Resolution – Privacy and Data Protection

Directing the City to advance privacy protections, steward data assets, and minimize risks from data brokers, uncontrolled sharing of personal information, and secondary data use, including Large Language Models (LLMs) for the use and development of artificial intelligence.

WHEREAS, the City of Portland has built a legacy of privacy protections through prior Council actions, including Resolution 37437 (adopted June 19, 2019) establishing Privacy and Information Protection Principles; Ordinances 190113 and 190114 (adopted September 9, 2020) prohibiting the use of face recognition technologies by City bureaus and in public accommodations; and Resolution 37608 (adopted February 1, 2023) establishing a Citywide Surveillance Technology Inventory and privacy review processes; and

WHEREAS, the City of Portland has a core value of transparency to support accountability and democracy and has adopted the Open Data Resolution 36735 (adopted 2009) and established an Open Data Policy (Ordinance 188356, adopted May 2017), which, alongside the work of the Data Governance Planning and Analysis Team, led to the Citywide Data Governance Committee coordinated by BPS; and

WHEREAS, since these policies were adopted, new generations of surveillance technologies, artificial intelligence (AI)-enabled camera networks, automated license plate reader (ALPR) systems connected to nationwide sharing platforms and interconnected "smart city" sensors embedded in traffic systems and public spaces, have expanded the scope and precision of government and commercial monitoring. These systems generate continuous streams of data, often analyzed in real time, and combine disparate data, from geolocation and license plate scans to facial recognition, enabling the creation of detailed patterns of movement, association, and identity across entire communities; and

WHEREAS, data brokers play a central role in this evolving surveillance ecosystem by aggregating and selling personal information from multiple sources, including public records and state and local data streams. Data brokers increasingly provide services to federal law enforcement agencies and other entities seeking to circumvent local privacy and Sanctuary safeguards, allowing sensitive data originally collected for municipal purposes to be repurposed for unrelated enforcement or profiling activities; and

WHEREAS, federal law enforcement agencies exploit brokered datasets and access state and national information sharing systems, creating indirect pathways to City originating data that bypass local oversight and frustrate the intent of Portland's privacy principles and Sanctuary policy; and

WHEREAS, sensitive data most at risk, including but not limited to categories defined by the Oregon Consumer Privacy Act, personally identifiable information, biometric identifiers, and geolocation or utility data, upon aggregation or deanonymization, enable comprehensive surveillance of individuals and households well beyond the original context of collection; and

WHEREAS, such risks fall disproportionately on marginalized communities, including Black, Indigenous, and other people of color; immigrants; unhoused Portlanders; people living with mental health conditions; and individuals engaged in protest or civic activity, exacerbating inequities and eroding public trust in government; and

WHEREAS, enterprise data governance enables organizations to make decisions about data and hold those that work with data accountable to data and privacy policies, including ordinances, resolutions, and City values; and

WHEREAS, effective data governance requires knowledge and experience with business needs and strategy, data collection and analysis, data management, data culture change management; and

WHEREAS, to address these emerging threats and close gaps in current protections, Council seeks to enable data minimization, strengthen contractual controls, improve data security and advance data governance maturity, while enhancing public transparency and community oversight to prevent the misuse of City originating data and reaffirm Portland's Sanctuary and privacy commitments.

NOW, THEREFORE, the City Council directs

I. City Data and Privacy Office

A. Council affirms the establishment of the City Data and Privacy Office, pursuant to City Code Chapter 3.39. Council directs the City Administrator to develop a proposal to transition staff and functions related to data governance and privacy into the City Data and Privacy Office. The proposal will describe:
    1. Office staffing (including identifying the source of any reallocated positions);
    2. A plan for short-term position loans and workload realignment to ensure the work of the resolution is commenced in line with the deadlines outlined in this resolution;
    3. A plan for long-term resourcing of both data governance and privacy work, the Chief Data Officer position description (including a background in data governance or privacy); and
    4. A discussion of ongoing support of Bureau of Technology Services data platform and data management technology projects, including budget, personnel, and purchasing.

    The written proposal shall be submitted to Council within 60 days of the passage of this resolution.

B. Upon establishment, responsibilities for data governance, privacy oversight, and the surveillance technology inventory will be consolidated within the City Data and Privacy Office, with the Office functioning as the City authority on these matters. In the course of directing these matters, the City Data and Privacy Office will continue fruitful collaborations between City data governance staff and:
    1. The Office of Equity and Human Rights to ensure appropriate consideration of equity impacts;
    2. The Bureau of Technology Services to ensure data governance needs guide information technology decisions and information technology planning supports long-term stewardship of City data assets; and
    3. The Chief Information Security Officer to ensure alignment with City-wide information governance, risk, and compliance measures.

II. Sensitive Data Inventory and Risk Mapping

The City Administrator shall ensure that the City Data and Privacy Office, in concert with the Bureau of Technology Services, the Office of Equity and Human Rights, and other appropriate entities complete the following:

A. Build on the surveillance technology inventory process codified in Resolution 37608 to develop a mapping of how sensitive City data, including geolocation, sensitive personally identifiable information (PII), and utility data, flow to state and federal systems, vendor and subcontractor networks, and data brokers. Bureaus shall promptly reply to staff requests for information in service of this work;
B. Clarify the definition of "Sensitive Data" for the City of Portland, including a comprehensive list of specific data elements and/or categories that fit into this definition;
C. Review City open data portals, traffic feeds, and livestream cameras for potential privacy risks and misuse by external actors, including government entities external to the City, in violation of City values and Sanctuary policy. In performing this work, staff will continue to weigh City interests in transparency and open data;
D. Identify where current data practices, including sharing with state and federal systems, vendor and subcontractor networks, and data brokers, enable tracking or profiling of Portlanders in ways inconsistent with City privacy and Sanctuary values, including through aggregation, resale, de-anonymization, or secondary use;
E. Identify over-collection risks (e.g., information relating to place of birth, immigration status, extended retention practices) and recommend mitigation under a Citywide Data Minimization Standard; and
F. Evaluate the adequacy of existing contractual provisions, policy protections, and technical controls in light of emerging threats, identifying gaps related to data resale and transfer, use of City data to inform predictive models, de-anonymization, and other privacy risks.

Within five months of the establishment of the City Data and Privacy Office, the Office will deliver to Council a written report which will discuss progress on Sections II.A and II.B as well as the results of the assessments of Section II.C-F. Sections II.A and II.B shall be completed within eight months of the establishment of the City Data and Privacy Office.

III. Recommendations

Using the inventory findings, the City Administrator and staff referenced in Section II shall, within eight months of submission of the written report referenced in Section II, prepare a unified set of recommendations and proposed code changes that:

A. Contractual and Technical Data Controls

1. Establish a citywide data minimization framework applied across bureaus and vendor contracts;
2. Where appropriate, and in coordination with the Bureau of Technology Services effort to develop enterprise-wide software solutions, upgrade data classification and access controls, including reclassifying certain data for heightened protection, limiting external

access contingent on enforcement of a judicial warrant, or creating separate data handling protocols for high-risk datasets;
3. Establish heightened protections in City contracts and procurement procedure to close loopholes permitting onward sale, transfer, release, or use of City data, including in aggregated form, derived datasets or models, or in broker datasets;
4. Recommend policy language and mitigation measures for data practices that enable tracking or profiling of Portlanders, including risks identified in the inventory related to state/federal systems, vendor or broker networks, open data portals, benefits programs, the criminal legal system, public transit, and camera networks (public and private);
5. Provide a preliminary feasibility analysis of licensing, disclosure, and legal enforcement mechanisms for data brokers operating in or selling data of Portland residents;
6. Prepare a framework for ongoing review and continuous improvement of Sensitive Data protections, both policy and physical cybersecurity controls, including at minimum, the data included in the definition of "Sensitive Data" in the Oregon Consumer Privacy Act; and
7. Propose a set of penalties that can be applied to vendors that have failed to comply with City data standards or that have used City data illegally.
8. Outline next steps for establishing comprehensive data sharing and data collection policies, including establishing certain minimum standards for all software and hardware applications, including global limits on LLMs and artificial intelligence as well as capability to track and document how data is used, stored, and accessed.

B. Law Enforcement Protections

1. Review PPB participation in state and national data-sharing systems (e.g., LEDS, NLETS, fusion centers, and joint task forces) to identify where Portland-originating data may be accessed or repurposed by external entities in ways inconsistent with City privacy principles or Sanctuary policy; and
2. Evaluate and recommend firewall measures within these systems to ensure Portland originating data cannot be repurposed or accessed inconsistent with City privacy and Sanctuary values. This shall include developing MOUs or equivalent agreements with state agencies, database operators, or vendors, as well as technical measures (e.g., data tagging, access controls) to restrict retention, onward transfer, and secondary use of City data and require additional transparency on external access requests.

C. Transparency, Oversight, and Community Protection

1. Ensure any bureau operating or contracting for automated license plate readers (ALPR) or other traffic enforcement systems that collect or process license plate data prepare written, publicly available annual reports on the use of ALPR. Reports shall include: total number of scans, locations of scans, number of "hits" categorized by offense type, data retention period for hits vs. "non-hits," actions taken as a result of hits (e.g., arrests, citations), any data sharing (passive or active) with external agencies or vendors, and a description of any capabilities beyond scanning (e.g., tagging, geofencing, pattern analysis) along with whether those features have been deployed.

2. Ensure any bureau engaging vendors, research partners, or data brokers to implement pilots or programs involving Sensitive Data and technology, including but not limited to, algorithmic or automated decision-making systems, whether fully autonomous, supervised, or used for decision support (e.g., dynamic pricing, eligibility screening) shall conduct a privacy review prior to deployment. This review must be led by the City and may not rely on an assessment prepared by the entity whose product is being reviewed. The review must, at a minimum, assess adherence to City privacy and data minimization principles, bias risks, and protections against onward sale, transfer, or aggregation of data. The results of the review, including risks and mitigation measures, shall be made publicly available.

3. The Office of Community Engagement, with the assistance of the Office of Equity and Human Rights and in partnership with the City Data and Privacy Office, shall direct outreach efforts to underserved communities, with particular emphasis on immigrant and refugee residents. These efforts shall include the development of multilingual materials explaining data rights and privacy protections, as well as the convening of ongoing community technology listening sessions to surface concerns regarding data collection, use, and sharing.

4. The surveillance technology inventory review codified in Resolution 37608 shall henceforth include an assessment of data leakage and secondary use risks, including the potential for data to be sold, transferred, or aggregated by vendors, subcontractors, or commercial data brokers. The assessment will also evaluate protections against emerging practices that could bypass City privacy and Sanctuary values. There shall also be periodic reassessment of new or emerging technologies that may introduce similar risks. The expanded inventory shall be integrated into the City's data governance framework and overseen by the City Data and Privacy Office once established.

This unified set of recommendations and code changes shall be made publicly available for a review and comment period prior to acceptance by Council.

IV. Applicability

The foregoing shall be construed as binding City policy pursuant to Chapter 1.07 of City of Portland Code.