect on data sharing with other users.

MOVING DATA TO A CENTRALIZED CLOUD AND OPTIONALLY TO A MANUFACTURER'S CLOUD

Our recommended alternative is to have the fishing vessel transmit data to the centralized cloud, and optionally to a manufacturer's cloud (Figure 2c). With the data being transmitted directly to the centralized cloud for dissemination to other users, the manufacturer's cloud is not critical for minimizing gear conflict or enabling enforcement. Sending data to the manufacturer's cloud could be optional in the sense that a particular manufacturer may or may not offer this service, or a fisher could opt-out of sending their data to the manufacturer if a manufacturer provided the service. Although there may still be security concerns with this scenario, it is up to the fisher and the manufacturer to decide if this data sharing arrangement is mutually beneficial.

One Centralized Cloud or Many De-Centralized Clouds?

A centralized cloud to which all on-demand data (regardless of fishing jurisdiction) is transmitted simplifies data access and is particularly helpful at the edges of fishing grounds where fishers from two different jurisdictions may interact. The preeminent example of this is the Gray Zone that overlaps the border between the state of Maine and the province of New Brunswick where U.S. and Canadian fishers operate in the same waters. A centralized cloud that serves both U.S. and Canadian fishers would work seamlessly for such an area, whereas two separate clouds (one for U.S. fishers and one for Canadian fishers) may be much more challenging. However, if on-demand fishing becomes more widely used globally, it could make sense to decentralize the cloud.

A centralized cloud vs. multiple clouds serving the same function is not an unknown problem in the world of computer science. One way to think of the cloud for on-demand fishing is to think of how the cloud is used in other more common applications. One has no trouble accessing Facebook posts or Instagram feeds originating in other countries from the U.S. or Canada because both services use a centralized cloud (or at least what looks to the user like a centralized cloud; in reality, there may be many databases with bridges between them). This is an area where the advice of knowledgeable software engineers with specific expertise in cloud database development would be helpful, but it is likely that a single centralized database will serve the North American on-demand fishing community for a long time to come simply because the data volumes and transmission frequencies will be small.

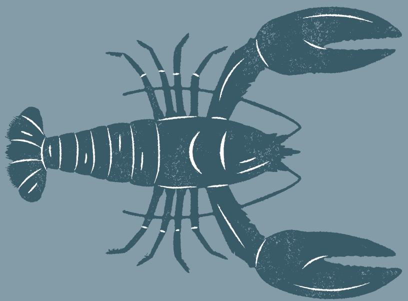
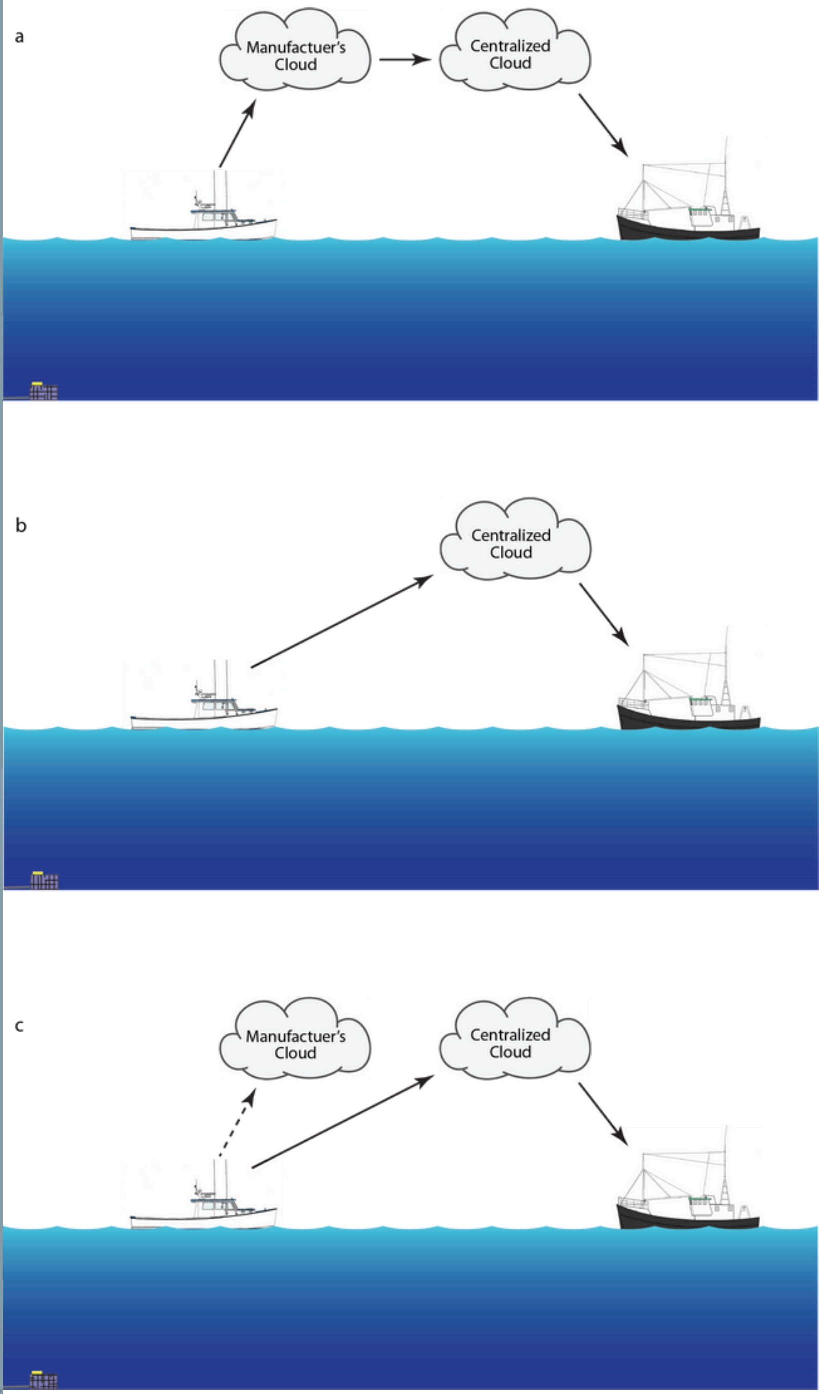


Photo: @aketchify via Canva.com

Figure 2. Options for moving data from a fishing vessel into the cloud, and then out of the cloud to other authorized users. The illustrated example shows location data for the on-demand gear (lower left) being transmitted from a fixed fishing vessel (at left) to the cloud, and the cloud transmitting that same data to a mobile fishing vessel (at right). Pathways include data relayed from the fixed fishing vessel to (a) a manufacturer's cloud database, then to the centralized cloud database, and finally to the mobile fishing vessel, (b) the centralized cloud database and then to the mobile fishing vessel, and (c) both a manufacturer's cloud database and the centralized cloud database, and then from the centralized cloud database to the mobile fishing vessel. Transmission to the manufacturer's cloud database in (c) could be optional (indicated by a dashed line). Latency is measured as the elapsed time between the fixed fishing vessel transmitting location data and the mobile fishing vessel receiving those same data.



DATA GOVERNANCE

The data to be shared to minimize gear conflict and enable enforcement for on-demand fishing can be considered to contain sensitive business information about a fisher's fishing operations (i.e., identification information, fishing locations). As such, data privacy is an important concern, so issues such as who owns the data, where it resides, and with whom it can be shared must be carefully addressed. Sharing on-demand fishing data is in the interests of both the fisher who generates the data as well as their fishing community, both to reduce gear conflict and to promote fairness through enforcement. Hypothetically, one could think of these data as being owned by the fisher who collects them; therefore they, the fisher, ought to control the use of and access to these data. However, the community benefits of minimizing gear conflict and enforcement suggest that some structure or framework for sharing should be agreed upon, and thereafter fishers using on-demand gear would share their data within the bounds and rules of that framework. We refer to this framework as the data governance policy. Because of the community benefits of data sharing, a fisher should not be free to opt-out of the framework and still fish on-demand gear; doing so would only increase gear conflict and thwart enforcement. Thus, some requirements for data sharing will be necessary for on-demand fishing, but who determines those requirements and how they are mandated and enforced needs to be resolved. The following sections contemplate the benefits and challenges of two potential approaches to data governance: one instituted and managed by regulatory authorities (government) and one managed by user agreements that operates outside of government. We do not recommend either approach as explicitly described below, but instead a hybrid of the two (described in the final paragraph as well as the Recommendations section above).

Data Governance by Regulatory Authorities

One model of data governance is to have the same regulatory authorities that issue commercial permits and regulate fishing operations take responsibility for collecting, managing, and disseminating all data associated with on-demand fishing for the purposes of minimizing gear conflict and enabling enforcement. In principle, government is involved in commercial fisheries to promote commerce, fairness and safety while simultaneously protecting the health and sustainability of target stocks and the environment. Providing the infrastructure for on-demand fishing is perfectly aligned with these goals, and therefore an appropriate role for government to assume. One of the primary benefits of having regulatory authorities manage on-demand data is that they have the authority to regulate (i.e., impose) a data governance policy as a rule or condition of a permit so that standardized data collection and dissemination is mandatory. As described above, this guarantees the benefits to both the individual fisher (as a data provider) and the fishing community (as users of those data) of minimizing gear conflict and enabling enforcement in a manner that is analogous to the currently regulated system of surface markers.

Photo: @aketchify via Canva.com

There are challenges with this model of data governance, however. In the U.S., data that are submitted to the Secretary of Commerce, a State fishery management agency, or a marine fisheries commission in compliance with the requirements of the MSA fall under the confidentiality provision of the MSA (Section 402b) and cannot be disclosed except under limited circumstances. This would suggest that a regulatory authority in the U.S. could collect on-demand data from fishers but might be unable to then share that data with other users. However, one of the exceptions to the confidentiality requirement in Section 402b allows disclosure "when the Secretary has obtained written authorization from the person submitting such information to release such information to persons for reasons not otherwise provided for in this subsection, and such release does not violate other requirements of this Act" 16 U.S.C. § 1881a(b)(1)(F). It may be possible, then, especially where the data are not required in order to comply with the MSA, for regulators to obtain written authorization from every fisher using on-demand gear that expressly allows on-demand data to be shared with other users only for the purposes of minimizing gear conflict and enabling enforcement. A careful legal review of the MSA is warranted to determine if this approach is tenable. In practice, the centralized cloud database could be housed within a government agency and the government could provide all of the information technology services required to receive, store and disseminate those data. A government-hosted cloud database may be slow to initially develop, slow to adapt to new and improved technologies in the future, and subject to varying degrees of funding depending on Congressional interest. Data contributions from other jurisdictions (e.g., from Canadian fishers to a NOAA Fisheries-hosted cloud database) may be very difficult to justify and implement. As such, it is more plausible and practical that a contracted organization outside of government could take on the technical role of receiving, storing and disseminating on-demand fishing data, which reduces the burden and most likely the cost of implementation for regulatory authorities. Depending on how this organization is contracted by the regulatory authorities, the data they collect may still be considered as submitted to a U.S. regulatory authority and therefore subject to confidentiality protections like those in the MSA. Additional legal review is needed to understand whether on-demand fishing data transmitted to an organization outside of government but supported by government to provide services necessary for on demand fishing are still considered as submitted to the government.

Another challenge with a government-run model of data governance is the fact that there are many regulatory authorities, such as state fishery agencies, NOAA Fisheries, and Fisheries and Oceans Canada. Each of these authorities have their own jurisdictions, regulations, licensing requirements, fishing conditions and enforcement agencies, and therefore may need different data access rules. It is important to note that data access rules do not need to be identical across jurisdictions to use a single centralized cloud database; the design of the cloud database should accommodate different data access rules for different jurisdictions. Regulatory authorities can decide on access rules for their jurisdiction in consultation with their fisheries, and then database administrators can work with the organization providing cloud services to ensure that those rules are incorporated into the database design (Figure 1). These same administrators would be responsible for maintaining user information in the cloud database for fishers and enforcement agencies in their jurisdiction (e.g., verifying and registering new users, providing user access permissions based on the data access rules). Some examples of data access rules include (1) the distance at which vessels at sea can have access to nearby on-demand gear locations, (2) how long gear location data should be stored in the cloud database after recovery, (3) who is allowed to access such post-recovery data, and (4) what data should enforcement have access to, when should they have access to it (e.g., only at sea or on shore as well?) and for how long should they have access.

Data Governance by User Agreements

Implementing data governance without involvement by any regulatory authority might be possible through user agreements. In this model, fishers wishing to fish with on-demand gear would agree to transmit their data to a centralized cloud database where it would be stored and disseminated exactly as described above. This cloud database service would be provided by an organization external to government. The user agreement would specify with whom the on-demand data could be shared, such as other fishers near one's gear as well as state and federal enforcement agencies. Data governance, in this model, would not be mandated, but instead fishers would opt-in to a system that is presumably mutually beneficial for all fishers because it would minimize gear conflict and promote fairness through enforcement. Although there may be government users of the data, such as enforcement agencies, the database itself would be entirely private, not unlike a cloud database used for text messaging services offered by a private company (e.g., WhatsApp from Meta or iMessage from Apple).

While this approach does have the potential advantage of being external to the U.S. government and therefore not subject to the confidentiality provisions of the MSA, there are some drawbacks. Without regulatory agencies involved, there is no mandate to use this private system. If a fisher does not like the user agreement (say, they do not want their on-demand gear location data to be shared with enforcement), would they be free to forgo using it and still be able to fish on-demand gear? There would be nothing to prevent multiple organizations from providing this same service, and there would be no guarantee that the various clouds would communicate with one another. It would then be possible to have many cloud databases providing services for fishers fishing the exact same fishing grounds, which would run counter to the goals of minimizing gear conflict. It is also difficult to envision how data access rules might change from one area to another without a regulatory authority to consult with the fisheries and establish those data access rules. It would be quite unclear who is authorized to set those rules, over what area those rules apply, and by what mechanism a fishery organization or group of fishers would assert authority to set the rules.

Finally, while the cloud services under the model of data governance by regulatory authorities would almost surely be paid for with government (tax) funds, a wholly private cloud database and associated services would need to be paid for by the users. One of those users might be government (enforcement), so perhaps government would pay most of the cost, but perhaps not.

Working Group Recommendations for Data Governance

While a fully private on-demand cloud database has many challenges, so too does a fully government-housed database. We recommend a hybrid approach that combines mandates, tailored data access rules and jurisdictional administration afforded by regulatory authorities together with the technical advantages of cloud database services provided by an organization external to government. User agreements for each jurisdiction could provide a mechanism for fishers to explicitly consent to data sharing under the data access rules established in their region, but these would be unnecessary if sharing is mandated through jurisdictional rules or permit provisions.