WASHINGTON ARTIFICIAL INTELLIGENCE RESISTANCE

WA-AIR

AI Policy Framework

April 2026

Contents

1 Executive Summary **2**

2 Problem Context **2**
- 2.1 Why We Need To Take on AI . . . 2
- 2.2 Building on 2026 Momentum . . . 2
- 2.3 Public Opinion Favours Regulation . . . 2
- 2.4 How Washington Can Lead . . . 3
- 2.5 Why Now is the Time for Bold Action . . . 3

3 Principles **3**
- 3.1 Why These Values? . . . 3

4 Gaps in Public Policy **4**
- 4.1 Data and Biometric Privacy . . . 4
- 4.2 Algorithmic Guardrails . . . 4
- 4.3 Public Infrastructure Transparency . . . 5
- 4.4 Economic Fairness . . . 6
  - 4.4.1 NLRA Gaps . . . 6
- 4.5 Executive Accountability . . . 6

5 Gaps for Labor Organizers **7**
- 5.1 Difficulty Protecting Workers' Rights . . . 7

6 New Public Policy Options **7**
- 6.1 Addressing Economic Fairness . . . 7
  - 6.1.1 Automation Impact Levy . . . 7
  - 6.1.2 Profit-Based Business Tax Models . . . 8
- 6.2 Addressing Data and Biometric Privacy . . . 8
  - 6.2.1 Prohibited Technology . . . 8
  - 6.2.2 Digital Rights Act . . . 9
  - 6.2.3 Institutional Guardrails . . . 9
- 6.3 Algorithmic Guardrails . . . 9
  - 6.3.1 Data Lineage Disclosure . . . 9
  - 6.3.2 Right to Authenticity . . . 10
- 6.4 Public Infrastructure Improvements . . . 10
  - 6.4.1 Public Records Reform . . . 10
  - 6.4.2 Tribal Consent . . . 10
  - 6.4.3 Data Center Sustainability Reporting . . . 10
  - 6.4.4 Commitment to Shared, Sustainable, Resistant Grids . . . 11
  - 6.4.5 Development Moratorium and Financial Risk Mitigation . . . 11
- 6.5 Executive Accountability . . . 11

7 Implementation Strategies **12**
- 7.1 The Interstate Compact . . . 12
- 7.2 Third Party Safety Audits . . . 12

Executive Summary

This is a comprehensive policy framework representing a shift from a reactive regulatory model to a proactive, rights-based structure of governance. This policy framework synthesizes international standards from the European Union General Data Protection Regulation (GDPR), the EU AI Act, and domestic frameworks from Colorado and California.

The state of Washington seeks to establish a global gold standard for technological accountability. This evidence-based framework addresses the critical intersection of data privacy, algorithmic fairness, infrastructure transparency, and economic fairness to secure the state's democratic and ecological future.

The document serves not only as a legislative roadmap for the 2027 session but as a universal standard for coalition partners and private institutions seeking to align their operations with ethical AI principles. Via implementing computation levies, executive liability standards, and critically enhanced public disclosure requirements, this framework provides tools that reduce the power disparity between global corporate technological interests and that of Washington state and the public it represents.

Problem Context

Why We Need To Take on AI

Over the last two decades, Big Tech has rolled out product after product with virtually no oversight or accountability. Their "move fast and break things" model has caused serious societal harm while they have flooded local, state and federal governments with campaign contributions to stop regulation before it can start.

As of 2026, one in four federal lobbyists represent the AI industry, which is increasingly a clear and present danger to democracy, privacy and our world.

Building on 2026 Momentum

In the 2026 legislative session, multiple bills made significant progress despite the short session. While bills to regulate data centers (HB 2515) and surveillance pricing (HB 2481) were unable to overcome the combination of industry opposition and a crowded calendar, advocates were able to muster significant public support.

With time to build a real coalition and mobilize voters, plus the full-length session, we believe Washington can make meaningful progress in 2027.

Public Opinion Favours Regulation

Polls show that a growing, cross-partisan majority of voters is deeply concerned about the rapid growth of AI. There is also growing public opposition to the construction of

new hyperscale data centers required for AI, with their impact on power costs, general affordability of life in Washington state, and people's livelihoods.

A wide, cross-partisan majority supports strong regulation of AI as well as adoption of general privacy regulations that can also combat the rapid development and deployment of AI. With the Trump administration and much of the GOP in Washington fully captured by the industry, the burden falls on states to take regulatory action.

How Washington Can Lead

Washington is uniquely positioned to model a "third way" of AI governance that preserves the capability to innovate while protecting already strained public resources. Washington can create a unified regulatory front that resists federal preemption and protects the powers of the state to regulate consumer safety and state resources.

Why Now is the Time for Bold Action

Voters are disillusioned with tech billionaires who control the economy and create a life that is harrowed and unaffordable all while evading accountability. With the convergence of public momentum on this issue, the inadequacy of existing legal standards, and the opportunity afforded by a full legislative session, this can be rectified. Postponing action would allow harms to become further entrenched in the state's infrastructure and legal code.

Principles

This framework is built on four pillars that mirror the expectations of a democratic society, echoing Washington's Chinook state motto "Al ki" / "into the future."

Why These Values?

These core values were selected because they represent the primary vectors by which AI technology exerts power over individuals and communities.

> **Without Fairness,** AI becomes a tool for perpetuating biases in high-impact settings, including commerce, employment, housing, education, healthcare, lending, and government services. AI becomes a tool that worsens existing economic hardships and inequalities. AI becomes a tool that obstructs the path to an affordable and safe Washington.
>
> **Without Transparency,** the public cannot verify the safety or sustainability of the digital systems upon which they depend.

Without Privacy, our digital commons transform into a one-way surveillance economy. In a broader environment where Washington needs to guarantee the safety of its residents from a federal government aggressively intruding on local affairs, Washington residents need checks and balances against a digital oligarchy that can weaponize their data against them.

Without Accountability, the risks of innovation are distributed to the public while the rewards are privatized. AI is likely to worsen already present systemic inequalities, which must be mitigated and remediated.

Gaps in Public Policy

Current policies fail to anticipate the impact of AI and modern technology upon:

Data and Biometric Privacy

HIPAA presents with significant gaps, also not covered by WA "My Health My Data," which lead to lapses whereby Washington residents cannot control their privacy and outcomes following from the compromise of that privacy:

- HIPAA "anonymized" healthcare data can be deanonymized using AI, revealing medical conditions of vulnerable individuals.
- Data stored according to HIPAA rules is not regulated for accuracy, and uncorrectable medical chatbots are considered by physicians to be a top public health hazard in 2026.
- Employers penalizing workers for low output, tracked with AI, may be measuring metrics related to medical conditions, with workers having no recourse.

Similarly, both FERPA and the WA "Student User Privacy in Education Rights" act do not cover:

- That algorithmic advertising is banned but not predictive analytics, flagging "at risk" students in ways that they cannot object to or control well into adulthood.
- "School officials," via a loophole, can expose intellectual property of minors to train AI models with neither student nor parental consent.
- The lack of recourse for students from marginalized communities who cannot opt out of AI disproportionately flagging them for academic integrity and behavioural concerns.

Algorithmic Guardrails

Current consumer protection laws do not account for the phenomenon of "surveillance pricing" where AI algorithms adjust the price of essential goods like groceries in real

time, based on an individual's inferred willingness to pay.

The practice of surveillance pricing transforms community-based retail into a demographically targeted advertising engine that exploits vulnerable customers and attempts to obviate any enforcement on price discrimination by using algorithms as a shield.

When applied to wages, as it is used for much of "gig economy" labor, it becomes a vector for rampant wage discrimination that the state cannot effectively regulate.

Further, there are no state-level mandates that require or guarantee that a human has reviewed high-stakes decisions in healthcare, criminal justice, lending, or employment. This will lead to opaque and increasingly biased outcomes, unless liability of a decision can be ascribed to an actor that can appear to defend that decision in a public court of law.

Public Infrastructure Transparency

Data center construction and operation often involve a total lack of transparency with regards to their use of public environmental resources. Current state law does not require data center operators to disclose via audited third party, their water consumption, carbon emissions, or energy mix to the communities in which they operate.

The use of nondisclosure agreements (NDAs) are prevalent and yet unregulated, as are the use of shell corporations to obscure information, and prevent local governments from making informed decisions on land and water use. Communities that have data centers permitted for construction will often find, only many years after project completion, that:

- Consumer electricity prices exceed headline CPI inflation
- They experience more than a 25% increase in electricity prices over 5 years
- There can be a constant low-grade "jackhammer-like" background noise in surrounding communities, creating nuisance, driving away wildlife, and lowering property values
- Data centers can use more than 10% of an entire county's water consumption allotment per day, necessitating in one case $212,000,000 in water infrastructure grants, widening state and federal deficits for private gain
- Data centers contribute significantly to air pollution within their campus regions, the effects of which result in chronic illnesses manifesting many years post-construction, estimated to cause $20,000,000,000 of burden to public health systems

Further, these new data center projects present with particularly unique pressures in our state given the rapid "net absorption" of 154.5 megawatts of data center power capacity suddenly foisted onto our state's natural resources and power grid in 2025

alone. Public policy does not adequately address the scale of the problem posed by AI-enabling data centers.

Economic Fairness

The federal and state tax codes are currently "automation biased," incentivizing the replacement of human labor with capital-intensive AI systems.

Companies can frequently deduct 100% of their investment in hardware and software while human payroll remains heavily taxed through FICA and other labor-based levies. This creates a fiscal "death spiral" where the tax base shrinks even as the demand for social safety nets increases due to job displacement.

Given this incentive structure, Washington state will additionally experience further constrained B&O tax revenues and constrained contributions to the recently implemented WA Cares tax and PFML tax as employers attempt to reduce payroll counts. This may increase insolvency risk of one or several funds as firms essentially opt out of taxation by using automated, "pirated labor."

This situation is parallel to how increasing adoption of electric vehicles contributed to Washington's budget shortfall because the state failed to account for lower gas tax revenues, but potentially much more severe:

- The state is estimated to have lost conservatively $100,000,000 in gas tax revenue due to increased EV registrations per annum.
- If AI automates 1 out of 10 jobs, with no income taxes otherwise offsetting rapid payroll tax declines, worker safety net programs like PFML, WA Cares, and Unemployment Insurance will face immediate insolvency totalling more than $4,000,000,000 in impact.

NLRA Gaps

A recognized opportunity created by gaps in the National Labor Relations Act of 1935 is that it does not provide for automatic mechanisms that trigger collective bargaining processes.

AI systems are already being used to suppress labor organizing, profit from work outputs where workers cannot otherwise reap collective benefits, and to devalue and degrade labor. It is therefore of paramount importance to use the moment of AI deployment to equalize that dynamic.

Executive Accountability

Under current regulations, the "Developer Liability Shield" (analogous and complementary to Section 230) diminishes the legal incentive for AI providers to implement downstream safeguards.

There are no established criminal or civil mechanisms to hold executives responsible

for "critical safety incidents" caused by autonomous AI agents, leaving a profound accountability gap when these systems cause real-world damage.

Gaps for Labor Organizers

Unions have unique risks to protections they have collectively bargained to obtain, for which they need to prepare:

Difficulty Protecting Workers' Rights

AI will pressure the sizes of collective bargaining units and their economic leverage:

- AI facilitates increasing atomization of labor into "gig work," displacing labor categories and reducing the base of workers who can collectively bargain.
- Unions operating under older contracts may opt to protect workers but not also their work outputs: By using worker output to automate work and thereby replace workers, AI reduces worker leverage.
- All known tactics of union busting will be exacerbated greatly, and will be an early application for AI surveillance.
- AI is primarily impacting the jobs of entry-level professionals, eroding the base of workers who can support the entire lifetime of a strong, vibrant labor union.
- Because response to worker grievances will be increasingly based on algorithmic decisions, and without the ability to challenge the factual basis of that reporting, unions will be less able to assist.

New Public Policy Options

Addressing Economic Fairness

Automation Impact Levy

To address the displacement of human workers, Washington may leverage the existing framework of the "Advanced Computing B&O" levy via an "Automation Impact Fee" on commercial AI deployments, scaled by usage volume; exempting nonprofits, academic research, and small businesses for whom it would be costly to assess and administer the tax.

Using a localized capture model of a reported $650 billion in capital expenditure across the AI sector, given only Microsoft and Amazon's footprint in our region, with a 10% automation surcharge assessed per dollar of corporate AI spend, the state could recover up to $700M a year in revenue, cutting the current annual budget deficit from $2.3B to $1.6B.

At a 20% software automation surcharge rate, bringing in ~$1.4B per annum, some or all of this revenue could also fund a general wage insurance program for the estimated 110,000 workers in sectors vulnerable to AI automation in Washington, covering:

- Up to 80% of the wage gap for workers who accept lower-wage work after displacement, up to $40,000 (~$500M cost per annum est.)
- Initial, short-term wage displacement stipends of up to $10,000 (~$120M cost per annum est.)
- Universally accessible retraining vouchers, credits, and grants for public educational institutions up to $10,000 per person (~$500M cost per annum est.)
- Portability of wage insurance benefits, tying them to the individual and not the job

Profit-Based Business Tax Models

The state must also shift its tax base to capture the "supernormal" profits of the AI industry. This could include:

- A state-level Value Added Tax (VAT) / Business Activity Tax (BAT) to replace shrinking payroll tax revenues
- A "high automation business" additional B&O surcharge to offset losses to public funds from labor displacement, via tiering schemes by which corporations above a certain headcount with high revenue-per-employee ratios pay additional B&O surcharges

Addressing Data and Biometric Privacy

Prohibited Technology

Washington must enact a categorical ban on the deployment of facial recognition technology in all consumer goods, including "smart" glasses and doorbell cameras. Additionally, parallel to the EU AI Act we must ban:

- Social scoring systems
- Surveillance-based pricing
- Subliminal manipulation (the use of AI to reinforce addiction or harm consumers)
- Employee surveillance, including prohibiting the use of AI to suppress labor organizing

Legislation should also prohibit the "passive harvesting" of data by mass surveillance systems like Automated License Plate Readers (ALPRs) that lack restrictions on data retention, targeting, or clear signals for when they are enabled.

Digital Rights Act

The state should implement a comprehensive Digital Rights Act that codifies European-style data subject rights into Washington law, including but not limited to:

- **Right to Erasure** — Requirement for "machine unlearning" where personal data must be removed from model training weights upon request.
- **Right to Review and Rectification** — An obligation for AI developers and deployers to provide a mechanism for Washington residents to correct data processed by AI, as well as to correct resulting decisions.
- **Right to Object** — An absolute right for residents to opt out of data collection for automated decisioning purposes, with clearly defined high-risk categories including credit and lending, predictive analytics, targeted advertising, employment, healthcare, education, housing, and government service determinations.
- **Right to Accountability** — An obligation for AI developers and deployers to bear the legal liability for decisions made by their autonomous systems.
- **Data Portability** — Mandate for companies to provide data in machine-readable formats (JSON/XML) for easy transfer between services and for legal audit.

Institutional Guardrails

To fill federal gaps, the state must extend HIPAA-level protections to all entities processing health-related data, regardless of their status as a healthcare provider. Similarly, FERPA protections should extend to all entities processing education-related data. This includes a "Safe by Default" requirement where AI wellness applications, education applications, and chatbots must utilize the highest available privacy settings as the baseline configuration.

Furthermore, AI deployments in the workplace should be grounds for mandatory collective bargaining. Washington should guarantee that workers have a right to bargain around conditions of AI usage in the workplace, freely and in good faith.

Algorithmic Guardrails

Data Lineage Disclosure

Transparency requires moving beyond the "opaque box" model. Developers must be required to provide a "Data Lineage Disclosure" for all AI models commercially deployed in Washington. This includes:

- A sufficiently detailed summary of the training data, including its origin and owners
- Documentation of efforts to identify and mitigate historical biases in datasets, specifically regarding race, ethnicity, and gender
- Publicly available "Model Cards" that outline the system's intended purpose, limitations, and performance metrics

This framework should also align with CA AB 2013, which provides acceptable institutional trade secret protection—therefore any firm also operating in California cannot argue this is unduly burdensome.

Right to Authenticity

The state must establish a "Right to Authenticity," requiring that all AI-generated images, audio, and video include persistent, machine-readable metadata identifying the content as synthetic, and a human-visible watermark as well. Furthermore, residents possess a "Right to Interact with a Human" in any interaction with an AI chatbot that represents a licensed professional, such as a psychologist or medical practitioner.

Public Infrastructure Improvements

Public Records Reform

Washington should ban the use of nondisclosure agreements (NDAs) between data center developers and government agencies. Public records laws must be reformed to ensure that all data center permit applications, water rights transfers, and energy usage projections are subject to immediate and full public disclosure, with clear connection to the actual entity filing the original document.

Tribal Consent

Washington should guarantee that no large-scale energy or industrial project shall proceed without meaningful consultation and the free, prior, and informed consent of affected Tribal Nations, particularly regarding impacts on treaty-protected water rights and salmon recovery.

Data Center Sustainability Reporting

Each "Emerging Large Energy Use Facility" (ELEUF), defined as a facility with a demand of 20 megawatts or more, must publish an annual sustainability report including:

- **Water:** Daily and annual usage in gallons, including source and cooling technology used; Water Usage Efficiency (WUE) metrics
- **Energy:** Total usage and percentage derived from fossil fuels vs. renewable sources; Power Usage Efficiency (PUE) metrics
- **Grid Impact:** Estimated infrastructure upgrades required and impact on local rates, including electrical transmission costs, water infrastructure costs, and estimated impact on utility ratepayers
- **Emissions:** Scope 1, 2, and 3 emissions including leakages of high GWP refrigerants; reporting on total online time of backup diesel generators

Before seeking permits, data center operators should communicate the annualized impact of a data center project in clear and plain language to community residents, including construction duration, expected long-term jobs, contractor information,

utility rate impacts, and community grievance procedures.

Commitment to Shared, Sustainable, Resistant Grids

Small Modular Nuclear Reactors (SMNRs) as a solution for data center demand should be categorically unpermitted, unapproved, and rejected due to unproven commercial viability, high-level waste concerns, and opposition from Tribal Nations. Mature, cost-effective technologies like wind, solar, and long-duration storage should be promoted instead. Data centers should be mandated to add renewable capacity to the grid beyond their own demand as a form of public betterment.

Development Moratorium and Financial Risk Mitigation

Washington should enact a statewide moratorium on new data center development until new legislation has ensured that renewable energy buildout, watershed protections, and annual sustainability reporting can be guaranteed. Furthermore, with AI development tied to high-risk, publicly opaque, and questionably solvent private credit funds, a moratorium should also be emplaced so as to validate the nature of the underlying demand, such that residents of Washington do not allocate significant public resources for projects that neither complete nor return investment.

Executive Accountability

The state must establish clear criminal and civil liability for executives of companies whose products cause harm to Washington residents. This may include:

- Establishing the elements of "mens rea" (recklessness or indifference) for executives who deploy agentic AI systems that cause critical infrastructure failures or large-scale physical harm
- Adopting frameworks like the Colorado AI Act, establishing a "Duty of Care" standard for AI developers
- Firms deploying AI with the demonstrable outcome of increasing employment-related discrimination should be included in existing law covering Unfair Labor Practices
- Strengthening the Consumer Protection Act to allow for fines amounting to the greater of $100,000 or 5% of worldwide annual gross revenue, per diem, for ongoing violations
- For individual non-recurring violations, fines of $10,000 per violation, accounted for as per se injury with no proof of resulting economic injury required
- Enabling a private right of action, as in HB 2225, so that the state attorney general is not the bottleneck to preventing just and fair outcomes
- Requiring developers to fund a "Decommissioning Bond" to ensure that defunct data centers are transitioned or dismantled without leaving an ecological or financial burden on the host community

Implementation Strategies

The Interstate Compact

To circumvent the "America's AI Action Plan" and its associated federal preemption threats, Washington should form an "AI Governance Interstate Compact" with Colorado, California, and other like-minded states. This compact would create a unified legal theory defending state authority under the Tenth Amendment and the Dormant Commerce Clause to regulate the local impacts of a global industry. This "Persuasive Resistance" strategy would signal a unified state position to Congress and provide a collective defense against DOJ litigation.

Third Party Safety Audits

Compliance with the Washington AI Bill of Rights should be a condition for business licensure. The state will establish a "Center for AI Safety and Evaluation" to oversee third-party audits based on the NIST AI Risk Management Framework and ISO/IEC 42001 standards.