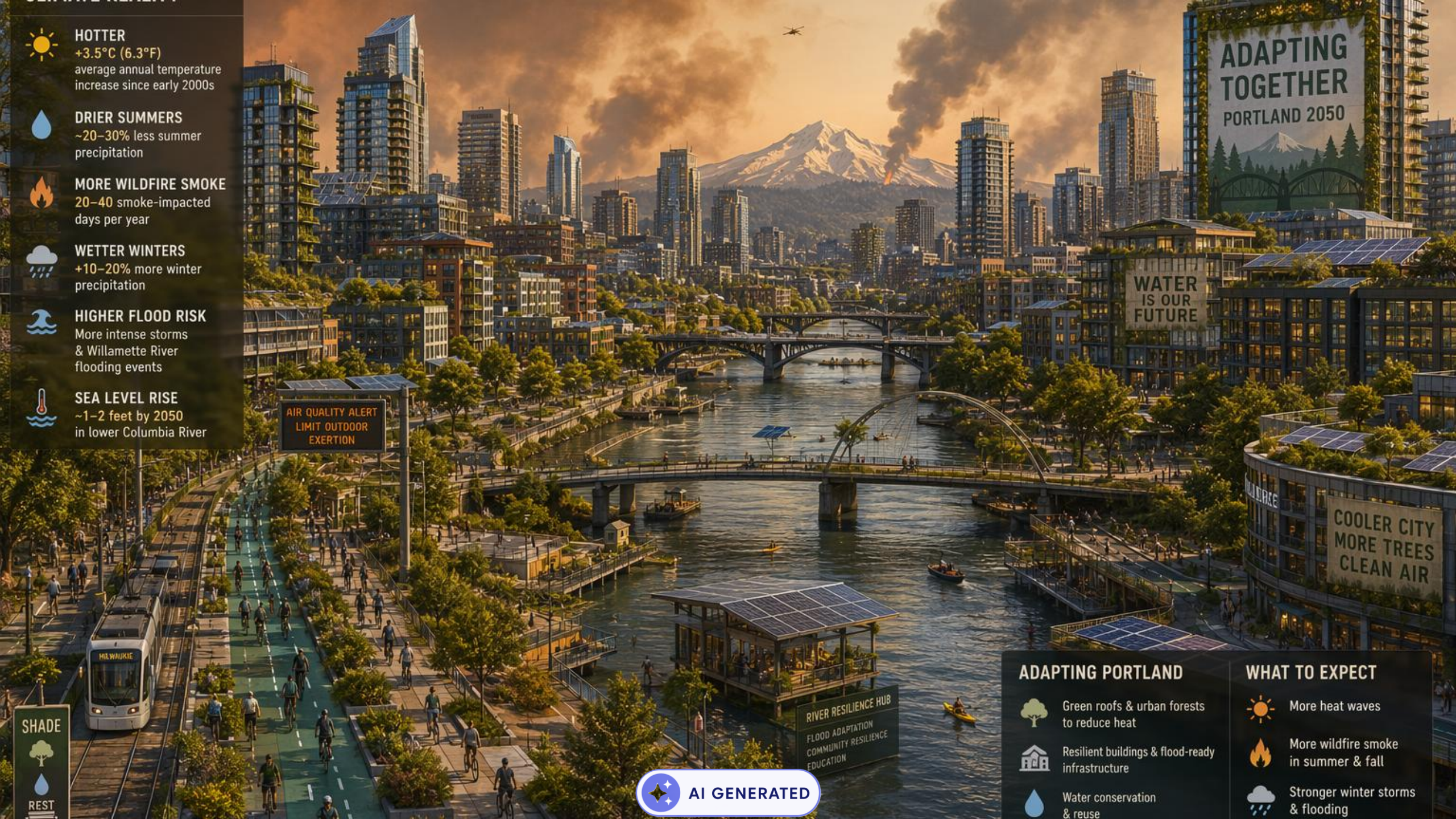

2026 DATA EQUITY SUMMIT
OUR DATA. OUR RIGHTS. OUR FUTURE.
Data Governance for a Just and Equitable Future
DATA SHOULD SERVE PEOPLE NOT POWER
Portland Oregon
OLD TOWN
DATA GOVERNANCE PRINCIPLES
PRIVACY BY DESIGN
SECURITY & ACCOUNTABILITY
COMMUNITY OWNERSHIP
TRANSPARENCY & TRUST
FAIRNESS & INCLUSION
People-centered. Community-driven. Equity-focused.
DIGITAL RIGHTS
CIVIL LIBERTIES
DATA JUSTICE
DIGITAL EQUITY
PRIVACY IS A HUMAN RIGHT
CLOSING THE DIGITAL DIVIDE
OUR DATA OUR DECISIONS
CO-CREATE
CO-GOVERN
SHARED BENEFIT
TECHNOLOGY
AI GENERATED


OLD TOWN
FUTURE
FOCUSED
PORTLAND
2050
GREENER
KINDER
TOGETHER
PORTLAND
AI GENERATED


HOTTER
+3.5°C (6.3°F)
average annual temperature increase since early 2000s
DRIER SUMMERS
~20–30% less summer precipitation
MORE WILDFIRE SMOKE
20–40 smoke-impacted days per year
WETTER WINTERS
+10–20% more winter precipitation
HIGHER FLOOD RISK
More intense storms & Willamette River flooding events
SEA LEVEL RISE
~1–2 feet by 2050 in lower Columbia River
ADAPTING TOGETHER
PORTLAND 2050
WATER IS OUR FUTURE
AIR QUALITY ALERT
LIMIT OUTDOOR EXERTION
COOLER CITY
MORE TREES
CLEAN AIR
RIVER RESILIENCE HUB
FLOOD ADAPTATION
COMMUNITY RESILIENCE
EDUCATION
SHADE
REST
AI GENERATED
ADAPTING PORTLAND
Green roofs & urban forests to reduce heat
Resilient buildings & flood-ready infrastructure
Water conservation & reuse
WHAT TO EXPECT
More heat waves
More wildfire smoke in summer & fall
Stronger winter storms & flooding

Equitable data governance through privacy and information protection.

Lessons Learned from the City of Portland's Privacy and Open Data Programs

Embedding Data Equity into Data Governance

Hector Dominguez
Privacy and Surveillance Technologies Lead
Data and Privacy Office
City of Portland



Storytelling

Privacy: People's Data

Surveillance Data

People-Centered Data Governance

Example: Automation Bias

Future – AI and Digital Sovereignty

PRIVACY IS A FUNDAMENTAL HUMAN RIGHT

My life. My information.
My right.



UNIVERSAL DECLARATION
OF HUMAN RIGHTS
ARTICLE 12

No one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honour and reputation.

AI GENERATED

Your Information. Your Life. Our Responsibility.



Restricted Cont

AI GENERATED

Find people

Predict people

Sorted by Most relevant

Megan Lee
33, United States

Zach Taylor
29, United States

Priya Sharma
31, India

Carlos Rivera
28, Spain

Aisha Khan
26, United Kingdom

Daniel Park
30, Canada

Emma Johnson
27, Australia

This is Megan's digital footprint
It is created by her online activity across the internet.

Personal Profile
(What she shares)



Megan Lee
33, Female
United States
Seattle, WA

Megan is a 33-year-old administrative services professional living in Seattle. She enjoys reading about human rights, health and wellness, traveling, and trying new foods. In her free time, she practices yoga and volunteers in her community.

Job	Administrative Services
Education	Bachelor's degree
Relationship Status	Married
Lives in	Seattle, Washington, US
Birthday	April 12, 1991

This is information Megan chooses to share about herself.

Digital Identity
(How she presents herself)

Social Media Bio (example)



Megan Lee
@meganlee
Passionate about social justice, health, and lifelong learning. Seattle | Coffee lover | Yoga enthusiast ☕🧘

Interests & Topics She Follows

Human Rights | Health & Wellness | Sustainability | Education | Travel | Yoga

Content She Shares

- Photos from hikes and travels
- Posts about equality and justice
- Book recommendations
- Yoga tips and mindfulness

Online Presence

@meganlee
linkedin.com/in/meganlee
@megan_lee
Megan Lee

This is Megan's digital identity—how she chooses to present herself online.

Digital Footprint
(What her actions leave behind)

Recent Online Activity (examples)

- Searched: "best vegan restaurants in Seattle" — Today, 10:15 AM
- Visited: Patagonia.com — May 8, 8:22 PM
- Watched: "Climate change explained" — May 6, 7:45 PM
- Liked a post about racial equality — May 6, 6:30 PM
- Checked in: Volunteer event at food bank — May 5, 11:02 AM

Activity Over Time (examples)

- Uses cookies on news websites
- Opened email from a travel newsletter
- Uses fitness app 4 times a week
- Backed up photos to cloud storage

This is Megan's digital footprint—the data and traces left behind by her online actions, often without her intention.

In short: **Personal Profile** is what Megan shares. **Digital Identity** is how she presents herself. **Digital Footprint** is what the internet records about her based on her actions.

AI GENERATED

Digital Identity, Profile, and Footprint

Portland's Privacy and Information Protection Principles



These principles guide how the City of Portland manages information and uses data and technology, including artificial intelligence, to serve the public.

Transparency and accountability

We are open about how we collect, use, and share data and are accountable for our practices.

Data openness

We make data open and accessible to drive innovation, transparency, and better public outcomes.

Equitable data management

We use data in ways that advance equity and do not reinforce bias or discrimination.

Automated decision systems

We design and use automated systems responsibly, with human oversight and clear safeguards.

Full lifecycle stewardship

We manage data responsibly from collection to deletion.

Data utility

We use data and technology to improve services, inform decisions, and create value for the public.

Ethical and non-discriminatory use of data

We respect privacy and human rights and use data in ways that are fair, lawful, and respectful of all people.

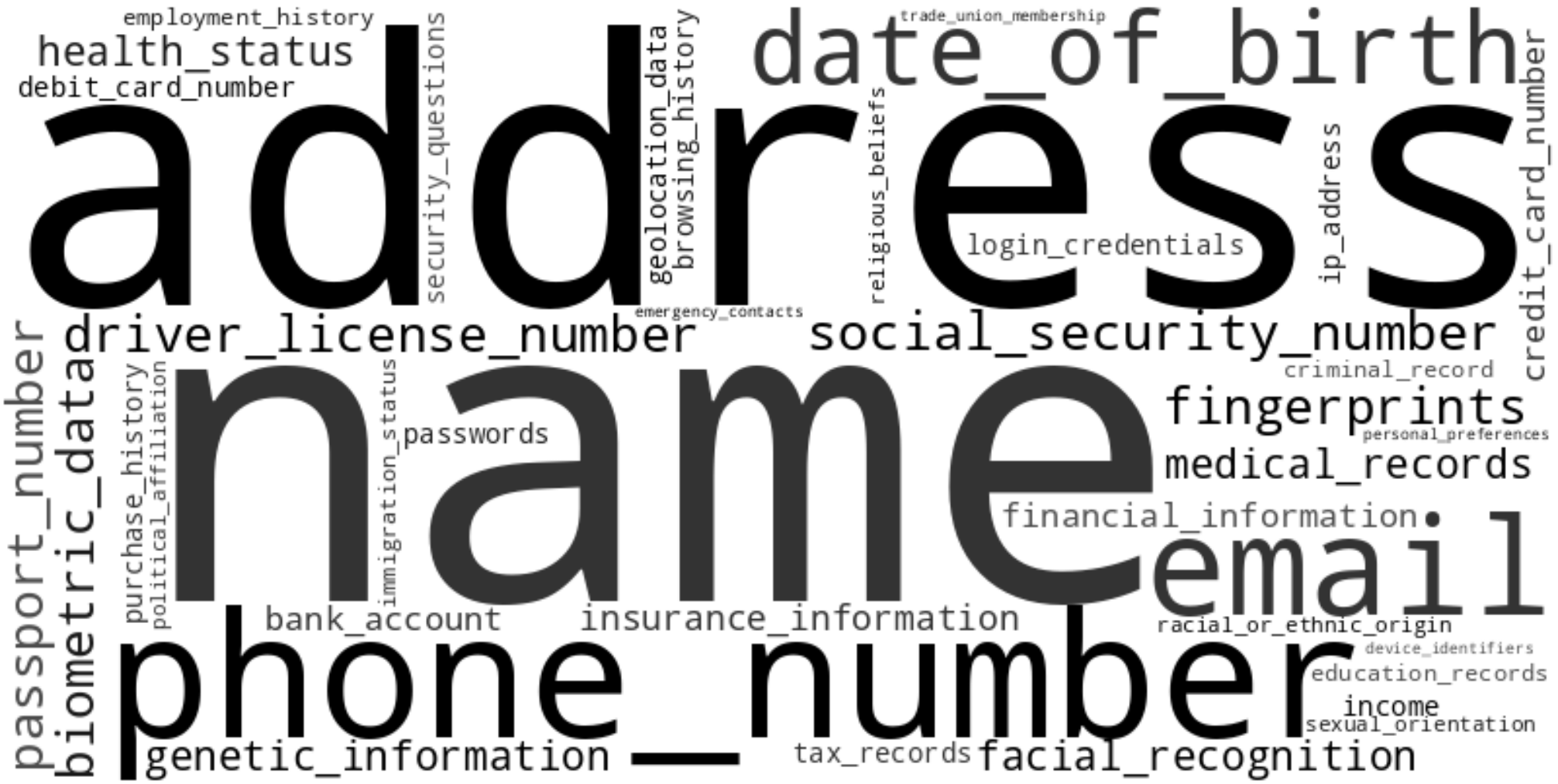


AI ASSISTED

Building trust. Protecting privacy. **Better data for a better Portland.**

CITY OF PORTLAND

Personal and sensitive information



How to Identify Personal Sensitive Information

1. 
Information that can uniquely identify a person
(full name, Social Security number, driver's license number, passport number)

2. 
Contact details tied to a specific individual
(home address, personal phone number, personal email address)

3. 
Financial information
(bank account numbers, credit card numbers, tax returns, income)

4. 
Health or medical information
(medical records, diagnoses, prescriptions)

5. 
Biometric identifiers
(fingerprints, facial scans, retinal scans, voiceprints, mental state)

6. 
Location data that tracks a person's movements
(GPS logs, travel history, check in data)

7. 
Labor and Education history
(employer history, union membership, salary information, schooling history, grades)

8. 
Authentication and device credentials
(passwords, PINs, security questions and answers, IP addresses, Device ID numbers)

9. 
Highly sensitive demographic data
(race, religion, sexual orientation, political affiliation when tied to an identifiable person)

10. 
Political, religious, and cultural affiliations and preferences
(voting history, church, temple, mosque, or spaces of worship)

11. 
Immigration and citizenship status

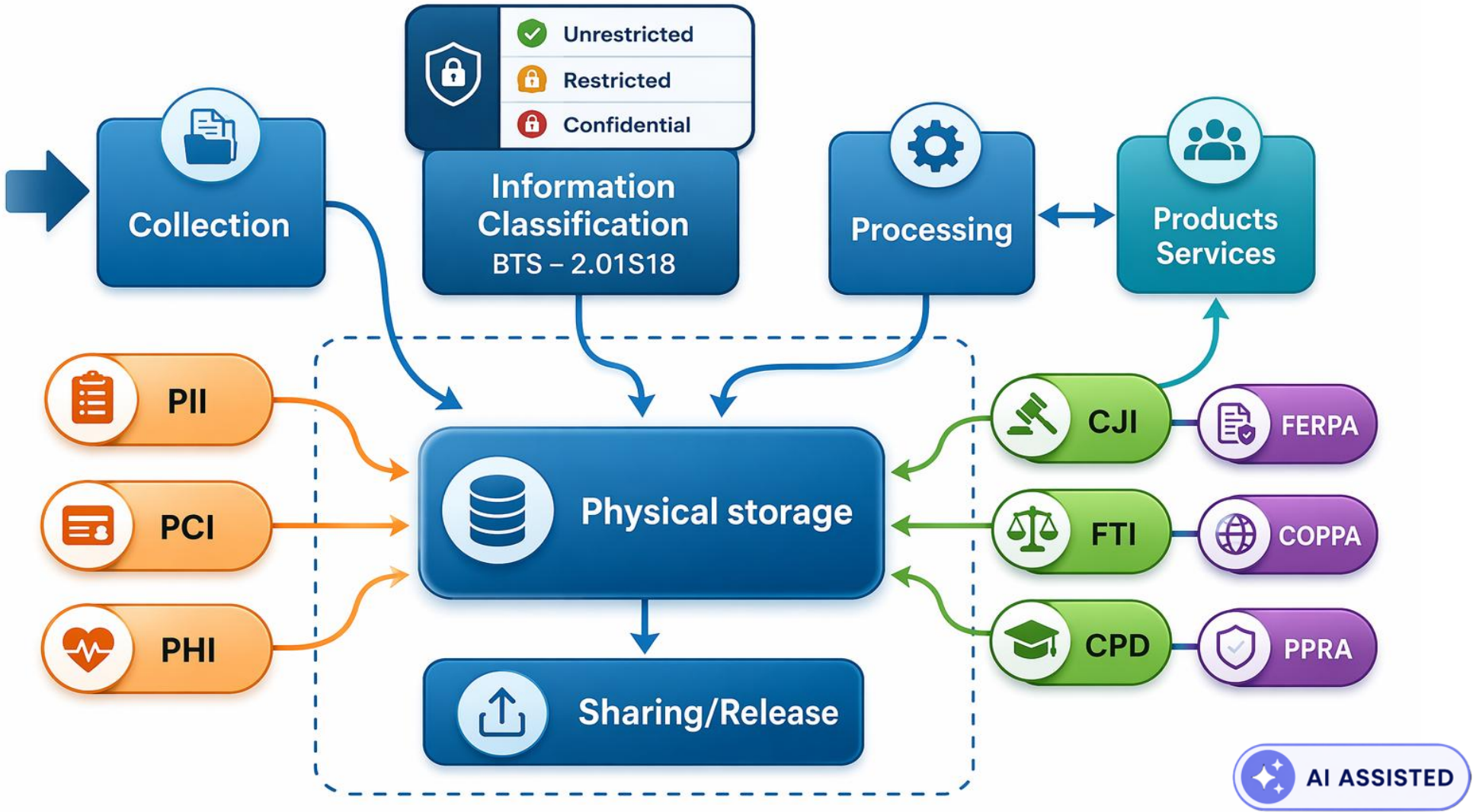
12. 
Any combination of data that can reasonably identify a person

AI ASSISTED


When in doubt, treat it as sensitive. Protect personal information. Protect people.


Be Aware. Be Secure. Be Trusted.

Contextual Information Workflow



Surveillance Technologies

Surveillance technologies are equipment or information systems that collect data from people's lives and their social, work, and/or physical interactions.

This information includes identity, movements, culture, linguistic knowledge, nature, and history of an individual or group of individuals.



Portlanders are saying …





Porch cameras are everywhere now. Can they be used in a way that harm to the community?



My friend's employer records her on camera to make sure she is being productive at work. That seems invasive.



I attended a protest downtown and I heard that the police were taking footage of the crowd.





When I use Biketown or Parking Kitty, I wonder if my personal information if being stored or shared.

[Report of public engagement for the surveillance technologies policy]

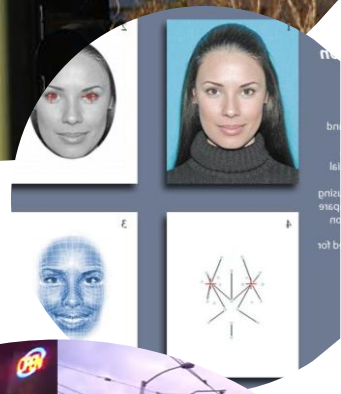
Surveillance technologies Examples

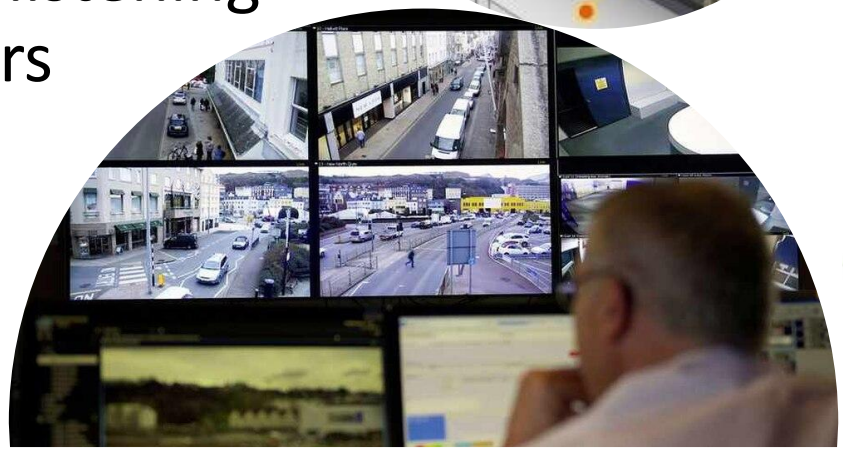
- Automated license plate readers
- Body worn cameras
- CCTV
- Connected transportation
- Digital kiosks
- Drones
- Gunshot detectors
- Red light cameras
- Social networks monitoring/listening
- Smart payment/Smart meters
- Face recognition/Biometrics
- Geolocation services
- Public Wi-Fi
- RFID/Bluetooth













Over Surveillance and Bias

Deploying surveillance on specific neighborhoods or just monitoring specific groups will lead to biased information and, in some cases, oversampling.

Information collection practices must be assessed to identify bias and gaps.



The Surveillance Gap

Legal and social phenomenon where extreme privacy or "functional invisibility" causes marginalized populations to be excluded from mainstream data flows, leaving them vulnerable to severe harms

These people include undocumented immigrants, day laborers, homeless persons, and people with felony conviction histories suffering collateral consequences of their convictions.



Native Invisibility - Indigenous Data Sovereignty

Dominant stories, or narratives, about Native peoples in North America.

Who holds these views?

How do these views affect public perception, public support and public policy?



Connecting to Data Governance



Data governance is the policies and practices that enable and maintain data usability, integrity, and privacy within an organization.

Key project goals for Portland's City Data Governance Committee:

- Citywide demographic data standards
- Citywide minimum metadata requirements
- Data catalog
- Best practices for data collection
- Best practices for data sharing

DATA GOVERNANCE PRINCIPLES

People-Centered. Rights-Respecting. Equity-Driven.

Good governance of data empowers people and advances a just and sustainable digital society.

1. ACCOUNTABILITY

Define and assign clear ownership, roles and responsibilities for data and its use.

2. TRANSPARENCY

Make data practices visible and understandable. Communicate clearly and openly.

3. DATA QUALITY

Ensure data is fit for purpose, reliable, accurate, complete, timely and accessible.

4. DATA USE

Use data purposefully and responsibly to create value and positive impact.

5. DATA SECURITY

Protect data throughout its lifecycle to ensure confidentiality, integrity and availability.



6. PRIVACY

Respect and protect privacy and personal data. Empower individuals with control over their data.

7. DATA LIFECYCLE

Manage data across its lifecycle with stewardship—from creation or collection to use, retention, sharing and disposal.

8. INTEROPERABILITY

Enable data to work across systems and organizations to deliver greater benefit for people and society.

9. COMPLIANCE

Comply with applicable laws, regulations and standards. Uphold ethical and professional obligations.

FOUNDATIONS: RIGHTS & EQUITY VALUES

HUMAN DIGNITY
Uphold the inherent dignity and rights of every person.

DIGITAL RIGHTS
Respect, protect and promote digital rights online and offline.

EQUITY & INCLUSION
Advance fairness. Address bias. Remove barriers. Include all.

PARTICIPATION
Involve diverse voices and communities in data decisions.

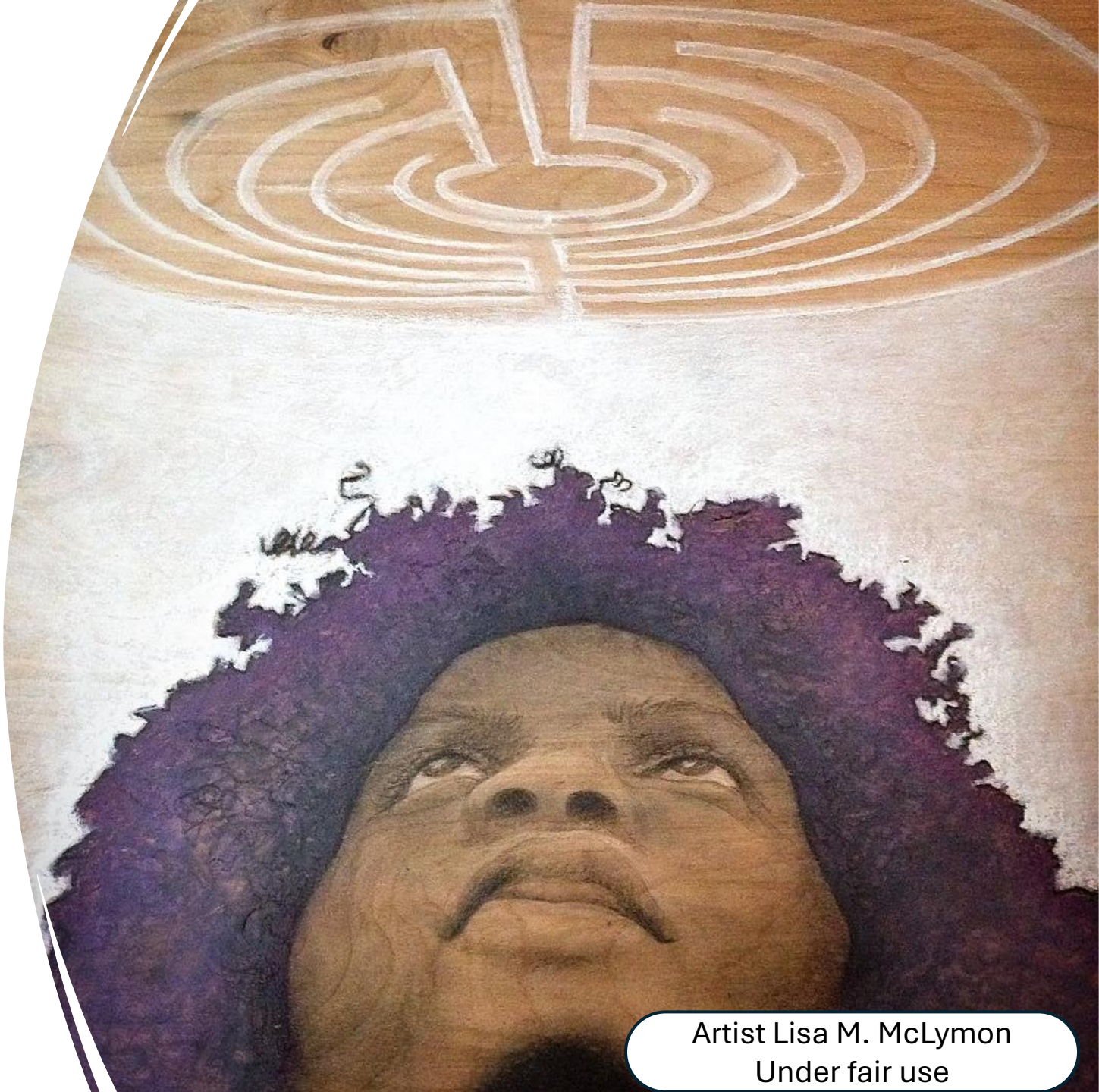
BENEFIT & JUSTICE
Ensure data benefits are shared and harms are prevented.

SUSTAINABILITY
Consider impacts on people and planet—today and tomorrow.

Digital Justice

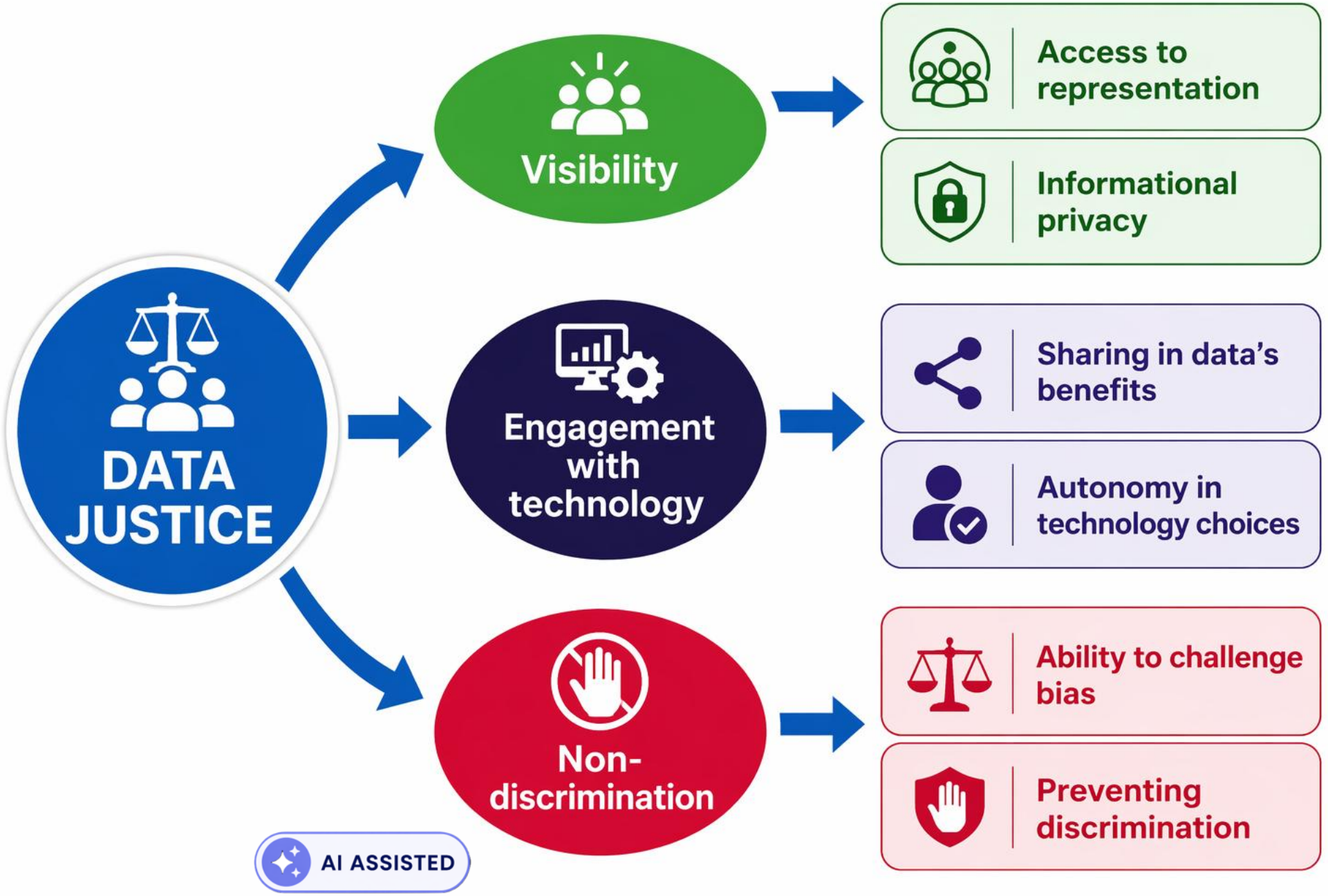
The equitable treatment of all people in technology and information, regardless of race, abilities, gender, age, personal circumstances or social context.

Digital justice ensures that people have the digital rights and resources they need to thrive—including access to digital infrastructure, shared ownership of digital resources, data protection, and open and accountable digital governance.



Artist Lisa M. McLymon
Under fair use

Data Justi



https://journals.sagepub.com/doi/full/10.1177/2053951717736335

Example: Automation Bias

Automation Bias is the human tendency to:

- Over-trust automated systems, assuming they are always correct.
- Ignore contradictory evidence because automated recommendation seems more reliable.
- Follow automated outputs even when they are clearly flawed (e.g., GPS sending someone down a closed road).



AUTOMATION BIAS

The tendency to over-rely on automated systems and disregard or override one's own better judgment.

	HEALTHCARE	HIRING	POLICING	EDUCATION	LENDING
	AI system flags patient as "low risk" for complications.	AI ranks candidates and recommends not advancing this applicant.	Predictive policing system identifies an area as "high risk."	AI predicts a student is "low likeilhood of success."	AI assigns a low credit score and recommends denial.
					
AUTOMATED RECOMMENDATION	Doctor trusts the system and does not order additional tests.	Hiring manager accepts the recommendation without further review.	Officers focus patrols in the area, trusting the prediction.	Teacher lowers expectations and recommends fewer advanced opportunities.	Loan officer denies the application without reviewing details.
HUMAN RELIES ON THE SYSTEM					
POTENTIAL NEGATIVE OUTCOME	Condition is missed. Patient's health worsens.	A strong candidate is overlooked. Less diverse workforce and lost talent.	More police presence leads to more stops and arrests, perpetuating bias and eroding trust.	Student is not challenged and may underperform, reinforcing the prediction.	Qualified applicant is denied credit, limiting financial opportunity.
					

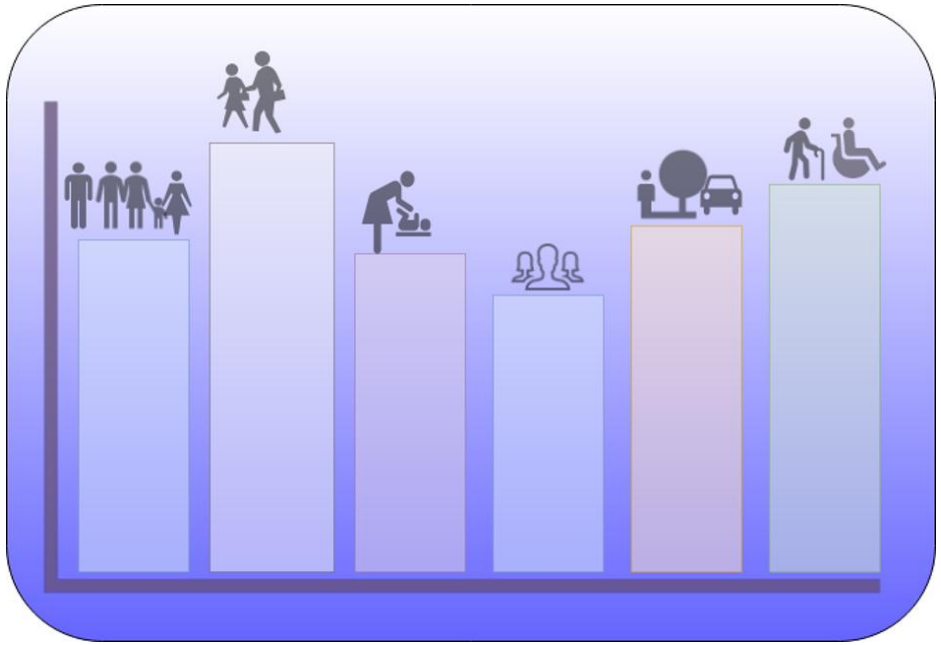
AI GENERATED

Data Governance and Automation Bias

Automated systems often learn from biased historical data

Automation bias connects with data governance:

- Automated systems rely on data quality
- Automated decisions can amplify bias and compliance risk
- Data governance defines human-in-the-loop (human-in-control) requirements
- Governance ensures transparency and explainability in automated systems
- Governance provides training and policy controls



AI ASSISTED

REDUCING AUTOMATION BIAS
WITH DATA GOVERNANCE

Strong data governance ensures automated systems are trustworthy, fair, explainable, and used responsibly.

DATA GOVERNANCE RECOMMENDATIONS

1 DATA QUALITY RULES



Define and enforce data quality standards to ensure accurate, complete, consistent, and representative data.

→ **Better data in, better decisions out.**

2 BIAS DETECTION AND FAIRNESS ASSESSMENTS



Continuously test for bias across data and models. Assess fairness across relevant groups and act on findings.

→ **Fairer models, greater equity.**

3 MODEL DOCUMENTATION AND EXPLAINABILITY REQUIREMENTS



Require clear documentation of data sources, model design, assumptions, and limitations. Ensure models provide explainable outputs.

→ **Transparency builds trust and understanding.**

4 HUMAN-IN-THE-LOOP OVERSIGHT FOR HIGH-RISK DECISIONS



Ensure a qualified human reviews and can override automated recommendations in high-impact decisions.

→ **Human judgment where it matters most.**

5 ACCESS CONTROLS AND CLASSIFICATION TO PREVENT INAPPROPRIATE USE OF SENSITIVE DEMOGRAPHIC DATA



Classify sensitive data, limit access by need-to-know, and prohibit uses that may cause harm or discrimination.

→ **Protects privacy and prevents misuse.**

6 AUDITABILITY AND TRACEABILITY FOR REVIEWING QUESTIONABLE OUTCOMES



Log decisions, data, and model versions to enable end-to-end traceability and support investigations and learning.

→ **Accountability and continuous improvement.**

BENEFITS & IMPACTS IN DATA MANAGEMENT

IMPROVED DATA QUALITY
Higher accuracy, completeness, and consistency across data assets.

REDUCED BIAS AND DISCRIMINATION
Fairer outcomes and better representation for all individuals and groups.

GREATER TRUST AND TRANSPARENCY
Clear documentation and explainability build confidence with users and the public.

BETTER DECISIONS
Human oversight ensures context, nuance, and accountability in high-stakes decisions.

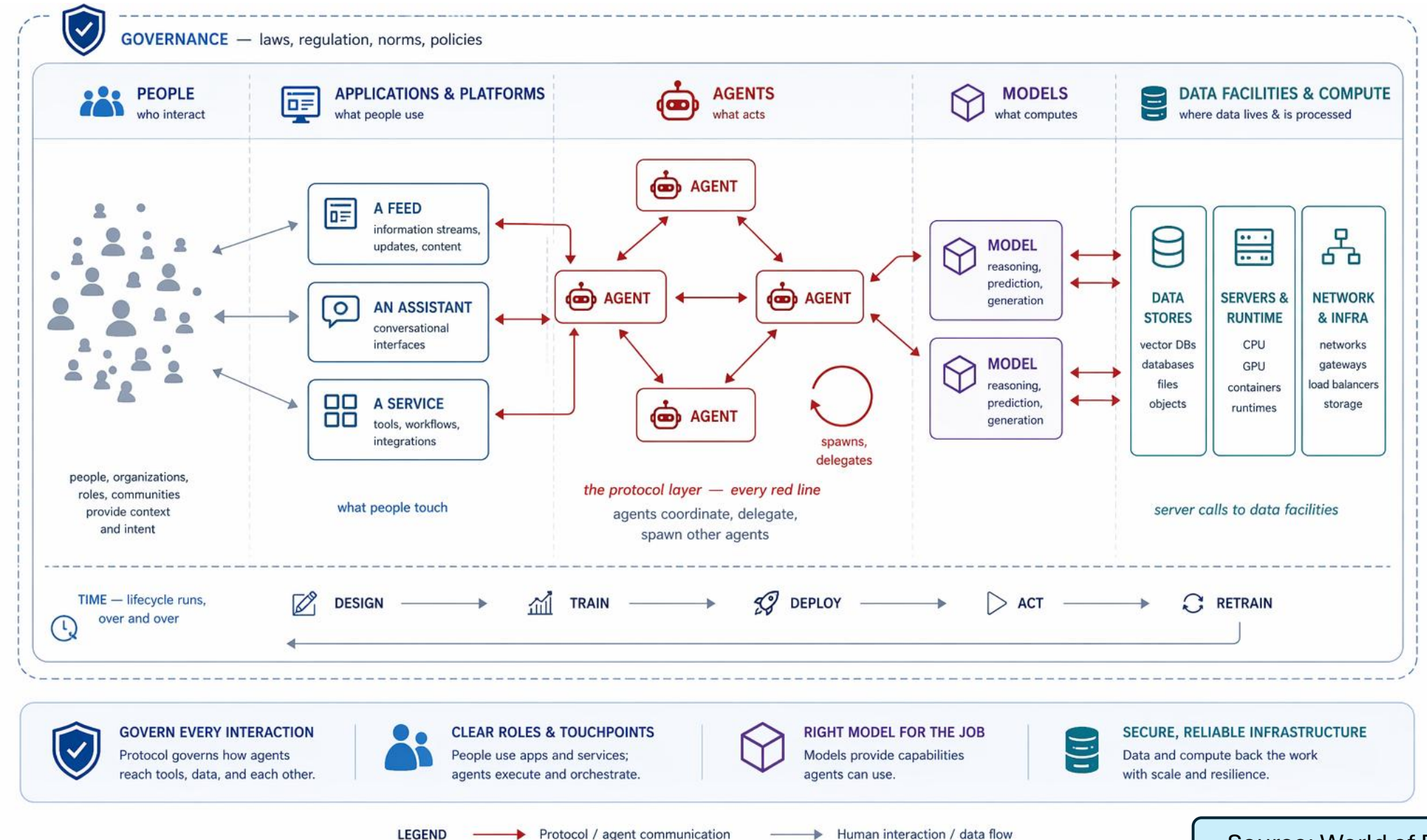
STRONGER PRIVACY AND COMPLIANCE
Proper data controls reduce risk and support legal and ethical obligations.

CONTINUOUS LEARNING AND IMPROVEMENT
Traceability enables issue identification, remediation, and ongoing system improvement.

THE BOTTOM LINE | Thoughtful data governance reduces automation bias, protects people, and drives responsible, high-quality data management for better outcomes.

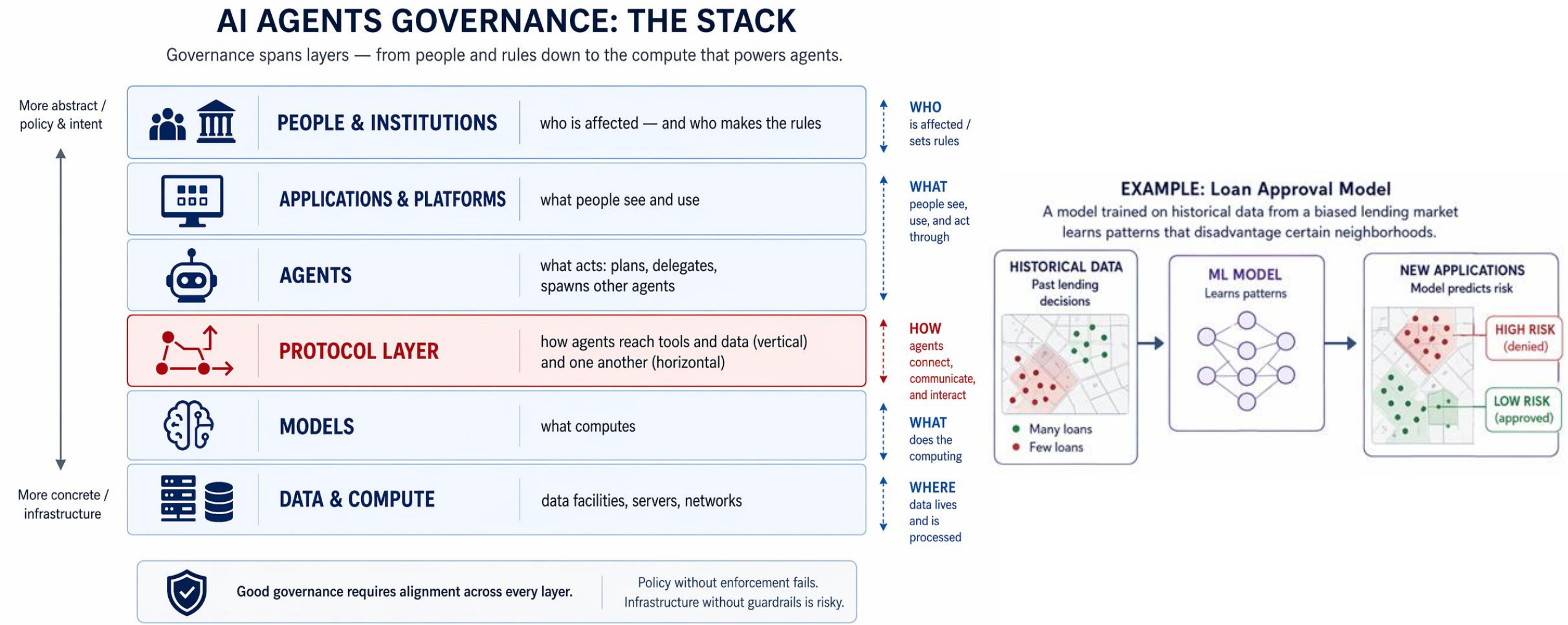
AI GENERATED

New Distributed Governance Challenges



Source: World of Privacy Forum

Agentic AI, data governance, and equity



Source: World of Privacy Forum

Future – Digital Sovereignty

Personal digital sovereignty is the idea that individuals have meaningful control over their digital identity, personal data, and how that data is used, regardless of where the data flows or which systems handle it.

Data Governance Can Implement Personal Digital Sovereignty:

- Data Ownership and Access Rights
- Data Minimization and Purpose Limitation
- Interoperability and Portability Standards
- Transparency and Auditability
- Encryption and Differential Privacy
- Decentralized or Federated Data Models



AI ASSISTED

Contact:

Hector Dominguez
hector.dominguez@portlandoregon.gov

Data and Privacy Office
City Operations
City of Portland, OR