

Data Governance, Privacy, and AI

By: Kate Garman Burns

MetroLab Network

Why Does Data Governance Matter

Tension: Local Governments must be transparent and comply with “sunshine laws” while upholding best practices with respect to resident privacy

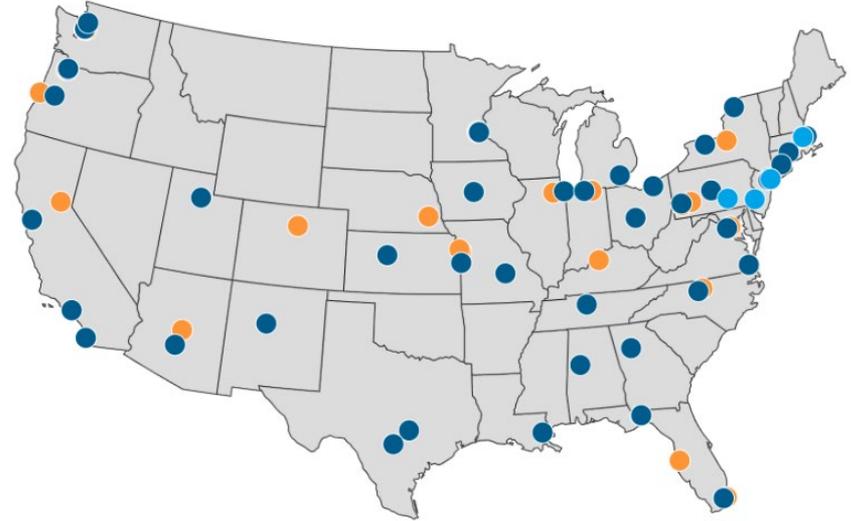
Challenges: Rapidly evolving algorithms and technology capabilities present significant challenges;

Imperative: Establish comprehensive policies and practices on data collection, storage, protection, use, dissemination, and sharing.

MetroLab: putting science in cities and counties.

Driving policy and impact by working in partnership with local governments and universities.

- Supporting an ecosystem of doers and innovators
- Scaling programs in partnership with state and federal agencies
- Developing policy with practitioners and subject matter experts



Featured Map: Our Friends of MetroLab Ecosystem

MetroLab: putting science in cities and counties.

Driving policy and impact by working in partnership with local governments and universities.

- Executive Director of MetroLab since 2022
- Technology + Innovation Policy Advisor
 - Mayor Jenny Durkan | Seattle, WA
 - Mayor Sly James | Kansas City, MO
- A Proud Jayhawk and Mom to two humans and a dog

Disclaimer: nothing in this presentation should be considered legal advice. Please consult legal counsel.



Kate Garman Burns | Executive Director

MetroLab Network: In the Lab

In the Lab Initiatives

2022-2023 Data Governance for Local Governments

2023-2024: Generative AI Policy for Local Governments



In the Lab: Data Governance Initiative

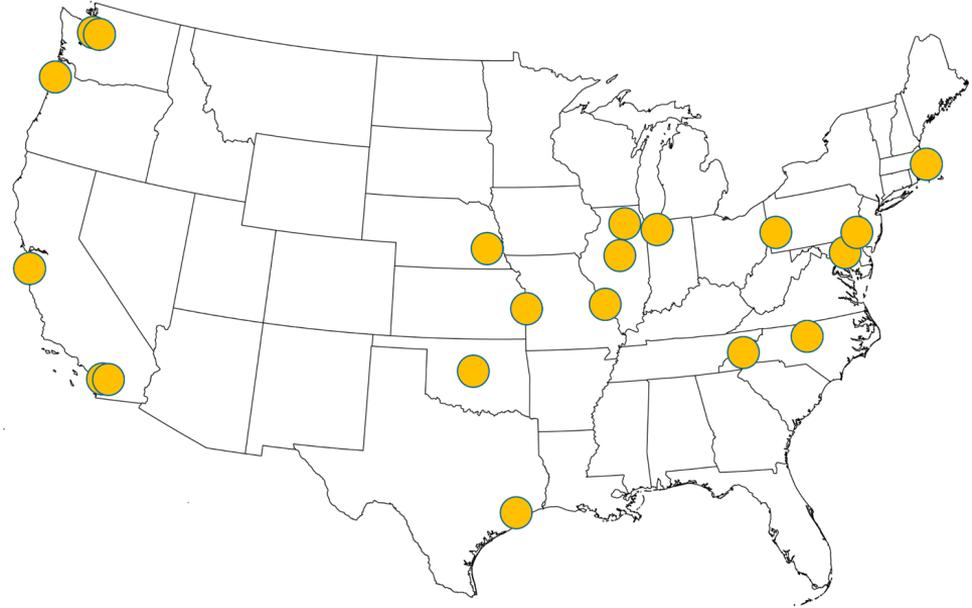
27 City Representatives

4 County Representatives

7 University Representatives

1 MPO Representative

11 Representatives from other groups like FPF



Chief Privacy Officer • Chief Data Officer - Information Technology • Manager-Data Services • Co-Founder • Project Manager, General Services-Information Technology • Executive Director • Assoc. Professor • Chief Data Officer • Managing Director • Open Data, Privacy & Surveillance Technologies Coordinator • Equity through Data and Privacy Fellow • Chief Information Officer • Chief Information Officer & Assoc. V.P. • Senior Privacy Officer • Director, Dept. of Innov. & Tech. • Digital Privacy Officer • Policy Counsel • Manager-Data & Performance • Resilience & Technology Officer • Data Governance Fellow • Assoc. Professor • Community Planner • Smart City PDX Data Services Manager • Asst. City Manager & Chief Innovation Officer • Executive Director • Digital Services Manager • Chief Data Officer, Dept. of Technology Services • Data Specialist, Dept. of Innov. & Tech. • Policy Counsel • Professor & Director-Entrepreneurship • Manager, Smart Cities PDX • IT Data Manager • Chief Information Officer • City Attorney • Chief Information Officer • Lecturer--Master/Urban Spatial Analytics • ACPP Project Mgr-Center for Analytical Approaches to Social Innov. • Chief Innovation Officer • Budget Officer • Chief Privacy Officer • Director of Civic Innovation • Director of Strategy & Technology • Director of Open Source Operations • Program Manager • Director • Vice President of U.S. Policy • Assistant City Attorney • Mayor's Deputy Chief of Staff • Asst. Professor

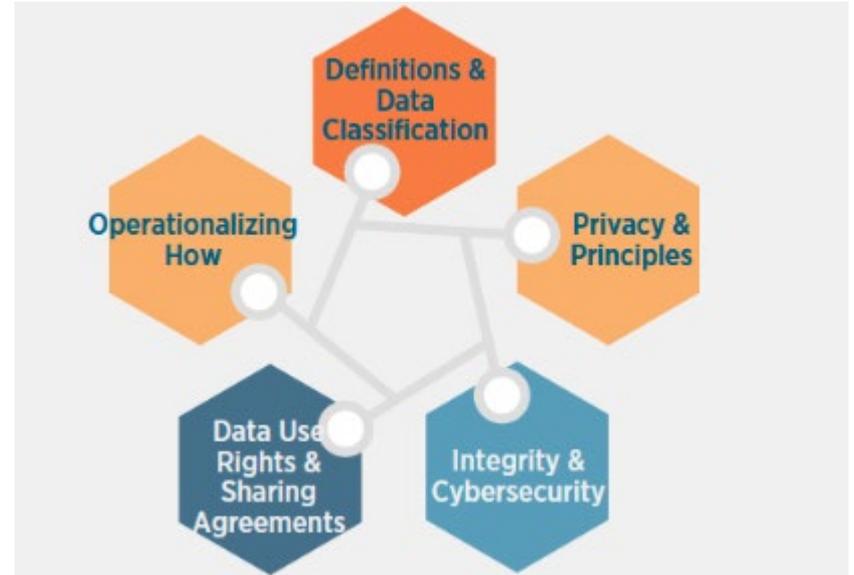
Task Force Outcomes

Model Data Governance Policy & Practice Guide

For Cities and Counties

READ →

www.metrolabnetwork.org/datagovernance



MetroLab Model Data Governance Policy & Practice Guide

Got Data?

Use whatever portions of this guide fit well with your needs and circumstances.

Scope of Work

The suggested governance approaches in this Guide are for **Data that is owned or in possession of a city or county**—this includes Data that the Jurisdiction directly collects, or Data received by a local government intentionally (i.e., the local government has contracted with a third party or is working with a third party on a project/pilot, such as a grant).

MetroLab Model Data Governance Policy & Practice Guide

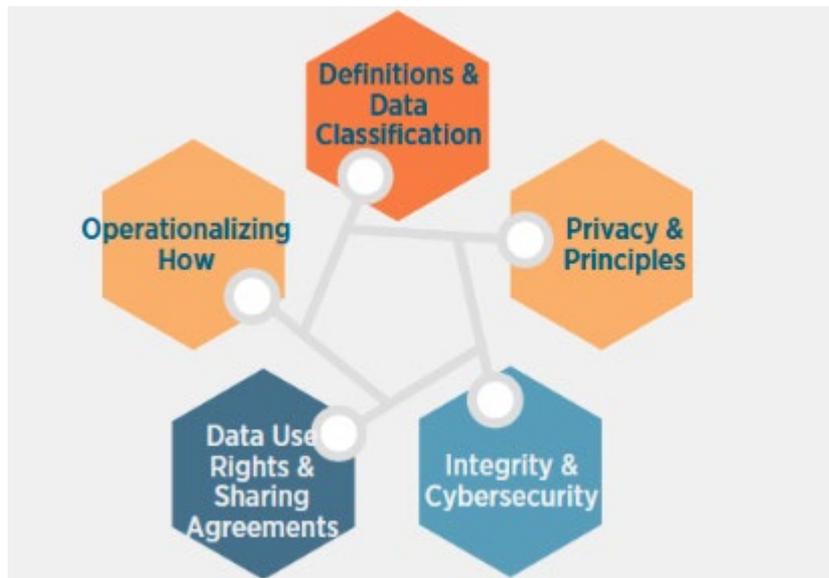
Recognizing Maturity Levels:

We recognize that cities and counties are at different levels of established processes with respect to data governance. We have included the full gamut of recommended policies. This Guide includes resources and recommendations for varied maturity levels and the website search tools will be maintained in a way designed to help users at varying stages in their data governance journeys navigate to the resources most pertinent to their needs and circumstances.

MetroLab Model Data Governance Policy & Practice Guide

Section 1: Definitions and Data Classifications

- ❖ Approximately 30 relevant definitions
- ❖ Data Classifications Recommendations and Flow Chart
- ❖ Data Classification Examples



Guide Section 2: Data Classifications

Data Sensitivity Classification



Classification 0: Open Data

Any dataset regularly published or treated as open data is considered "Level 0 - Open." Examples include public websites, reports, and job announcements. These datasets are freely accessible to the public, ensuring transparency and fostering trust within the community.

Classification 1: Public

Public data, not proactively released, or data available for public access or release, but are not subject to any restrictions under public disclosure law.

Examples:

- Health or building inspection information and organizational charts.

Guide Section 2: Data Classifications

Data Sensitivity Classification



Classification 2: Internal

Internal Governmental use refers to information that is subject to public disclosure law exemptions but is not highly sensitive. This includes operating information that is not proactively released to the public.

Examples:

- Draft memos
- Certain financial data
- License plate numbers

Guide Section 2: Data Classifications

Data Sensitivity Classification



Classification 3: Sensitive

Sensitive data is information intended for release on a need-to-know basis, often restricted by contracts, grants, or other agreement terms and conditions.

Examples:

- Sensitive security information
- Trade secrets
- Privileged information

This type of data requires stringent handling and protection protocols to prevent unauthorized access and ensure compliance with legal and contractual obligations.

Guide Section 2: Data Classifications

Data Sensitivity Classification



Classification 4: Protected

Protected data refers to information that, if compromised, triggers a requirement for notification to affected parties or public authorities of a security breach.

Examples:

- Social security numbers
- Driver's license numbers
- Federal tax information.

The handling of protected data necessitates rigorous security protocols to prevent unauthorized access, theft, or exposure. Organizations must implement advanced encryption techniques, regular security audits, and comprehensive incident response plans to safeguard this information.

Guide Section 2: Data Classifications

Data Sensitivity Classification



Classification 5: Restricted

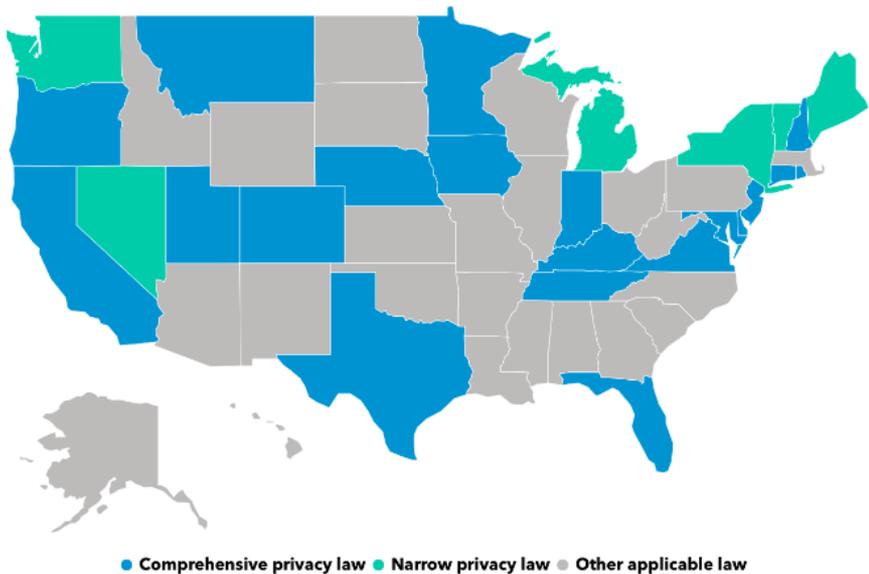
Restricted data poses direct threats to human life or could lead to catastrophic loss of major assets and critical infrastructure if compromised.

Examples:

- Emergency response information
- Data obtained from the federal government
- Infrastructure information

Consumer Privacy Laws – State by State

— U.S. states with consumer data privacy laws



Source: *Bloomberg Law*

Key Policy Considerations:

1. Threshold of customers or revenue to trigger compliance by private companies
2. Right to know what's been collected
3. Right to correct
4. Right to opt-out for purposes of a sale of information, targeted advertising, profiling
5. Right to be forgotten
6. Private Right of Action

Consumer Privacy Laws – State by State

Other key terms that these bills consider:

“**Pseudonymous data:**” means personal information that cannot be attributed to a specific individual without the use of additional information, so long as the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable individual.

“**De-identified data:**” means data that cannot reasonably be linked to an identified or identifiable individual, or any device linked to such natural person.

Source: Georgia Bill SB473 [not enacted]

Consumer Privacy Laws – State by State

Delaware

Delaware became the 12th state to join the comprehensive privacy law race, giving consumers more control over how their data is processed and stored. Effective Jan. 1, 2025, the Delaware Personal Data Privacy Act has stronger privacy rights for consumers, such as heightening protections for children's data, broadening definitions of sensitive data, and being able to opt out of the processing of personal data for targeted advertising purposes.

Source: *Bloomberg Law*

Consumer Privacy Laws – State by State

Florida

While Florida adopted many of the same provisions as other states' comprehensive privacy laws, there is reasonable debate as to whether it is truly "comprehensive" in scope. The Sunshine State tackles issues related to tech platforms, like addressing alleged censorship of conservative viewpoints. The law requires search engines, such as Google, to disclose if they prioritize results based on political ideology and prohibits government-mandated content moderation on social media.

Florida's law only regulates companies that make more than \$1 billion in gross annual revenues and derive more than half their revenue from online ads. Most provisions will go into effect July 1, 2024.

Source: [Bloomberg Law](#)

Consumer Privacy Laws – State by State

Iowa

The sixth state to sign comprehensive data protections into law, the Iowa Consumer Data Protection Act (ICDPA), is considered one of the most business-friendly so far, which privacy advocates say results in weaker data protections. Slated to go in effect Jan. 1, 2025, Iowa's law does not grant consumers the right to delete or correct data collected by third parties.

Source: *Bloomberg Law*

Consumer Privacy Laws – State of Georgia

Georgia Consumer Privacy Protection Act (SB 473) [2024]

Status: passed a vote of the full Senate, didn't leave committee in the House.

Threshold: Entities that conduct business in Georgia that exceed \$25M in revenue AND:

EITHER 1) control/process person personal information of at least 25,000 Georgia residents and derive more than 50% of gross revenue from sale of information OR 2) control or process information of at least 175,000 Georgia residents.

It does NOT apply to (among others):

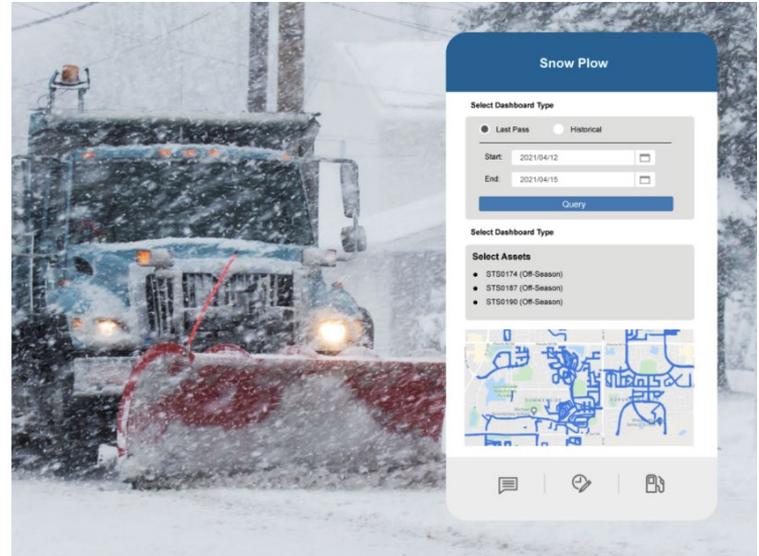
1. Research conducted in accordance by the protection of human subjects requirements
2. Non-profit organizations
3. State, judicial branch, legislative branch, or any local government
4. Any institution of higher education that does not engage in the sale of personal information

Why Should I Still Pay Attention to you, Kate?

The power of shifting expectations.



Source: Britannica



Consumer Privacy Laws – State of Georgia SB 473

Creates rights for consumers, including:

- The right to confirm whether a controller is processing a consumer's personal information;
- The right to access said personal information;
- The right to correct inaccurate personal information;
- The right to delete personal information;
- The right to data portability; and
- The right to opt-out of the processing of personal information for purposes of sale of personal information, targeted advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Source: [WilmerHale](#)

Consumer Privacy Laws – State of Georgia SB 473

- Does not create a private right of action; rather, grants exclusive enforcement authority to the Georgia AG.
- Requires that the AG provide entities with a 60-day cure period before initiating an enforcement action.
- State AG may seek civil penalties of up to \$7,500 per violation, with treble damages available for knowing or willful violations.
- Creates an affirmative defense for entities that comply with a privacy policy that conforms to the NIST privacy framework (“A Tool for Improving Privacy through Enterprise Risk Management Version 1.0”) or an equivalent framework.

Source: [WilmerHale](#)

The Evolution of Personally Identifiable Information

California Consumer Privacy Act

Personal information includes:

- Name or nickname
- Email address
- Purchase history
- Browsing history
- Location data
- Employment data
- IP address
- Profiles businesses create about you, including pseudonymous profiles (“user1234”)
- Sensitive personal information

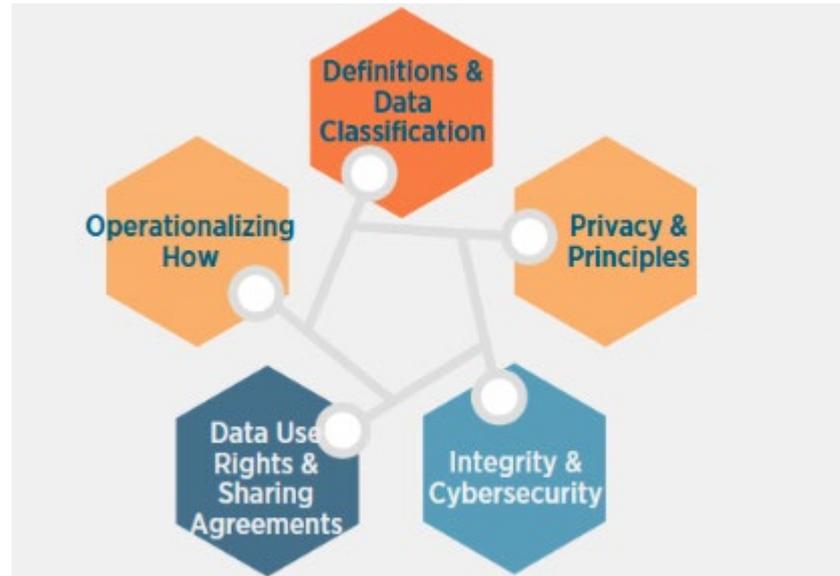
Sensitive personal information includes:

- Social security or passport number, driver’s license, or state ID
- Financial account credentials
- A consumer’s precise geolocation
- Racial or ethnic origin, citizen or immigration status, religious or philosophical beliefs, or union membership
- Contents of messages (e.g., emails, texts, chats), unless it’s directed to the business
- Genetic data
- Biometrics, like facial recognition
- Information concerning your health, sex life, or sexual orientation

CA Civ Code § 1798.192 (2023)

MetroLab Model Data Governance Policy & Practice Guide

Section 2: Privacy Policies and Resolutions



Privacy Resolutions

Privacy principles are a way to establish a commitment to privacy values that will provide guidance and parameters as a local government moves forward in developing its privacy practices. Use these central themes as a guiding list to consider and employ best practices for community engagement.

- **Minimal and intentional collection of Data:** the best form of Data protection is at the onset.
- **Transparency and notice:** when possible, describe for what purpose the Data is being collected. [23]
- **Equity:** consider the collection of key demographic data and the relationship to race and social justice efforts.
- **Ethical and non-discriminatory use of Data:** Data is used only for its intended and described purpose.
- **Data openness:** maintaining transparency on the type of data collected and when appropriate, publishing on open Data.
- **Cyber security:** ensure the protection of Data.
- **Contracting with outside parties:** consider privacy protections and transparency requirements for third parties.
- **Ongoing accountability:** put measures into place that allow for regular accountability.

Privacy Impact Assessments

- Learning from the City of Seattle, the City defines a PIA as “a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project.
- Why is this important?
 - A Privacy Impact Assessment is another way build a privacy review into IT processes to protect resident privacy

Privacy Impact Assessments



A Privacy Impact Assessment (PIA) is used to review and document the privacy implications of a program or project by collecting detailed information on data collection, use, sharing, security, and access controls. The City of Seattle publishes all PIAs for public access to ensure transparency.

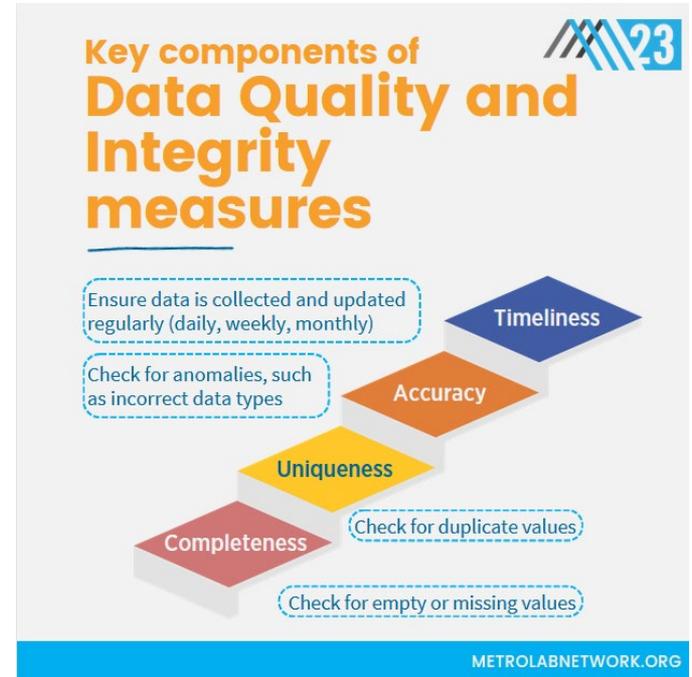
Privacy Impact Assessments

- Purpose and benefits of the technology
- Users of the technology
- Legal standards and conditions
- Data collection details
- Measures to minimize improper data collection
- Data access and storage
- Data retention policy
- Audit processes for compliance
- Accuracy checks on collected information
- Privacy training for users

Key components of a privacy impact assessment.

Guide Section 3: Data Integrity and Protection – What and Why

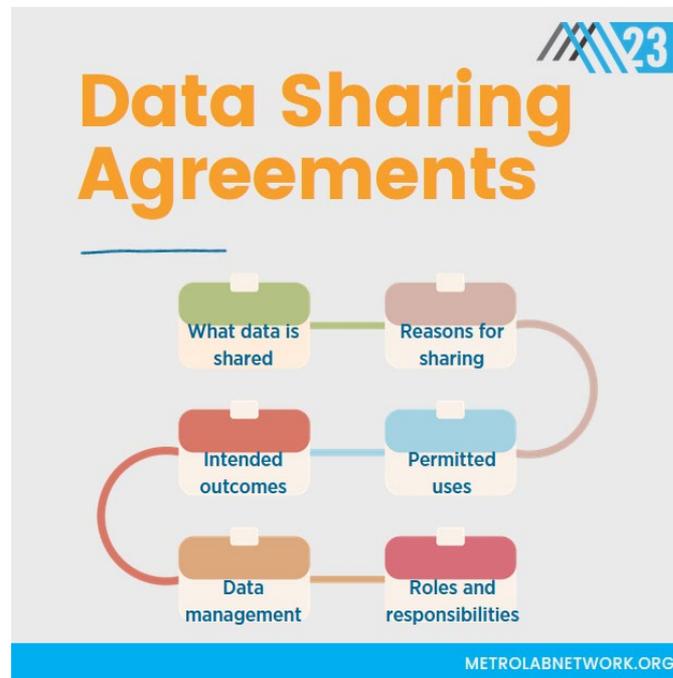
- What do we mean when we say “Data Quality and Security measures”?
 - A Data quality check includes assessment of Data accuracy, validity, timeliness, and completeness.
 - A “Data Security Policy” for establishes and communicates Data security requirements across all jurisdictions, departments, and agencies
- Why is this important?
 - “Data Quality” is critical to avoid garbage in garbage out. A Data quality check includes assessment of Data accuracy, validity, timeliness, and completeness.
 - A Data Security Policy establishes clear, organization-wide guidelines for Data Security and Data Handling



Guide Section 4: Data Sharing Agreements – What and Why

Data Sharing Agreements (DSAs) are formal arrangements that outline the terms for data exchange between parties.

- Purpose of the data sharing
- The entities involved
- The type of data shared, and the authorized uses
- Privacy and security measures to protect the data, legal compliance requirements, and how the data will be handled and stored.



Coverage of Asheville, Technology Procurement Governance Checklist

- Data Ownership & Rights
- Data Privacy
- Confidentiality
- Data Center Security (SaaS)
- PCI Compliance
- Exit strategy (avoid lock-in)
- Data Standards
- Accessibility
- Software Usability
- Open, Published APIs
- Financial Integration
- Other Data Integration Needs
- Public Record Law
- Data backup and disaster recovery
- Service Level Agreement
- On-Premise infrastructure requirements
- Access needed to on-premise infrastructure to our network
- Webforms
- Equity and Digital Inclusion
- Portfolio Alignment or Duplication
- Administrative Rights

Guide Section 5: Operationalizing & Community Engagement

- The purpose of community engagement is to involve community members in decision-making processes and activities that affect them.
- It aims to foster inclusivity by ensuring that diverse voices and perspectives are heard and considered.
- It also aims to build trust and transparency by establishing open communication channels between communities and organizations.



In the Lab: GenAI for Local Governments

Local Governments

Arapahoe County, CO
 Borough of Prospect Park, NJ
 City of Asheville, NC
 City of Boston, MA
 City of Chicago, IL
 City of Detroit, MI
 City of Fontana, CA
 City of Fort Worth, TX
 City of Glendale, CA
 City of Kirkland, WA
 City of Raleigh, NC
 City of Rochester, NY
 City of San José, CA
 City of Seattle, WA
 City of South Bend, IN
 City of Syracuse, NY
 City of Tempe, AZ
 City of Williamsport, PA
 Harris County, TX
 Harris County Flood Control District
 Lane County, OR
 Metropolitan Area Planning Council (MAPC)
 Southeastern Pennsylvania Transportation Authority (SEPTA)
 Town of Normal, IL

Universities

Carnegie Mellon University
 Iowa State University Extension & Outreach
 Syracuse University
 University of Michigan- Ann Arbor
 University of Missouri Kansas City School of Law
 University of Notre Dame
 University of Oregon
 University of Washington Information School
 Washington State University

GenAI for Local Governments Task Force by Numbers



45+ local govt's



15+ universities



20+ private sector



15+ other agencies

Subcommittees

Community Engagement

**Open Data + 311
Transportation Safety**

Public Safety + Policing

Intergovernmental Regulations

Permitting + Optimizing Services

Transportation +

Cybersecurity + Privacy

What We've Heard So Far

What is preventing me from using a GenAI use case?

1. Local governments are hesitant to use GenAI without proper policies in place first
2. Privacy concerns
3. Lack of diverse vendors
4. Technology capabilities and lack of common definitions
5. Staff Capacity and expertise

Team



Prof. Xiaofan Liang

Urban and Regional
Planning Assistant
Professor, University of
Michigan - Ann Arbor

www.xiaofanliang.com;
xfliang@umich.edu



Eman Mozaffar

M.S. in Data Science,
University of Michigan -
Ann Arbor

mozaffar@umich.edu



Arjun Suri

B.S. in Urban
Technology,
University of Michigan -
Ann Arbor

arsuri@umich.edu

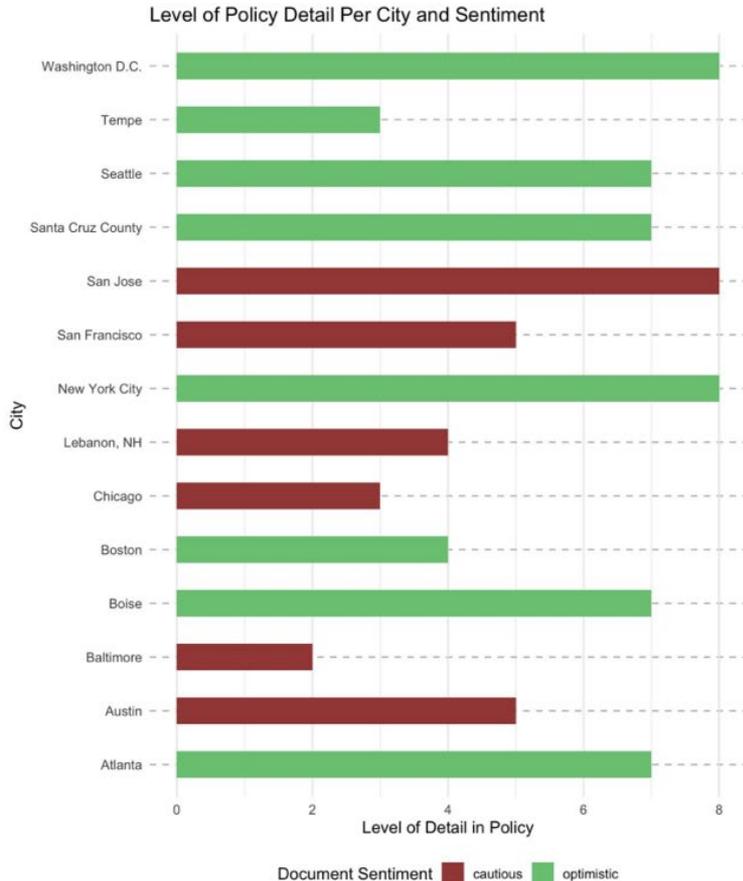
Policy Map Creation



Level of Policy Detail Per City and Sentiment

Takeaways

- Trends in detail versus optimism?
- Plans/announcements vs implementation
- Room for evolution in policy
- Political affiliations? Is AI a bipartisan issue?



Common Themes Across City/County AI/GenAI Guidelines

1. **Verify AI-Generated Content:** Rigorously fact-check all AI outputs, especially for public use or decision-making. Ensure accuracy, proper attribution, and respect for intellectual property.
2. **Ensure Fairness:** Screen content for unintended bias, offensive material, or potentially harmful elements.
3. **Promote Transparency:** Disclose AI use to build trust. Provide public documentation on AI systems, enabling stakeholders to understand and scrutinize decision-making processes.
4. **Maintain Accountability:** Implement ongoing monitoring, evaluation, and auditing to uphold ethical standards.
5. **Protect Privacy:** Safeguard sensitive information. Never include personal or confidential data in AI prompts.

Georgia AI Legislation: SB37

Requires action from Government Entities:

'Governmental entity' means any department, agency, board, bureau, commission, authority, county, municipal corporation, school system, or other political subdivision of this state.

Establishes an AI Board

The board shall advise governmental entities through the publication of model comprehensive artificial intelligence system usage plans.

GEORGIA RECORDER

Georgia Recorder

GOVERNMENT/POLITICS ENERGY/ENVIRONMENT EDUCATION HEALTH CRIMINAL JUSTICE CIVIL RIGHTS

CULTURE & SOCIETY

GOVERNMENT & POLITICS

Bill to help guide Georgia's AI growth stalled after GOP U.S. Rep. McCormick raises concerns

BY: ROSS WILLIAMS - FEBRUARY 26, 2025 7:23 PM



Georgia AI Legislation

Each governmental entity shall be required to publish by December 31, 2026, on a public website, and thereafter maintain, a comprehensive artificial intelligence system usage plan, which shall, at a minimum, include the following:

- Specific goals and objectives for AI system deployment, including the **benefits** the governmental entity aims to achieve;
- Steps taken by the governmental entity to **avoid bias** and ensure fairness across diverse user groups;
- **Data privacy measures** implemented in the use of AI systems, including data storage and collection protocols;
- Roles and responsibilities for AI system governance within the governmental entity;
- Details of compliance with relevant laws;
- The role of **human oversight** in AI system processes;
- Training programs for employees of such governmental entity on the **safe and ethical use** of AI systems;
- Protocols for **incident response** in case of AI system malfunctions, biases, or breaches; and
- Reporting procedures for AI system related incidents to affected authorities and parties.

Moving Forward

As of February 28, 2025, state legislatures across the United States have introduced at least 127 bills related to artificial intelligence (AI) regulation. This legislative activity reflects a growing trend, anticipates that the number of AI-related bills in 2025 will surpass the nearly 700 bills introduced in 2024.

These bills address various aspects of AI, including consumer protection, employment practices, data privacy, and the establishment of oversight bodies. For instance, Virginia's HB2094 proposes requirements for the development and use of high-risk AI systems, introducing civil penalties for noncompliance. Similarly, New York's AB 768 aims to enact the "New York Artificial Intelligence Consumer Protection Act," preventing the use of AI algorithms to discriminate against protected classes.

Sources: [LexisNexis](#) and [NatLawReview](#)

Lessons Learned from Emerging Technology



GenAI Optimism is
+100% vs Last Year



60% responses from
Govt. Agencies

- Consistently, there is a concern about privacy
- There is worry about bad actors
- There is worry about reliability
- Push for AI education for residents to empower them

Research Questions from Local Governments

Establishing and Sustaining Trust in AI-Optimized Services Provided by Local Government

- What are potential pillars to a comprehensive measurement framework (from the outset) to gauge both the effectiveness and potential harm of AI solutions?
- What are the potential impacts on the local government workforce? What are key indicators that can help track workforce needs for training effectiveness?

Enhancing Open Data and 311 Operations

- What existing case studies or examples focus on the assessment process of AI systems for accuracy, and what diverse approaches have groups or individuals employed?
- In the context of 311 systems, how might residents potentially abuse the system to manipulate AI functionality?
- Could AI inadvertently generate or hallucinate false problem areas in a city based on inaccurate interpretation of 311 data? What are the potential implications of such an issue on a city's operations?

Research Questions from Local Governments

Revolutionizing Community Engagement with GenAI

- How is the general public presently leveraging GenAI technology? Any specific references to engaging the government would be helpful.
- What are the common community concerns about general use of GenAI, pertaining to safety, reliability, quality of output or other factors?

Addressing Cybersecurity and Privacy Concerns

- What scenarios surround the various risks posed by GenAI with respect to cybersecurity, both in the near-term and long-term?
- How do local governments inadvertently introduce vulnerabilities through their own utilization of AI?

