Responsible Sensing Lab

Responsible data use Digitale Gracht

Thijs Turèl, Girish Vaidaya and Fabian Geiser

7 May 2024

Management Summary

The Digitale Gracht was conceived a few years ago. As we approach a new tender cycle, now is a favorable moment for a thorough reassessment. This report outlines the findings of an investigation conducted by the Responsible Sensing Lab in collaboration with experts from Delft University of Technology (TU Delft). The focus of the investigation was on evaluating and suggesting alternatives to the Digitale Gracht system and the associated “binnenhavengeld” (Dutch for inner harbor fees) payment process, as requested by "Programma Varen." The investigation is based on non-statutory norms, particularly responsibility and proportionality. The term 'responsible' refers to the consideration of public values outlined in Amsterdam's policy notes, while 'proportionality' involves assessing the alignment between system goals and the methods employed. Table 1 presents the primary issues and corresponding recommendations identified in this investigation.

General issues and recommendations for improvement	
5.1 Vendor dependency	5.1.a Retain system knowledge internally
	5.1.b Reduce single vendor dependency
5.2 Function creep	5.2.a Appoint data stewards
5.3 Limited shared understanding between municipality and vendors	5.3.a Simplify the system
	5.3.b Maintain living documentation
	5.3.c Monitor system performance
5.4 Limited awareness about Digitale Gracht of waterway users	5.4.a Establish proactive public communication
5.5 Undefined data access policy	5.5.a Limit data access on a need-to-know basis
	5.5.b Limit dependence on the Vignette Administration
5.6 Information-driven enforcement	5.6.a Don't rely exclusively on a data driven approach for prioritizing the deployment of enforcers
Issues and recommendations for specific objectives	
5.7 Excessive data collection for traffic monitoring	5.7.a Aim for data minimization for during traffic monitoring
5.8 Proportionality of approach towards detection of illegal passenger rides	5.8.a Reconsider illegal passenger shipping detection approach
5.9 Proportionality of approach towards noise monitoring	5.9.a Reconsider approach to noise monitoring via sensors to combat noise pollution

Table 1: Overview of the identified issues and corresponding recommendations.

Table of Contents

1. Introduction

The Digitale Gracht (Dutch for Digital Canal) is a traffic monitoring system operating on Amsterdam's inland waterways. The system serves to support policy development, management of the waterways and monitoring and enforcement on the water. The Digitale Gracht, initially developed by Waternet, and since 2020 owned by the municipality of Amsterdam, has recently become a subject of scrutiny within the municipal operations in discussions on public values. While some of the system's features proved to be valuable in monitoring the waterways, its design has sparked concerns within the municipality and has prompted the ICT team of the “Programma Varen” to act by deactivating several functionalities of the Digitale Gracht. A comprehensive re-evaluation has become necessary to address the growing questions surrounding the Digitale Gracht's alignment with the municipality's digitalisation objectives.

This report presents the outcome of an investigation aiming to evaluate and propose alternatives to the Digitale Gracht system and the related “binnenhavengeld” (Dutch for inner harbor fees; also known as BHG) payment process carried out by the Responsible Sensing Lab in collaboration with experts from the Delft University of Technology (TU Delft) on request of the “Programma Varen.” The investigation focused on identifying issues and proposing alternatives based on non-statutory norms (in Dutch “bovenwettelijke normen”) with a specific emphasis on responsibility and proportionality. The term 'responsible' encompasses the degree to which relevant public values, outlined in Amsterdam's policy documents, including the Digital city agenda, Amsterdam data strategy, and coalition agreement, have been conscientiously considered in the operation of this socio-technical system. Proportionality, on the other hand, revolves around the examination of the relationship between the system's goals and the methods used to reach these goals.

This investigation is confined to the current state of the Digitale Gracht system (September to December 2023) and concrete proposals for changes to systems that are in development or have been tested in the past. Additionally, the scope extends to the examination of the relation with the BHG payment process. The BHG payment process was included in the scope of this investigation, although it is not formally integrated into the Digitale Gracht system, as it relies partially on the same technological foundations and is described in a single shared privacy statement.

This report is structured as follows. Section 2 introduces the approaches employed in this investigation. Section 3 presents an outline of the Digitale Gracht system. Section 4 introduces the BHG payment process. Section 5 lists the identified issues and corresponding recommendations for alternative solutions. Section 6 concludes the report presenting potential follow up projects to further develop some of the most promising alternatives recommended in the previous section.

2. Process

This section describes the approaches employed throughout the investigation in three main steps.

2.1 Step 1: Building a comprehensive understanding of the Digitale Gracht system and BHG payment process

The primary aim of the initial step was to establish a comprehensive understanding of the Digitale Gracht system and its operational intricacies. Additionally, the focus extended to gaining insights into the BHG payment process. This involved exploring the system's objectives, key stakeholders, and operational processes, both theoretically and in practical implementation.

The exploration of the Digitale Gracht system and the systems deployed for the BHG payment process was done based on a list of questions compiled from impact the assessment toolkits IAMA (Impact Assessment Mensenrechten en Algoritmes), AIIA (AI Impact Assessment), DPIA (Data protection impact assessment) and Plot4ai. These toolkits were chosen as they are adopted by the Dutch national government and/or industry. The questions from these toolkits were suitably reformulated to remove the artificial intelligence focus. Furthermore, only descriptive questions (i.e., questions exploring how a system works) were considered. The full question list can be found in Appendix 1.
Information on the Digitale Gracht and BHG process was gathered from seven semi-structured interviews with a total of ten participants playing critical roles in the development and use of the Digitale Gracht system. The list of participants includes representatives from:

- Nautical policy (Programma Varen),
- “Nautisch Beheer”, Dutch for Nautical management (Programma Varen),
- “Nautisch Toezicht & Handhaving”, Dutch for Nautical supervision and enforcement (THOR),
- ICT team of the “Programma Varen”,
- Global Guide Systems (Supplier),
- PortPay (Supplier).

Furthermore, relevant documentation such as the privacy statement and DPIA related to the Digitale Gracht system were studied. The information gathered from the interviews and documents was refined through follow-up meetings and emails with the interviewees. Lastly, a description of the Digitale Gracht and BHG payment systems was written up based on the information gathered and verified with all interview participants.

2.2 Step 2: Identify issues and improvement opportunities

The exploration of issues and improvement opportunities associated with the Digitale Gracht and BHG payment systems was a collaborative effort undertaken by the Responsible Sensing Lab team in conjunction with Marijn Janssen (Professor in ICT & Governance) and

Kars Alfrink (Researcher Contestable AI) from Delft University of Technology. Building upon a foundational understanding of these systems, the joint analysis drew from all collaborators' collective expertise, incorporating insights from previous projects as well as policy guidelines embraced by the city of Amsterdam, such as the Digital city agenda. Furthermore, established frameworks from relevant literature, including the "Data Governance Principles" (Janssen et al., 2020) and "Contestable AI by Design" (Alfrink et al., 2022) frameworks were applied to systematically identify potential issues and improvement opportunities. A number of issues and improvement opportunities were additionally highlighted by the collaborators from the "Programma Varen" of the city of Amsterdam.

2.3 Step 3: Recommend alternatives

The recommendations for alternatives to the Digitale Gracht and BHG payment system were formulated in response to issues identified in Step 2. This was done in collaboration with Prof. Marijn Janssen, Kars Alfrink, and Sander Flight (Privacy expert of the Responsible Sensing Lab).

3. The Digitale Gracht system

This section presents an outline of the Digitale Gracht system. The information presented in this section, together with the description of the BHG payment process presented in section 4, serves as a foundation for the issues and improvement opportunities identified in this report.

3.1 Goals and related systems

The Digitale Gracht has five key objectives, which are presented below in order of importance as indicated by the Digitale Gracht team:

1. Insight into the crowdedness in the canals,
2. Reducing illegal passenger shipping,
3. Reducing noise pollution on the water,
4. Reducing speed violations,
5. Regulate mooring places for commercial vessels.

1. Insight into the crowdedness in the canals

In support of the legal mandates, to guarantee smooth and safe traffic on the waterways, the municipality of Amsterdam has implemented a comprehensive system for monitoring waterway traffic. This encompasses commercial, private, and non-motorized vessels, contributing to the prevention of nuisance, enhancement of livability, and optimal utilization of the city's water resources.

The Digitale Gracht employs various sensing systems to gather information on waterway activity:

- **RFID readers and vignettes:** These devices record passages by detecting chips in vignettes (Vignettes are mandatory for motorized vessels). With each passage the chip's unique hardware number, timestamp, sensor ID, and direction is captured.
- The data collected by the RFID readers are classified by vignette type (e.g., pleasure or passenger shipping vessel) using the hardware number by connecting it to the BHG database. This database is a list of hardware numbers and the associated vessel categories. (This is a database separate from the Vignette Administration. More about the Vignette Administration in section 4.)
- **Cameras** are used to identify vessels without vignettes, recording passage events, time, sensor IDs, and directions. No video data is saved.
- **AIS transponders and antennas** are employed to monitor the traffic of commercial and larger privately owned vessels and determine the crowdedness per reach. In the Netherlands, AIS data is mandatory for commercial vessels and for private vessels at least 20 meters long. Their data is visible in near real-time. AIS antennas record vessel information, including the MMSI number (Maritime Mobile Service Identity Number), which acts as a vessel ID, as well as the vessel's location, timestamp, direction, and speed. This data is captured every five to fifteen seconds. Additional details such as the vessel name, type, size, and flag are collected with lower

frequency. AIS data is labeled as personal data as people may live on the boats that are being monitored.

An overview of the distribution of sensors used for the Digitale Gracht can be seen in Figure 1. Figure 2 shows an example of a Digitale Gracht sensor.

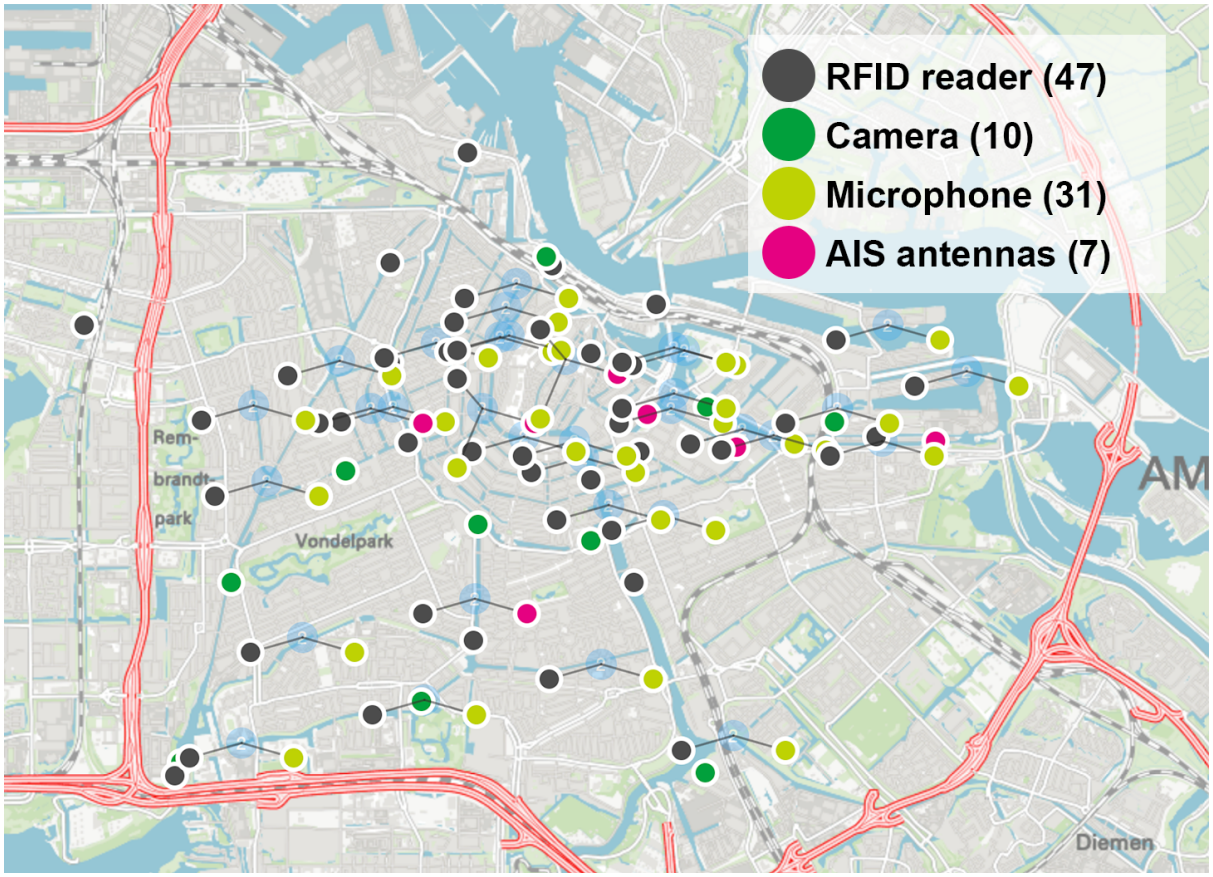

Figure 1 - Overview of the placement, type, and amount (between brackets) of sensors used for the Digitale Gracht system taken from sensorenregister.amsterdam.nl. Note that this overview represents the situation in 2022. Some changes have been made since then.

2. Reducing illegal passenger shipping

The specific objective of this segment of the system is to identify privately owned vessels engaged in illegal passenger rides. A license is required for commercial passenger transport. To achieve this, a rule-based algorithm was developed which would profile and detect vessels suspected of providing passenger rides without the requisite permit. The algorithm is currently not active (see figure 3 and table 2). It was intended to process the data collected by RFID readers to identify vessels showcasing repetitive sailing patterns. Suspected vessels identified through this algorithm were included in a weekly report.

3. Reducing noise pollution on the water

The issue of noise pollution on and around the waterways of Amsterdam is evident and reflected in reports submitted by residents and stored in the municipal incident reporting system ‘Signalen in Amsterdam’ (SIG). In response, the municipality aims to address noise concerns caused by waterway users through the Digitale Gracht system.

Until recently, noise events from the canals were registered using AllSense sensors. These sensors are a combination of an RFID reader, a camera and two microphones. The camera and microphones in the AllSense sensors are inactive at the time of writing. AllSense used to record the timestamp, sensor ID (and thereby location), and dB level of noise events, indicating occasions when a specific dB threshold was exceeded at a specific time and place.
To detect noise violation by an individual vessel, a noise monitoring reporting application was developed and tested several years ago. This application is currently inactive. The reporting application relied on data collected from the AllSense sensors, which in case of a noise event on the water, would capture audio, video, sensor ID, time, and the unique hardware number of the vessel present during the noise event.

Figure 2 - A Digitale Gracht sensor and reference sticker (red box) at the Marineterrein. The sensor depicted in the picture is an AllSense sensor.

4. Reduce speed violations

The municipality of Amsterdam aims to minimize speed violations by commercial vessels within the waterways. The Digitale Gracht system was originally designed to detect such violations utilizing AIS data. The AIS data collected by the Digitale Gracht system provides insights into the speed, location, and the unique MMSI number of commercial vessels. An algorithm was intended to leverage this data to monitor speed violations and generate reports, identifying vessels involved in such violations.

5. Regulate mooring places for commercial shipping

Commercial vessels (such as passenger vessels and transport vessels) may only moor at berths licensed to them or at marinas. The Digitale Gracht system was intended to identify and generate reports on vessels which moor outside of these locations at night. If a vessel is

found to be outside its licensed berth or a safe zone during these hours, it is included in the daily report. It is important to note that, as of now, this functionality is currently deactivated.

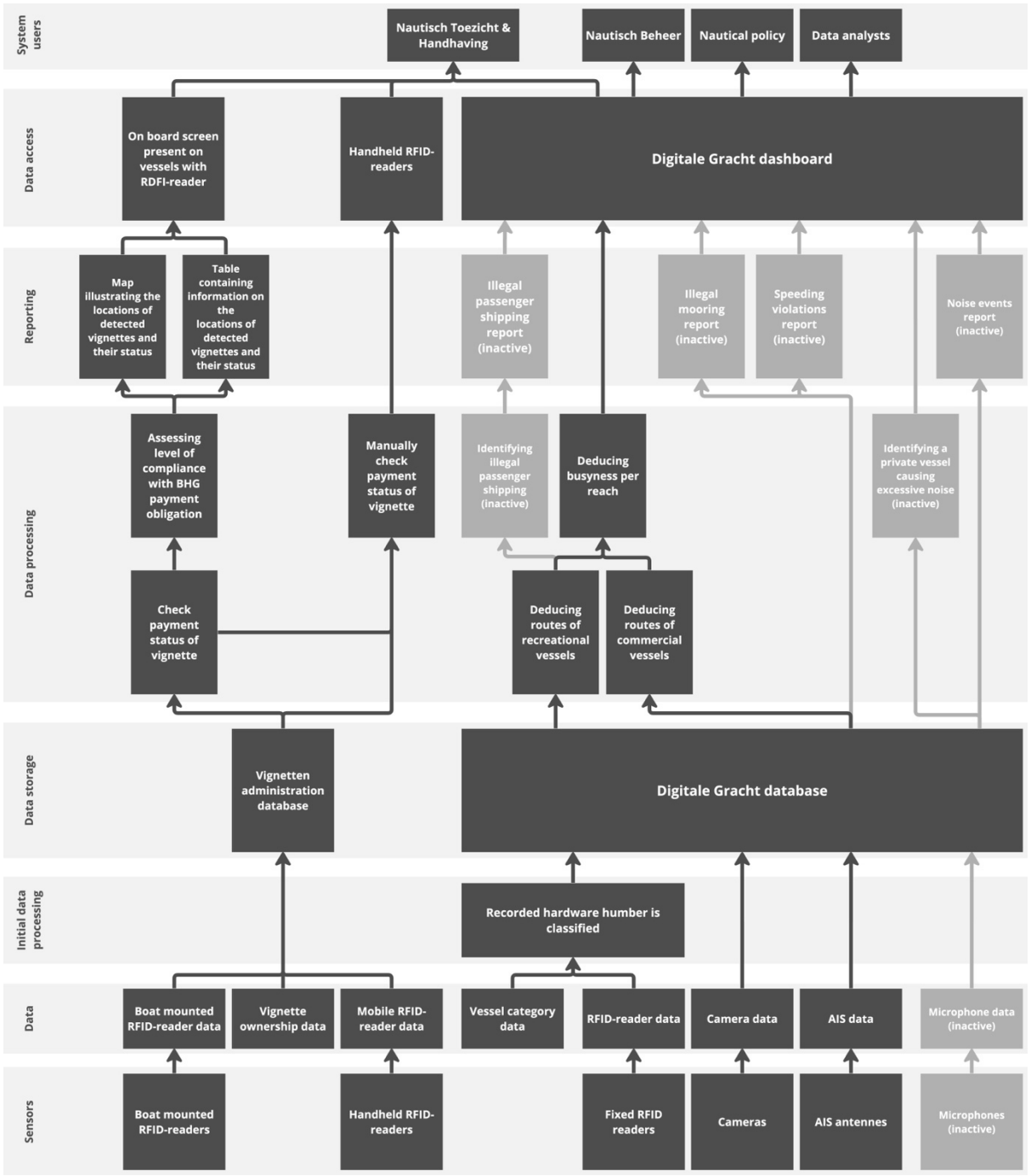

Figure 3 - Overview of the data collection and data processing activities carried out in scope of the Digitale Gracht.

Functionality	Status
1. Overview busyness	Available
2. Noise pollution detection	Deactivated
3. Detection of illegal passenger shipping	Deactivated
4. Speed violation indicator	Available for commercial shipping
5. Detection of illegal use of mooring places	Deactivated

Table 2: Overview of Digitale Gracht functionalities and their status.

3.2 Internal stakeholders

The stakeholders which are actively involved within the municipality in the oversight and operation of the Digitale Gracht system are “Programma Varen” and “Toezicht en handhaving openbare ruimte”. These organizational entities play distinct roles in managing and utilizing the data collected by the Digitale Gracht.

1. Programma Varen

As the municipality’s internal party responsible for the Digitale Gracht, "Programma Varen" assumes ownership of the collected data and is made up of several teams involved in the Digitale Gracht system:

- ICT Team: Responsible for articulating the Digitale Gracht's requirements, coordinating changes with suppliers, and managing accounts for the Digitale Gracht dashboard.
- Nautical policy: Utilizes insights from the Digitale Gracht to and evaluate and substantiate existing policies and potentially propose new policies related to traffic, permits for commercial vessels, noise, speed, and mooring. The Nautical policy team ensures that citizens, businesses, and visitors are not disproportionately affected by policy changes.
- Nautisch Beheer: Interested in the information gathered to inform and justify short-term interventions, such as closing off waterways during works or events such as such as canal closures during events like the “Prinsengracht” concert.

2. Nautisch Toezicht & Handhaving

The team of Nautisch Toezicht & Handhaving of “Toezicht & Handhaving in de Openbare Ruimte” is responsible enforcing regulations and uses Digitale Gracht data for monitoring and intervention:

- Monitors speed, mooring, and noise violations, as well as detects illegal passenger rides.

- Responsible for issuing fines to violators and interested in information-driven deployment of BOAs (Buitengewoon Opsporings Ambtenaar) and sending warnings to vessels committing violations.

3. Suppliers

The Digitale Gracht system is developed and maintained by two suppliers: Global Guide Systems (GGS) and PortPay, a trading name for Improvement IT.

- GGS is a small-scale organization responsible for developing and managing the functionalities of the Digitale Gracht, including the dashboard. GGS owns the software code of the Digitale Gracht applications and collects AIS data.
- PortPay is a sub-supplier who provides sensors (excluding AIS receivers and antennas) for the Digitale Gracht. PortPay is responsible for system maintenance and conducts initial data processing and filtering before forwarding the data to GGS.

3.3 The Digitale Gracht dashboard

The information derived from the data collected by the Digitale Gracht system is made available through the Digitale Gracht dashboard. Access to this dashboard is exclusively granted through personal accounts managed by the ICT team, with eligibility restricted to municipality employees. Currently, certain BOAs of Nautisch Toezicht & Handhaving, policy advisors from Nautical policy, Nautisch Beheer, and researchers (such as data analysts from the city's department "Verkeer en Openbare Ruimte") have accounts. Via these accounts, all the information listed below is accessible. Researchers can, in addition, download raw data. According to GGS, the municipality has the possibility to finetune access within the dashboard. This functionality is currently not used.

The City of Amsterdam does not exchange personal data collected in scope of the Digitale Gracht with other organizations. In the past, other organizations, such as the police, have shown interest in gaining access to (sections of) the data. On the dashboard, the following information is accessible.

- Data collected by sensors:
    - The status of the vignette (Whether it is expired or not).
    - The type of vignette (e.g., passenger vessel).
    - The unique hardware number of vessels with vignettes for which a passage has been recorded by an RFID reader in the last 72h. Routes taken by private vessels (based on RFID data) are not directly visible on the dashboard but can be deduced from the hardware numbers that are recorded in a list.
    - MMSI number, Vessel name, Size of vessel, Current location, Route taken in the last 72h, Speed and Vessel name of commercial and large private vessel.
    - Noise events at specific locations (color indicator).
- Reports (currently no reports are accessible):
    - Illegal passenger shipping reports.
    - Noise reports.
    - Speeding reports.
    - Illegal mooring reports.

3.4 Relationship with citizens

The public is informed about the Digitale Gracht system through official stickers positioned alongside the sensors placed in public space as well as records of the sensors shown in the sensor register and an online privacy statement. The sensor register as well as the privacy statement prove to be somewhat outdated. Recently, a description of the algorithms used has been added to the algorithm register of the municipality of Amsterdam. Upon purchasing a vignette, vessel owners receive a letter which refers to a video on the website of the municipality. In the video it is mentioned that the vignettes contain chips which help the municipality to monitor traffic.
Citizens can inquire about the sensors and voice complaints via the contact information provided on the stickers and in the sensor register. There are no formal processes in place for objection, rectification, inspection, or deletion. As it stands, the system offers citizens no channels to access information about their vessels, except for publicly available AIS data collected for larger vessels.

4. The Binnenhavengeld (BHG) payment process

This section introduces the BHG payment process. The description presented in this section, together with the knowledge gathered on the Digitale Gracht system presented in the previous section, serves as a foundation for the issues and improvement opportunities identified in this report.

The municipality of Amsterdam has implemented a system to enforce compliance with the BHG payment obligation for non-commercial boat owners that use the city's waterways and moor within the city. The primary objectives are to verify BHG payments and sending reminders.

PortPay has been commissioned by the municipality to manage the BHG registration and collection process. For every vignette purchased, PortPay collects the following data: name, address, and city (NAW); citizen service number (BSN) and payment data from the person making the purchase; hardware number of the RFID chip and license number of the vignette; pictures of the vessel for which BHG is paid. The collected data is stored in the Vignette Administration database managed by PortPay.

BHG checks are executed by BOAs of Nautisch Toezicht & Handhaving. BOAs are deployed following a grid approach to manually inspect vessels in these areas. Handheld RFID-readers allow BOAs to access vignette records, providing personal information about the owner. In case of a violation of the payment requirement, a vessel owner is notified via SMS. If payment is not made within the stipulated period, the vessel may be towed away.

Service vessels of Nautisch Toezicht & Handhaving are equipped with vignette readers that count the number of vignettes in the vicinity of the vessel. Once a year, they compare the number of vignettes that are counted by this reader with the number of vessels counted by BOAs in the field to gain insight into compliance with the BHG payment obligation and the total number of vessels with and without vignettes present on the water. Additionally, the passage counts from cameras are compared with counts from the RFID-readers installed next to the waterways to gain insight into the compliance level. Cameras only record passages, meaning that no distinction can be made between vessels that do not require a BHG vignette, such as kayaks, and vessels that violate the BHG payment obligation and have not purchased a BHG vignette.

5. Issues and recommendations for alternatives

This section outlines the issues identified by the Responsible Sensing Lab in collaboration with Prof. Marijn Janssen and PhD candidate Kars Alfrink. For each issue, we provide one or several recommendations suggesting alternative approaches. The section is divided into two parts: the first addressing general issues and recommendations for the Digitale Gracht and BHG payment process, while the second delves into issues and recommendations for the specific objectives introduced in sections three and four of this report.

General issues and recommendations for alternatives

5.1 Vendor dependency

It is common for cities to engage the services of technological service providers and vendors. This necessarily introduces a dependence. Yet a lock-in should be avoided and the power balance addressed. The distribution of work in the current tender has led to a situation in which the one vendor and their supplier have substantial level of control over the system compared to the municipality of Amsterdam. The knowledge on the technical system predominantly resides with the vendors rather than within the city personnel. This introduces several risks.
The city is responsible for the day-to-day operation of the system but does not have the best information position to understand the operations and weigh the risks that come with operation. This is especially important in unforeseen situations. Should current vendors no longer be available (e.g., due to bankruptcy) the lack of documented knowledge could prove problematic. It prevents the city from taking over (part of the work) (Hubert, 2020, 2022).

But even in a planned shift of vendors (e.g., in case of a new tender period) the captive knowledge of the system makes it difficult for another vendor to take over the system without support from GGS and PortPay. The system has been custom built by the vendor for this application implying that the sensors and the software cannot be procured from the market. The city might lack the necessary knowledge to assess the incoming bids of competitors on their technical feasibility.

Furthermore, overdependence on a few vendors can limit innovation, increase costs, and influence security as vendors are bound to the commercial logic of providing what the tender requires, but not anything beyond. Lastly, a remote but possible security risk is posed by the possibility of a vendor being acquired by a company located in a non-European, non-friendly country.

Inspired by:

- *Digital city agenda 2023-2026, ambition on digital dependency (Gemeente Amsterdam, 2023).*
- *Amsterdam data strategy, Legitimate and monitored 'important that data flows are verifiable' (Gemeente Amsterdam, 2021).*

5.1.a Recommendation: Retain system knowledge internally

For the upcoming tender round, we advise to insource part of the 'higher-value chain' work that is now given out to vendors to retain internal knowledge and remain innovative.
We could imagine an internal design/development/operations team that builds and maintains applications that make use of the sensing data, where the availability of working sensors is procured from the market.
The city of Amsterdam is experimenting with this setup at the Innovation Departments Computer Vision Team. There, a tender has been written out successfully which keeps more high-end tasks in house, while outsourcing the less critical/easier to replace work.

5.1.b Recommendation: Reduce single vendor dependency

Avoid putting all your eggs in one basket. If the entire technological support is sourced at one vendor, this becomes problematic in a situation where the vendor would not deliver.

Alternatively, source the different applications with different vendors. Figure 4 presents a suggested system architecture diagram. One application could be for monitoring current traffic, which utilizes RFID and AIS data. Another application could be for analysis or simulation of traffic interventions, using the same data as traffic monitoring but including historical data. Further applications could support enforcement directed at private individuals, for issues like illegal passenger shipping or noise pollution and applications in support of enforcement directed at commercial companies, addressing concerns such as speed violations and mooring places. AIS data should be used prudently, because the system was introduced only for identification and position of vessels as specified in 2006 in the covenant between the Ministry of Traffic and Water and the inland shipping industry (Bureau Telematica Binnenvaart, 2024).

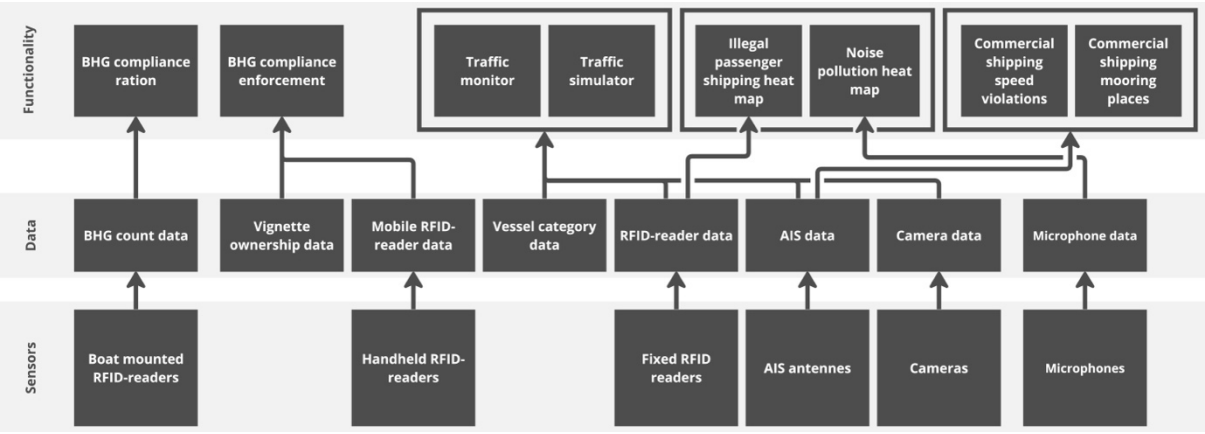

Figure 4 - Suggested system architecture diagram. This diagram represents a suggested departmentalization including functionalities that we advise to reconsider in this report. Colors indicate discrete purposes. Responsibilities and access can be distributed along verticals (policy aims) or horizontals (sensors/data/functionality).

5.2 Function creep

It is common for digital systems to be used for goals that were never originally intended. In a democratic organization this is called function creep. According to Bert-Jaap Koops, Professor of Regulation & Technology, University of Tilburg, function creep refers to a scenario where there is a sense that there hasn't been adequate opportunity for discussion regarding the desirability of a new function before its implementation (Koops, 2021).
With digital systems compared to physical systems, an added risk for function creep is that the amount of people involved, the needed effort and cost to make substantial changes that could make a system more invasive can be very low. Changing some lines of code, changing access rights or aggregation levels, adding a new tab to a dashboard combining some data can have grave effects, but can be done quickly. In a situation where suppliers would make their own decisions, new functions could remain unnoticed by Amsterdam.
The ultimate guard against function creep is continuous democratic legitimation for changes to the system. As costs to make technological changes decline, it is worthwhile to design barriers for unintended changes.

Inspired by:

- *Tada principle: Democratic and legitimate (tada.city, 2017).*

5.2.a Recommendation: Appoint data stewards
Knowledge compartmentalization helps to prevent unintended use of data. Data stewards can play an essential role in this. Data stewards should be from the municipality of Amsterdam as this enables the city to remain in control of their own data.

For example, consider splitting the system with a single data steward for each data source or sensor type, such as sensor hardware, RFID, sound, cameras, and other data sources like vignettes and AIS (see figure 4). A data steward is a role that is accountable for the data they collect and handle, ensuring it is used solely for its intended purpose and only by authorized individuals, who can be positioned internally or at suppliers. These stewards are the exclusive custodians of their respective data sets, and they are obligated to maintain transparency in data access by logging who accesses what data and when.

5.3 Limited shared understanding between municipality and vendors

Members of the Digitale Gracht team do not always have complete knowledge about the current functional status and that there is no complete up-to-date documentation. For example, while some of the interviewees from the municipality believed that radars were still active and used to record passages, the suppliers told us that radars had been switched off some time ago.

It is imperative for the personnel of the City of Amsterdam to possess a thorough understanding of the technical system as a prerequisite for maintaining control and assuming responsibility. The lack of shared understanding can be attributed to the complexity of the system, and the many changes that have been made to it over its lifetime. Insufficient up-to-date documentation further adds to the problem. In addition to presenting challenges for the city organization, this situation also adds complexity for individuals that do not belong to the city organization in understanding the ongoing developments.

Inspired by:

- *Amsterdam data strategy, Legitimate and monitored 'important that data flows are verifiable' (Gemeente Amsterdam, 2021).*

5.3.a Recommendation: Simplify the system

Simplify the system as much as possible. We contend that a simpler system provides clarity for the project team, delineating what it can and cannot accomplish. Moreover, simplification facilitates external scrutiny, protecting the project's reputation and mitigating PR risks. We believe that the complexity of the Digitale Gracht system stems from at least two characteristics. First, the system is complex due to the number of different aims and the integratedness of these different aims. An example of this is the use of the unique electronic identifiers for traffic monitoring as well as checking for payment of BHG. Splitting the system up as suggested in figure 4 could help to reduce complexity caused by entanglement of objectives and technical solutions. Second, some of the specific solutions chosen to enable certain functionalities contribute to the complexity of the Digitale Gracht system. An example of this is the current approach to traffic monitoring which uses a variety of sensors and processing approaches, among other recording passages of individual vessels and deducing the route these vessels most likely traveled. We reckon that a solution employing a single type of sensor and simply counting passages reduces complexity and would be easier to understand for all stakeholders. Thus, we advise to choose solutions that are straightforward and easy to understand, rather than those that are complex and require extra effort to explain.

5.3.b Recommendation: Maintain living documentation

We recommend that the documentation about the system must be continuously updated. This documentation should be an integral part of both development and operations workflows. New features must be fully documented and publicly announced (e.g., by communicating the features via the algorithm register) before their deployment, as seen from the perspective of the public or a public representative. For example, a sensor can only be activated if it is officially listed in the sensor register. It is possible to enforce such a condition by integrating the checks into the technical flow. In this specific case, the software algorithm could read the valid sensors from the sensor register and only then process the data recorded by them. Thus, any data recorded by the sensor not included in the sensor register is ignored by construction.

We recommend maintaining two types of documentation: one for internal use and another for the public, which should be accessible through the Amsterdam online algorithm register. It is important to ensure that every new feature added to the system is accompanied by

comprehensive documentation.

5.3.c Recommendation: Monitor system performance
Carry out quality assurance checks following the deployment of the system. This involves using performance indicators to gauge the system's effectiveness. These indicators should be tied to the system's development phase and be established in accordance with standards like data protection laws. The indicators should reflect both functional objectives as well as normative standards. Functional objectives relate to the purpose of the system. Some functional objectives are already being monitored, such as the accuracy of vessel detection, which is the basis for traffic monitoring. An example of a normative standard is to count access to a database that contains personal data as an indicator that tracks adherence to privacy measures.
The performance metrics need to be actively monitored and displayed in real-time. The monitoring task should fall under the responsible operations department, which should also notify relevant stakeholders if the system's performance exceeds or falls below acceptable thresholds.

5.4 Limited awareness about Digitale Gracht of waterway users

Not all users of Amsterdam’s waterways seem to be aware of Digitale Gracht, and even if they are, they have a limited understanding of Digitale Gracht's functioning. Currently, a somewhat outdated overview of the sensors that are used and their location is provided in the Amsterdam sensor register (state of sensors in 2022). The algorithms used are described in the algorithm register on a high level (The Digitale Gracht team has stated that the descriptions will be updated in more detail before a high-risk algorithm is deployed). In addition, vessel owners are referred to a video on the municipality website mentioning the use of chips present in the vignettes for traffic monitoring upon purchase of a vignette. These resources explain the working of the system in an understandable way. But most people do not know of the existence of these resources. We believe that the municipality should do better in raising awareness about this system. Vessel owners are presented with too little information about the system. The information at the point of sensing is limited to a sticker which we believe does not provide sufficient information about the sensor and in many cases hardly legible for someone traveling by boat.

Facilitating a functional democratic discussion on smart city systems within Amsterdam's society necessitates a certain level of citizen awareness and understanding of technical systems. The absence of this information contradicts the city's aspirations for transparency in smart systems, as articulated in the Tada values (tada.city, 2017).

Apart from awareness and information about the workings (algorithm register), there is the actual data that is being collected by Digitale Gracht. Here we can distinguish between data on waterway users themselves (What did the city collect about me and my vessel?), as well as having access to the overall data on an aggregated level (in depth but aggregated historical or live crowdedness information). Currently waterway users cannot find data that was collected on them, nor get aggregated data.

Inspired by:

- *Tada principle: Open and transparent, From everyone for everyone (tada.city, 2017).*
- *VNG principles for Digital Society 2022, paragraph 4.3. (Vereniging van Nederlandse Gemeenten, 2022).*
- *Amsterdam data strategy, Data of the city, for the city, p.19 (Gemeente Amsterdam, 2021).*

5.4.a Recommendation: Establish proactive public communication

The municipality of Amsterdam should be more proactive in raising public awareness of the system's existence.

To ensure that the public is informed about and engaged in the system's operations, the signage at data collection points should be updated in accordance with the "Landelijke communicatierichtlijn overheid sensoren in de publieke ruimte". This includes a link pointing to further resources (sensor register, algorithm register). Figure 5 presents an example.

Transparency of the system is enhanced by making the collected data accessible on established touchpoints, including the sensor register and/or the algorithm register. Making aggregated data accessible to the public necessitates the development of a dedicated website, serving as a platform for the public to access both live and historical data. In addition, measures should be taken that enable individual citizens to discern who has accessed data related to them or their vessels. Privacy risks should be addressed through the abstraction of publicly available data using summarization, grouping, and perturbing techniques (Hoepman, 2022), aimed at reducing re-identification risks when integrating dashboard data with personal data, such as recorded videos.

Figure 5 - Example of communication guidelines developed in the "Landelijke communicatierichtlijn overheid sensoren in de publieke ruimte" project. More detailed information on this project can be found on responsiblesensinglab.org.

5.5 Undefined data access policy

Access to the data is not adequately guided by the role and responsibility of the person and the municipality appears to have insufficient overview over who has access to data. The access privileges are coarsely defined, which implies that people have access to data that is not required for their current role. For example, currently all users of the Digitale Gracht dashboard, including Nautisch Beheer and the Nautical policy team, have real-time access to the individual hardware numbers of private vessels recorded by the fixed RFID readers. However, we consider this information to be irrelevant to their responsibilities. Researchers have access to raw data which may not be essential for their analyses. In the past, all users of the Digitale Gracht dashboard had access to all the reports generated. The Digitale Gracht team has previously already identified adequate access control as a problem and addressed the issue by deactivating reporting features until access control is improved.

Inspired by:

- *Tada principle: Legitimate and monitored (tada.city, 2017).*

5.5.a Recommendation: Limit data access on a need-to-know basis
In the context of data access management, we advise making access permissions temporary by default and incorporating expiration dates. Users should also receive alerts signaling the imminent expiration of their access. To safeguard privacy, measures should be in place, ensuring that data analysts are not provided access to raw, non-anonymized data. The utilization of near-real-time data views is recommended only when necessary; otherwise, abstracting data is encouraged for enhanced security and efficiency. Specifically, the functionality used to direct BOAs (i.e., information driven enforcement), should make use of abstracted data to balance operational needs with privacy concerns.
While authorization is necessary for limiting the data access on a need-to-know basis, it is still necessary to decentralize the system as described in Recommendation 5.1.b so that no one party can become too powerful in the development and operation of the system.

5.5.b Recommendation: Limit dependence on the Vignette Administration
We remain somewhat uncertain about whether applications of the Digitale Gracht make use of the Vignette Administration. Generally, we recommend eliminating or, at the very least, significantly limiting the dependency of any current or future Digitale Gracht applications on the Vignette Administration for data minimization concerns. For example, if unique electronic identifiers linked to personal data are used for checking for payment of BHG, it needs to be ensured that no other application such as traffic monitoring makes use of these identifiers. This involves stringent control of access to the vignette administration database, separating it both physically and logically from other systems as well as limiting data access on a need-to-know basis, and discarding any data that is not used by any functionality. This is in line with the advice provided earlier by “Commissie Persoonsgegevens Amsterdam” (2020).

5.6 Information-driven enforcement

Using data to establish hotspots for information-driven enforcement is seen as problematic by several researchers. A fundamental objection is that people within hotspots are under more scrutiny than those outside based on factors for which they cannot be held responsible. In the case of Digitale Gracht a hotspot approach to checks for noise violations and detecting illegal passenger shipping, as well as checks for speeding or mooring violations of commercial vessels has been proposed.

We believe that an enforcement approach that is entirely driven by information gathered through a hotspot approach is undesirable from an ethical perspective. From a practical standpoint, a hotspot-based approach may be seen as favorable given the limited enforcement capacity available. However, the use of a hotspot approach can only be justified if it significantly and demonstrably increases efficiency over other approaches.

5.6.a Recommendation: Don't rely exclusively on a data driven approach for prioritizing the deployment of enforcers
Balance the hotspots-based-approach with a grid-based approach (random checks) during checks. The grid-based approach must help continuously redefine the hotspots. Thus, the hotspots are dynamic, and the locations are justified through the grid-based approach.

Further, to maintain transparency, the hotspots must be public facing, i.e., the information about areas subjected to higher scrutiny must be publicly available.

Issues and recommendations for specific objectives

5.7 Excessive data collection for traffic monitoring

The traffic overview is created predominantly through a system of RFID sensors placed at strategic locations that scan the unique hardware numbers of RFID vignettes of passing vessels. By combining data of the sensors, the likely routes that vessels have taken between sensors can be deduced.
Tracking individual vessels for the purpose of traffic monitoring can be done in accordance with the GDPR but brings a risk with it. In addition to being legally compliant, the system must also provide a perception of privacy. For example, the slow-traffic monitoring system operational in the city center (CSMA/LVMA) operated by Amsterdam V&OR (“Verkeer en Openbare Ruimte”) has chosen not to use WIFI-tracking for the traffic of pedestrians because of the political and societal sensitivities associated with tracking and its effects on privacy.

The current approach of sensing and processing the data for estimating the traffic has the following potential issues.
Firstly, although we cannot assume that the vessel owner is always present aboard the vessel (meaning that the vessel location data may not consistently qualify as personal data according to the GDPR) it seems likely that many vessels frequently do have their owners on board. Consequently, the continuous monitoring of vessel movements may be perceived as a potential infringement on privacy by both citizens and digital rights advocacy organizations.
Secondly, the data is currently processed and stored in its raw form thus making it susceptible to a security breach. In the event of a security incident, the data related to movement of individuals may be compromised. It's important to note that a security breach limited to data from vignette detections (i.e., the hardware numbers) alone does not automatically enable the identification of individuals. To achieve this, access to vignette administration is necessary, or the traffic pattern of a vignette must be distinctly traceable to a singular vessel/owner, though the latter scenario is unlikely.
Thirdly, the current traffic monitoring approach makes it possible that BOAs of Nautisch Toezicht & Handhaving might merge the database maintained by PortPay that contains personal information about the vessel owner (Vignette Administration) with the data available on the dashboard to monitor private boat owners. Combining the two databases makes it possible for the BOA to know the location and time of an individual vessel together with the personally identifiable data of the owner. We believe that Nautisch Toezicht & Handhaving does not have any intention of combining the databases at present, but the system does not currently have any inbuilt safeguards against it.

We consider collection of data related to commercial vessels to be less problematic because it is less privacy sensitive. However, there are instances when the data from the commercial

vessels could be considered as personal data (e.g., in case of one person company). In such cases, sufficient care must be exercised while collecting data from the commercial vessels. Ultimately, the decision to collect data of commercial vessels for policy purposes should be done in deliberation with the companies.

Inspired by:

- *VNG Principles for Digital Society 2022, section 7.5, data minimization (Vereniging van Nederlandse Gemeenten, 2022).*

5.7.a Recommendation: Aim for data minimization for during traffic monitoring

We recommend adopting privacy friendly approaches towards monitoring traffic in the Digitale Gracht. The type of sensing could be determined by the acceptable accuracy. We propose the following variants of the system from least to the most data-intensive:

Count-only traffic monitoring system

The principle of data minimization demands that only necessary data should be collected. We believe that it is not required to have information (RFID number & location) about individual vessels to estimate the traffic in the canals. Knowing only the count of vessels at discrete strategic locations should be sufficient. To achieve comparable accuracy, this may imply sensor deployment at more locations, however, such a strategy would enable adoption of privacy friendly sensing methods.

For example, usage of radars could be further explored. Through our interviews, we are aware that Digitale Gracht experimented the usage of radar sensors, but the study could not conclude. Radar technologies such as millimeter wave (mmWave) detect objects as a cluster of points (point clouds), thus ensuring privacy by design. These technologies have been studied for analyzing the road traffic and could work for counting vessels. Additionally, using a counting method independent of vignettes would help entirely isolate the Digitale Gracht from BHG administration, thus further avoiding function creep.

In the current systems, cameras are being used as supplementary sensors for confirming the number counted by RFID sensors. Cameras, by their nature, capture individuals' appearances, raising privacy concerns for which mitigative measures need to be implemented. This means additional work, and often a residual risk remains even after mitigation. Opting for less invasive sensing methods when they can accomplish the same objectives is preferable. This perspective resonates with the Agenda Digitale Stad which states that people should be able to navigate urban spaces without constant observation (Gemeente Amsterdam, 2019).

Manual counting could be used as a secondary means to validate the accuracy instead of cameras. Spot counts through manual checks at a few locations could be compared against those obtained through radar sensors.

Winnie Daamen, Associate Professor in the chair of Traffic Operations and Management of the Department of Transport & Planning at TU Delft, is currently performing analysis to optimize the number of locations for sensor deployment. The result of this analysis is the first step towards implementation of this suggestion.

Count and vessel category traffic monitoring system
If the usage of vignettes must be continued, only the discrete categories could be read and processed through the RFID numbers. Individual hardware numbers, either raw or anonymized, must not be recorded, processed, stored, and displayed on the dashboard. The system of retrieving categories from hardware numbers must be independent of the vignette database so that no personal information related to vignette could be retrieved.

RFID tracking traffic monitoring system
This alternative is suggested only if it is imperative to record the passage of individual vessels. In such a case the current system of reading the individual electronic identifier can continue.
However, even in this case, we recommend that the identifiers are not stored or displayed on the dashboard in its raw form. They must be pseudonymized early in the processing. Only pseudonymized data must be visible on the dashboard or made available during data processing for policy reports. Retrieving the raw electronic IDs must be allowed only in predefined situations with due approval from the data steward. Further, in case this data is accessed, the incidents must be logged with details such as who has accessed this data, when and for what purpose. This information must also be relayed to the vessel owner.

5.8 Proportionality of approach towards detection of illegal passenger rides

The city regulates commercial passenger shipping by means of a permitting process. This regulation is enforced by fining commercial passenger shipping without a permit. The fines serve the purpose of enforcing the prohibition of passenger shipping without a permit.
The enforcement practice entails BOAs identifying suspect vessels on the water, halting these vessels at the moment when they are suspect, questioning the shipper and those aboard on the situation and, in some cases, deeming the shipper to be guilty and handing out a fine.
For the identifying hotspots of suspect vessels, the current proposed approach makes use of an algorithm that identifies patterns in shipping movements that could be indicative of illegal passenger shipping. To be able to do this, all collected data of shipping movements of private vessels are processed. The data is collected by means of RFID sensors. This means that a large number of ships that do not engage in illegal shipping are being scrutinized. Critics of this approach call this dragnet surveillance. Because of the substantial infringement on the private sphere of vessel shippers, the demand of proportionality requires a grave justification. We question whether this demand is being met.
Proportionality ultimately is a judgment call and depends on the position of those making the call versus the matter at hand. It is also related to the effectiveness of the means and the availability of less invasive means. As a group of experts with a certain level of detachment from the project, we contend that the ends (identification of hotspots of passenger shipping without a permit) pursued do not warrant the employed means (tracking all vessel movements). We believe it brings limited usefulness and there are less invasive means to achieve a similar end.

There is a secondary use for the reports has been mentioned. The data could potentially serve as evidence in a potential court case about the fine between the municipality and the suspect of commercial shipping without a permit. However, the approach has not yet been validated and thus the reliability of the reporting is insufficient.

5.8.a Recommendation: Reconsider illegal passenger shipping detection approach
Instead of deploying an algorithm to identify hotspots of suspect vessels by monitoring shipping movements of all private vessels, we recommend relying on approaches that have previously been in use to detect illegal passage rides. This includes scanning the internet for advertisements for illegal passenger rides and deploying personnel to manually check for illegal passenger shipping with appropriate frequency and at locations prone to such incidents and where illegal rides may cause harm to legal providers by poaching clients. The frequency of manual checks can be adapted after evaluation.
If instead an approach relying on the unique electronic identifiers is chosen to monitor shipping movements of private vessels, access to this data should be strictly limited as described in the recommendation 5.5.a Limit data access on a need-to-know basis. BOAs should not be provided with the unique electronic identifiers of the vessels that have been flagged suspect, but only the locations where violations are suspected to take place.

5.9 Proportionality of approach towards noise monitoring

Until recently the combination of displaying the unique hardware number recorded by RFID readers and the illustration of noise events at specific measuring locations on the Digitale Gracht dashboard could have enabled dashboard users to identify individual vessels that are causing noise events. We believe this information was never used for enforcement, that is it did not influence decisions of BOAs; however we consider this to be an unnecessary privacy risk. Linking this information is not required for any application and it potentially enables BOAs, who have access to the Vignette Administration database, to link noise events to the owners of specific vessels.
In the past, an application was tested specifically to identify individual vessels causing noise pollution. This entailed recording video and audio footage of the vessel identified to cause noise pollution. Knowing the current locations of vessels causing noise pollution is however not advantageous for the enforcement process, considering the significant time required for enforcers to reach the site. Their service vessels travel at the same speed as other boats, diminishing the immediacy of response. Due to their reduced speed, Nautisch Toezicht & Handhaving vessels cannot easily verify and potentially penalize the identified vessel. For these reasons we feel that the goal does not justify the means, and the practice is not proportional. Recording audio and video footage, especially when the data is not actionable, violates the principle of data-minimization. In case of any security breach, the collection of excessive data risks the privacy of the individuals.

Inspired by:

- Agenda Digitale Stad, Amsterdammers have the right of not being spied on while moving through the public spaces, (Gemeente Amsterdam, 2019).

5.9.a Recommendation: Reconsider approach to noise monitoring via sensors to combat noise pollution

In any case, we advise to refrain from making audio recordings as we deem this to be disproportionate. Moreover, it should be made impossible (or only possible under certain predefined conditions) to link an individual vessel to a noise event. This entails not displaying noise incidents alongside unique electronic identifiers on the dashboard. To guide enforcement, we recommend adhering to the current approach of Nautisch Toezicht & Handhaving involving the monitoring of “Signalen in Amsterdam” and deploying BOAs to hotspots, without incorporating active noise monitoring sensors. If sound data is needed for policy purposes privacy-preserving sound sensors (e.g., use dB meters to measure noise at particular points.) should be used.

6. Possible follow-up projects

6.1 Privacy friendly sensing methods for traffic monitoring
In accordance with recommendation 5.7.a, we contend that the current strategy for monitoring traffic of private vessels, heavily reliant on unique electronic identifiers and route deduction, is not in line with the principle of data minimization. We propose a follow-up project which investigates an alternative traffic monitoring that embraces privacy-friendly sensing methods. Radar technologies, notably millimeter wave (mmWave), identify objects as clusters of points (point clouds), ensuring privacy by design. The follow-up project would study the feasibility of using mmWave radars for observing the traffic in the Gracht.

6.2 Sampling interval optimization - Balancing data collection with privacy
Building on the optimized sensor distribution designed by Dr. Winnie Daamen, a follow up project could explore an alternative in which sensors are not collecting data all the time but only during certain, possibly randomized moments. The project would investigate the tradeoff between accuracy of traffic data and data minimization, aiming to find a “sweet spot,” which would allow sufficient data to be collected but not excessive amounts.

6.3 Enhancing public awareness about the Digitale Gracht through signage
Our analysis concludes that the municipality should strive to make the Digitale Gracht more transparent and understandable. We suggest a follow-up project aiming to improve public awareness and level of engagement by piloting signage at data collection points in accordance with the "Landelijke communicatierichtlijn overheid sensoren in de publieke ruimte".

6.4 Building civic participation in the development of the Digitale Gracht
A follow up project focused on establishing an organization that can serve as the representative body for ongoing control of citizens (e.g., in the form of a citizen council) over the Digitale Gracht system. The project could aim to suggest who should participate, what the charter should be, and how they should function.

6.5 Monitoring system performance with regards to normative standards
Although functional objectives are currently monitored within the Digitale Gracht, there is a notable absence of active monitoring for standards based on public values. A follow up project could explore in detail how normative standards can and should be monitored and displayed in the context of the Digitale Gracht.

6.6 Towards an Amsterdam policy on hot spotting
The researchers we consulted consider the use of data to create hotspots for information-driven enforcement problematic. A hotspot approach results in a situation in which people within hotspots are under more scrutiny than those outside based on factors for which they cannot be held responsible. At the same time, we see that hotspot approaches for information driven enforcement are deployed by various governmental departments believing that it will increase enforcement efficiency. A follow up project could investigate this

tension, using the context of the Digitale Gracht as an example to explore how we should deal with this as a city/society.

References

- Alfrink, K., Keller, A. I., Kortuem, G. W., & Doorn, N. (2022). Contestable AI by Design: Towards a Framework. Minds and Machines: journal for artificial intelligence, philosophy and cognitive sciences. https://doi.org/10.1007/s11023-022-09611-z

- Bureau Telematica Binnenvaart, 2024. Convenant tussen het Ministerie van Verkeer en Waterstaat en Koninklijke Schuttevaer, Kantoor Binnenvaart, Centraal Bureau voor de Rijn- en Binnenvaart en de Vereniging van sleep- en duwbooteigenaren Rijn en IJssel. https://binnenvaart.org/wp-content/uploads/2009/08/convenant.pdf

- Commissie Persoonsgegevens Amsterdam. (2020). Advies digitale gracht 10 december 2020. https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/adviesraden/commissie-persoonsgegevens-amsterdam/adviezen-cpa-2020/advies-digitale-gracht-10-december-2020/#hae39d3ca-e06c-4fc3-8c39-8a959427bc38

- Gemeente Amsterdam. (2019). Agenda Digitale Stad. https://openresearch.amsterdam/nl/media/inline/2019/3/7/agenda_digitale_stad_versie_1_01_maart_2019.pdf

- Gemeente Amsterdam. (2021). City of Amsterdam Data Strategy. https://assets.amsterdam.nl/publish/pages/1017819/data_strategy_city_of_amsterdam_2021-2022.pdf

- Gemeente Amsterdam. (2023). Agenda Digitale Stad. https://assets.amsterdam.nl/publish/pages/964754/agenda_digitale_stad_2023_2026_wrt.pdf

- Hoepman, J.-H. (2022). Privacy design strategies. The little blue book. https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

- Hubert, B. (2020, January 20). 5G: The outsourced elephant in the room. berthub. https://berthub.eu/articles/posts/5g-elephant-in-the-room/

- Hubert, B. (Interviewee) (2022, May 22). Waarom je nerdfluisteraars nodig hebt bij de overheid [Audio Podcast]. Stuurloos. De Volkskrant. https://omny.fm/shows/stuurloos/waarom-je-nerdfluisteraars-nodig-hebt-bij-de-overh

- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. Government Information Quarterly, 37(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493

- Koops, B.-J. (2021). The concept of function creep. Law, Innovation and Technology, 13(1), 29-56. https://doi.org/10.1080/17579961.2021.1898299

- Tada.city. (2017). Het Tada Manifest. https://tada.city/

- Vereniging van Nederlandse Gemeenten. (2022). Principes voor de Digitale Samenleving. https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf

Appendix

Appendix 1: Question list

Below the question list inspired by the assessment toolkits IAMA, AIIA, DPIA and Plot4ai.This question list guided the exploration of the Digitale Gracht system and the systems deployed for the BHG payment process. Note list was only used to build an understanding of the above-mentioned systems. They were not used for the identification of issues or recommendations.

Original question(s)	Source(s)	Category	Derived question for Digitale Gracht and BHG payment process
What is the goal to be achieved with the deployment of the algorithm? What is the main goal here and what are subgoals? What is the purpose and intended outcome of the AI system? Describe the process and the (intended) processing activities and/or intended policies/regulations for which this DPIA is conducted. Give a brief description of the intended ai system (title, general description, problem statement, and domain)	IAMA, AIIA, DPIA	1. System version & Goals	**What are the goals of the system?**
	Own Question	1. System version & Goals	**What is the state of the system for which the questions are filled in? E.g. is it live, has it been prototyped, is it just an idea, etc.**
What type of algorithm will be used, or what type of algorithm will be developed? Why is this type of algorithm chosen?	IAMA	2. General description tech. system	**What type of sensors are being used in the system?**

What type of algorithm will be used, or what type of algorithm will be developed? Why is this type of algorithm chosen? Why is this type of algorithm chosen? Is there automated decision-making? If so, on what basis? Could our AI system automatically label or categorize people?	IAMA, DPIA, PLOT4ai	2. General description tech. system	**What type of processing is being used? Does the system rely on automated decision making in any way? If yes, explain. E.g. Does the system automatically label or categorize people?**
Location: where will deployment of the algorithm take place? Is it in a particular geographical area, is it with a particular group of people or files?	IAMA	2. General description tech. system	**Where is the system and its sensors deployed? How was the location chosen?**
What does the system architecture look like (how do the software components relate to each other)?	AIIA	2. General description tech. system	**What does the architecture of the system look like? I.e. what are the different components and parts and how do they relate to each other**
How can the AI system interact with other hardware or software (if applicable)?	AIIA	2. General description tech. system	**How can the system interact with other hardware or software (if applicable)? E.g. other sensors, boats, databases, etc.**
Are any specific hardware and software requirements documented?	AIIA	2. General description tech. system	**Are the hardware software requirements for the system documented? E.g. the camera must have a specific resolution for the system to work correctly.**
What type of data is going to be used as input for the algorithm, and from what sources is the data derived? Does the ai system handle personal data (does the AVG apply)? If yes, please complete the following questions also. If not, continue at 'relating to confidential data'. Indicate which (categories of) personal data are	IAMA, AIIA, DPIA	3. Data collection, Processing & Storage	**What type of data is collected as input for the system? E.g. categories of personal data, confidential data etc. For each type explain where this data comes from. E.g. sensors, databases etc.**

being processed?			
Is there any linking, enrichment or comparison of data from different sources?	DPIA	3. Data collection, Processing & Storage	**Is there any linking, enrichment or comparison of data from different sources?**
Are special personal data, criminal data and/or BSN also processed? If so, please indicate which data.	DPIA	3. Data collection, Processing & Storage	**Are special personal data, criminal data and/or BSN also processed? If so, please indicate which data.**
What are the purposes of the processing of personal data within the process?	DPIA	3. Data collection, Processing & Storage	**What are the purposes of processing personal data within the process?**
Will personal data be used for a purpose other than that for which it was collected?	DPIA	3. Data collection, Processing & Storage	**Will personal data be used for a purpose other than that for which it was collected?**
How is it ensured that the default settings of the relevant devices or applications are such that only the personal data necessary for the specific purpose is collected? Please indicate what measures have been taken.	DPIA	3. Data collection, Processing & Storage	**How is it ensured that the default settings of the relevant devices or applications are such that only the personal data necessary for the specific purpose is collected? Indicate what measures have been taken.**

Are personal data encrypted where possible?	DPIA	3. Data collection, Processing & Storage	**Is personal data encrypted where possible?**
Are personal data pseudonymised where possible?	DPIA	3. Data collection, Processing & Storage	**Are personal data pseudonymised where possible?**
Please indicate what alternatives have been considered to achieve the process in a way that is less intrusive in terms of impact on the privacy of data subjects?	DPIA	3. Data collection, Processing & Storage	**Please indicate what alternatives have been considered and which have been implemented to achieve the process in a way that is less intrusive in terms of impact on the privacy of data subjects?**
Describe the (categories of) data subjects whose personal data are being processed. Indicate whether vulnerable groups are involved.	DPIA	3. Data collection, Processing & Storage	**Describe the (categories of) data subjects whose personal data are being processed. Indicate whether vulnerable groups are involved.**
How many individuals' personal data are (approximately) processed as part of this process?	DPIA	3. Data collection, Processing & Storage	**How many individuals' personal data are (approximately) processed as part of this process? Name an amount in combination with an indication of time.**
How is personal or confidential data handled? (Consider the DPIA), How is the input(data) stored? Indicate on which data carrier the personal data is stored (hardware, software, networks)	AIIA, DPIA	3. Data collection, Processing & Storage	**How is the collected data handled /stored? Indicate also where it is stored. E.g. hardware, software, networks, etc.**

Is our data storage protected?	PLOT4ai	3. Data collection, Processing & Storage	**Is the data storage protected?**
Are we preventing Data Leakage?	PLOT4ai	3. Data collection, Processing & Storage	**What measures have been taken to prevent Data Leakage?**
Are personal data transferred to countries outside the European Union? If yes, please indicate which parties are involved and what safeguards are in place.	DPIA	3. Data collection, Processing & Storage	**Are personal data transferred to countries outside the European Union? If yes, indicate which parties are involved and what safeguards are in place.**
What is the retention period of the output(data)?, What is the retention period of the output(data)?, Have retention periods been identified? If yes, indicate what the retention periods are.	AIIA, DPIA	3. Data collection, Processing & Storage	**What is the retention period of each type of data?**
In what way is it realized that the data are actually deleted/anonymised?	DPIA	3. Data collection, Processing & Storage	**In what way is it realized that the data are actually deleted/ anonymised?**
If no retention periods are defined, are measures taken to delete the personal data nevertheless?	DPIA	3. Data collection, Processing & Storage	**If no retention periods are defined, are measures taken to delete the personal data nevertheless?**

Which internal and external responsible parties are involved in this process? Describe the division of roles within the set-up of the AI system (such as developer, client, project leader, management organizations and final manager). Which parties and individuals are involved in the development/use/maintenance of the algorithm?Who is the user of the AI system, who are the end users working with the system and which stakeholders are impacted by the AI system?	DPIA, AIIA, IAMA	4. Stakeholders, Roles & Responsibilities	**Which internal and external parties and individuals are involved in or impacted by the system? Consider the system's development, use and maintenance. What are their roles and responsibilities?**
Which people and/or groups were coordinated with when developing ai system? Have data subjects (or their representatives) been asked to give their views on the processing activities? Please indicate why yes/no. Indicate how the views of data subjects have been followed up. If this vision has not been followed up, explain why this has not been done.	AIIA, DPIA	4. Stakeholders, Roles & Responsibilities	**Which people, groups and/or organizations were coordinated with when developing the system? E.g. data subjects. How were their views followed up?**
Are we planning to use a third party AI tool?	PLOT4ai	4. Stakeholders, Roles & Responsibilities	**Are any third party tools / software used?**
If the algorithm was developed by an external party: have clear agreements been made about ownership and management of the algorithm? What are those agreements?	IAMA	4. Stakeholders, Roles & Responsibilities	**If the system or parts of it was developed by an external party: have clear agreements been made about ownership and management of the system? What are those agreements?**
Is access to the data controlled? Distinguish between input data and output data. Have all parties coming into contact with the personal data been identified?	IAMA, DPIA	4. Stakeholders, Roles & Responsibilities	**Who has access to what data? For what purpose do these individuals or groups have access to this data?**

Is access to the data controlled? Distinguish between input data and output data. Are access measures in place that allow only persons to access personal data to the extent necessary for the performance of their duties?	DPIA	4. Stakeholders, Roles & Responsibilities	**How is access to data controlled? Are access measures in place that allow only persons to access personal data to the extent necessary for the performance of their duties?**
	Own questions	4. Stakeholders, Roles & Responsibilities	**How is data, or insights derived from data, accessed? E.g. via dashboards, phone notifications etc.**
Through what procedures will decisions based on the algorithm be made?	IAMA	5. Influencing decision making procedures	**What decisions are influenced by the system? Who takes these decisions and how are these decisions influenced by the system? Feel free to mention examples.**
What role do humans play in making decisions based on the algorithm's output ('human in the loop') and how are they enabled to play that role? How is human control and supervision ensured?	IAMA, AIIA	5. Influencing decision making procedures	**What role do humans play in making decisions based on the system's output and how are they enabled to play that role?**
Will our AI system make automatic decisions without human intervention?	PLOT4ai	5. Influencing decision making procedures	**Does the system involve automatic decisions without human intervention?**
Are the personal data being used for another purpose that is not specifically defined?	DPIA	5. Influencing decision making procedures	**How is function creep avoided?**

To which individuals and groups inside and outside your own organisation is the operation of the algorithm made transparent, and how is this done? If personal data are collected directly from the data subject; what information is communicated at the time of collection? If the personal data are not collected directly from the data subject; what information is communicated at the time of collection (or at least within one month of being obtained)?	IAMA, DPIA	6. Communication & Consent	**To which individuals and groups inside and outside the Digitale Gracht is the system communicated to and its operation made transparent? For each of the individuals or groups, describe what is communicated to them as well as how and when this information is communicated.**
How are changes documented during the lifetime of the system?	AIIA	6. Communication & Consent	**How are changes during the lifetime of the system documented and communicated?**
	Own question	6. Communication & Consent	**Are the data subjects informed about who has access to their personal data?**
	Own question	6. Communication & Consent	**Are the data subjects informed about the retention periods of the sensed data?**
Is the consent given through a clear active act? If the processing activities are based on consent: is the consent freely, specifically, information-based and unambiguously given by the data subject?	DPIA	6. Communication & Consent	**Are the processing activities based on consent? If yes, describe how consent is given.**

Does the data subject have the possibility to withdraw consent at any time and without negative consequences?	DPIA	6. Communication & Consent	**Does the data subject have the possibility to withdraw consent at any time and without negative consequences?**
Are proper tools for evaluation, auditing and assurance of the algorithm provided?	IAMA	7. Scrutiny & Contestation	**What tools for evaluation, auditing and assurance of the system are provided? To whom?**
How is the output(data) tested (periodically) randomly and continuously for correctness?	AIIA	7. Scrutiny & Contestation	**How is the system or parts of it tested? What is tested? How often are these tests conducted? Who is responsible for the testing?**
How is the ai system monitored?	AIIA	7. Scrutiny & Contestation	**How is the system or its parts monitored? What is monitored? When are they monitored? Who is responsible for the monitoring?**
How is the ongoing accuracy of the system measured and ensured?	AIIA	7. Scrutiny & Contestation	**How is the ongoing accuracy of the system measured and ensured?**
In case of system failure, could users be adversely impacted?	PLOT4ai	7. Scrutiny & Contestation	**If the system is not working as intended, what plans are activated or actions taken?**

If a data subject wants to object, or file a complaint against a decision of the AI system, is it clear what steps they can take? The same applies to appeals. Do citizens have an effective possibility to lodge a complaint or object? Are mechanisms in place for end-users to make comments about the system (data, technology, target group, etc.)?	AIIA, IAMA	7. Scrutiny & Contestation	**Do citizens/stakeholders/data subjects have an effective possibility to comment or lodge a complaint or object? If so, in what way?**
Does the process take into account an effective exercise of the right to access?	DPIA	7. Scrutiny & Contestation	**Do the data subjects have the opportunity to access / review their personal data collected by the sensing systems?**
Are mechanisms in place for end-users to make comments about the system (data, technology, target group, etc.)? And how or when are these reports safeguarded (analyzed and tracked)? How is it ensured that comments from stakeholders and end-users are handled properly internally?	AIIA	7. Scrutiny & Contestation	**How is it ensured that comments, complaints or objections are handled properly internally?**
Are we protected from insider threats?	PLOT4ai	8. Known risks & Mitigation measures	**What threats with regards to this system is the Digitale Gracht team currently aware of? How is the system protected from them?**
Describe the measures proposed to mitigate the residual risk.	DPIA	8. Known risks & Mitigation measures	**Describe the measures proposed to mitigate the residual risk.**

Responsible Sensing Lab

Technologies like smart sensors can help solve urban challenges. But when collecting data, what public values are involved? The Responsible Sensing Lab explores how to integrate social values in the design of sensing systems in public space.

responsiblesensinglab.nl /responsible-sensing-lab

In partnership with

City of Amsterdam