

# Truth in Job Advertising and Applicant Data Protection Framework

July- 2026

## LABOUR MARKET & EMPLOYMENT POLICY | PRIVACY & DATA RIGHTS | TECHNOLOGY GOVERNANCE

Civic Sketches is a series of draft policy proposals by Lawrence Nault — an independent researcher and policy writer based in Alberta's Badlands. These proposals are working drafts, not party platforms or final answers. They are intended to invite discussion, challenge, and refinement across all levels of government and the broader public.

This policy proposal is published under the Creative Commons Attribution 4.0 International Licence (CC BY 4.0). You are free to copy, share, adapt, translate, and build upon this work for any purpose, including use by governments, organizations, advocates, researchers, and members of the public, provided appropriate credit is given to Lawrence Nault and any changes are clearly identified. Full licence: [creativecommons.org/licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/)

---

Every job posting asks something of the applicant.

It asks for time, attention, employment history, education history, references, contact information, salary expectations, and often enough personal detail to build a profile of a person's working life. That exchange should come with obligations.

If a job is not real, not active, already filled, only posted to build a résumé database, or dependent on a contract that does not yet exist, applicants deserve to know that before they apply. Job postings should not be allowed to function as fake labour-market signals, unpaid market research, or personal data harvesting tools.

The following proposal is a working framework for a Truth in Job Advertising and Applicant Data Protection law. It is meant to protect job seekers, improve labour-market data, and require employers, recruiters, and hiring platforms to be honest about what they are advertising and what they are doing with applicant information.

### 1. Purpose

The purpose of this framework is to protect job seekers, improve labour-market transparency, prevent deceptive employment advertising, and regulate the collection, retention, use, sharing, sale, and analysis of applicant data.

Job postings should exist to advertise real employment opportunities, not to harvest résumés, inflate perceptions of growth, test labour-market wages, create misleading job-market data, or collect personal information without meaningful disclosure.

No person should be required to surrender personal data to apply for a job that does not exist, is not actively being filled, or is being advertised for purposes other than hiring.

## 2. Guiding Principles

This framework is based on the following principles:

### *Truth in advertising*

A job posting should accurately represent the status of the position being advertised.

### *Applicant dignity*

Job seekers should not be misled, exploited, or used as a source of unpaid market intelligence.

### *Data minimization*

Employers and platforms should collect only the information required for a specific hiring process.

### *Purpose limitation*

Applicant data collected for one job should not be reused for unrelated purposes without clear, separate consent.

### *Retention limits*

Résumés and application materials should not be stored indefinitely.

### *Transparency*

Applicants should know who is collecting their information, why it is being collected, how long it will be kept, and whether it will be shared.

### *Platform accountability*

Job boards, recruitment platforms, and hiring software providers should not be passive beneficiaries of deceptive or exploitative job advertising.

### *Public data integrity*

Labour-market data used by governments, researchers, and the public should not be distorted by large volumes of fake, inactive, recycled, or misleading job postings.

## 3. Scope

This framework would apply to:

- Employers.

- Recruiters.
- Staffing agencies.
- Executive search firms.
- Third-party hiring firms.
- Job boards.
- Online employment platforms.
- Applicant tracking system providers.
- Labour-market data brokers.
- Public-sector employers.
- Crown corporations and government agencies.
- Contractors advertising jobs connected to public funding, grants, procurement, or government-supported projects.

It would apply to any publicly advertised job posting, including postings on:

- Company websites.
- Job boards.
- Social media.
- Recruitment platforms.
- Government employment portals.
- Staffing agency websites.
- Educational institution career boards.
- Professional association job boards.
- Automated hiring or recruitment systems.

## 4. Definitions

### *Job Posting*

A public communication inviting people to apply for employment, contract work, temporary work, paid placement, internship, apprenticeship, or other work opportunity.

### *Active Vacancy*

A real, approved, funded, and currently available position that the employer intends to fill within a stated hiring period.

### *Talent Pool Posting*

A posting used to collect potential applicants for future opportunities where no current active vacancy exists.

*Conditional Posting*

A posting for a role that depends on a future event, including contract award, grant approval, project approval, budget approval, client demand, or government procurement.

*Internal Candidate Posting*

A posting where an internal or preferred candidate already exists, but external applications are still being accepted.

*Evergreen Posting*

A recurring or continuously active posting used to gather candidates for roles that may open periodically.

*Ghost Job*

A job posting that is presented as an active vacancy when the employer does not have a real, approved, funded, and current intention to hire for that role within the stated hiring period.

Ghost jobs may include postings created to:

- Collect résumés without a current vacancy.
- Build a talent database.
- Test wage expectations.
- Create the appearance of company growth.
- Signal expansion to investors or competitors.
- Satisfy internal policy requirements despite a predetermined candidate.
- Gather market intelligence.
- Make an employer appear more active or successful than it is.
- Produce misleading labour-market data.
- Funnel applicant data into third-party systems.
- Applicant Data

Any information submitted, collected, inferred, generated, or analyzed during a job application process, including:

- Name.
- Address.
- Email address.
- Phone number.
- Employment history.
- Education history.

- Credentials.
- References.
- Cover letters.
- Résumés.
- Work samples.
- Portfolios.
- Salary expectations.
- Availability.
- Immigration or work authorization status.
- Disability accommodation information.
- Demographic information.
- Assessment results.
- Interview notes.
- Screening scores.
- AI-generated rankings.
- Personality test results.
- Background check information.
- Metadata collected through online platforms.
- Any profile created about the applicant.

## 5. Job Posting Classification Requirement

Every public job posting must clearly identify the status of the opportunity.

The posting must be labelled as one of the following:

### ***5.1 Active Vacancy***

The employer has:

- An approved position.
- Budget or funding for the position.
- Authority to hire.
- A real intention to hire.
- A defined hiring timeline.
- A role that is currently available.

### ***5.2 Talent Pool***

No current vacancy exists. The employer is collecting applicants for possible future opportunities.

A talent pool posting must not be presented as an active vacancy.

### ***5.3 Conditional Opportunity***

The job depends on a future event, such as:

- Contract approval.
- Grant approval.
- Budget approval.
- Client demand.
- Procurement award.
- Project start.
- Regulatory approval.

The posting must clearly state the condition that must be met before hiring can occur.

### ***5.4 Internal or Preferred Candidate Exists***

If an internal or preferred candidate already exists, the posting must disclose that external applications are being accepted, but that an internal or preferred candidate is under consideration.

### ***5.5 Evergreen Posting***

If a posting is continuously used for recurring recruitment, it must be labelled as an evergreen posting and must state that applications may not correspond to an immediate vacancy.

## ***6. Required Information in Every Job Posting***

Every public job posting must include:

- Employer name.
- Whether the employer is hiring directly or through a recruiter.
- Job classification status.
- Work location.
- Whether the role is remote, hybrid, or on-site.
- Whether the job is full-time, part-time, temporary, seasonal, contract, casual, or internship.
- Expected compensation range.
- Expected hours of work.
- Whether the position is unionized.
- Application deadline.
- Anticipated interview period.
- Anticipated hiring decision period.
- Expected start date or start-date range.

- Whether AI or automated screening tools will be used.
- Applicant data retention period.
- Applicant data use policy.
- Applicant data sharing policy.
- Applicant deletion or withdrawal process.
- Contact information for privacy or applicant-data concerns.

## 7. Hiring Timeline Requirement

An active vacancy must include a reasonable hiring timeline.

The employer must identify:

- Application closing date.
- Expected review period.
- Expected interview period.
- Expected decision date or decision window.
- Expected start date or start-date window.

If the employer does not intend to review applications within the stated period, the posting cannot be classified as an active vacancy.

If the hiring timeline changes, the posting must be updated.

If the employer cancels the hiring process, applicants must be informed.

## 8. Applicant Data Notice

Before an applicant submits any personal information, the employer, recruiter, or platform must provide a plain-language applicant data notice.

The notice must explain:

- What information is being collected.
- Why the information is being collected.
- Whether the information is required or optional.
- Who will access the information.
- Whether the information will be shared with third parties.
- Whether the information will be stored outside the applicant's jurisdiction.
- Whether AI, automated screening, ranking, or profiling tools will be used.

- Whether the information will be added to a broader talent database.
- Whether the information will be used for analytics, benchmarking, or training.
- Whether the information may be sold, licensed, transferred, or monetized.
- How long the information will be retained.
- How the applicant can request deletion.
- How the applicant can withdraw from consideration.
- Who is legally responsible for the information.

This notice must be visible before the applicant uploads a résumé or enters personal information.

It must not be buried only in a privacy policy, terms of service, or external legal document.

## 9. Consent Rules

Applying for a job may constitute consent to use applicant data for that specific hiring process only.

Separate, clear, opt-in consent must be required for:

- Adding the applicant to a general talent database.
- Sharing the applicant's information with affiliated companies.
- Sharing the applicant's information with unrelated employers.
- Using applicant data for labour-market analytics.
- Using applicant data to train AI or automated hiring systems.
- Selling, licensing, or transferring applicant data.
- Using applicant data for marketing.
- Keeping applicant data beyond the standard retention period.

Consent must not be bundled.

An applicant must be able to apply for a specific job without being forced to consent to unrelated data uses.

## 10. Data Retention Limits

Applicant data must be deleted after the hiring process ends unless:

- The applicant gives separate consent to longer retention.
- A specific legal obligation requires retention.
- The applicant is hired and the information becomes part of an employment record.



- The applicant has requested continued consideration for future opportunities.

A standard retention period should be established by law.

A possible model:

- Unsuccessful applicants: delete within 12 months.
- Withdrawn applications: delete within 90 days.
- Talent pool applicants: renew consent every 12 months.
- Assessment or screening data: delete within 12 months unless legally required.
- AI-generated applicant profiles: delete within the same period as the underlying application.

Applicants must receive a simple way to request earlier deletion.

## 11. Limits on Collection

Employers and platforms may only collect information that is reasonably necessary for the specific stage of the hiring process.

Initial applications should not require unnecessary sensitive information.

Unless legally required or directly relevant at that stage, employers should not require:

- Government identification numbers.
- Full birth date.
- Full home address.
- Driver's licence number.
- Passport details.
- Banking information.
- Credit information.
- Medical information.
- Disability information beyond accommodation needs.
- Family status information.
- Unrelated demographic information.
- Video recordings.
- Voice recordings.
- Personality testing.
- Social media access.
- Unnecessary references before interview selection.

More sensitive information should only be collected later in the process when genuinely required.

## 12. AI and Automated Screening

Where AI or automated tools are used in hiring, the posting and applicant data notice must disclose:

- That automated tools are being used.
- The type of tool being used.
- What the tool evaluates.
- Whether it ranks, scores, filters, or rejects applicants.
- Whether a human reviews automated decisions.
- Whether applicants can request reconsideration.
- Whether applicant data is used to improve, train, or test the system.
- Whether the tool was developed internally or by a third party.

Applicants should have the right to request human review of any rejection or ranking substantially influenced by automated systems.

Employers should not be allowed to use applicant data to train AI hiring systems without separate, explicit consent.

## 13. Ban on Résumé Sale and Unrelated Secondary Use

Applicant data must not be sold, licensed, traded, transferred, or monetized without specific, separate, informed, opt-in consent.

Employers, recruiters, job boards, and platforms must not use applicant data for unrelated secondary purposes without consent.

Prohibited secondary uses should include:

- Selling résumé databases.
- Sharing applicant profiles with unrelated employers.
- Training AI systems without consent.
- Creating commercial labour-market intelligence products without consent.
- Using applicant data for advertising.
- Using applicant data for unrelated behavioural profiling.
- Transferring applicant information through mergers or data-broker arrangements without notice and protection.

A résumé submitted for a job should remain an application, not become a commodity.

#### 14. Ghost Job Prohibition

It should be unlawful to advertise a job as an active vacancy if:

- No approved position exists.
- No budget exists.
- No hiring authority exists.
- There is no intention to hire.
- The employer is only collecting résumés.
- The employer is only testing wages or availability.
- The employer is only creating an appearance of growth.
- The employer is using the posting for market intelligence.
- The employer has already decided not to fill the role.
- The role is contingent but not labelled as conditional.
- The posting is evergreen but not labelled as evergreen.
- An internal or preferred candidate exists but that fact is not disclosed where required.

This does not prohibit talent pools, conditional postings, evergreen postings, or internal postings.

It simply requires them to be labelled honestly.

#### 15. Applicant Notification Requirement

Applicants must be notified when:

- The hiring process is cancelled.
- The job is filled.
- The posting is withdrawn.
- The role changes materially.
- The compensation range changes materially.
- The location or remote-work status changes materially.
- The hiring process is delayed beyond the stated timeline.
- Applicant data will be retained beyond the standard period.
- Applicant data has been shared with a third party.
- A data breach affects applicant information.

For large-volume hiring, notice may be automated, but it must still be clear and meaningful.

## 16. Platform Accountability

Job boards and hiring platforms must take reasonable steps to prevent deceptive postings.

Platforms should be required to:

- Verify employer identity.
- Identify third-party recruiters.
- Require job classification labels.
- Require applicant data notices.
- Remove expired postings.
- Flag continuously reposted jobs.
- Provide a process for reporting suspected ghost jobs.
- Investigate repeat offenders.
- Preserve posting records.
- Publish transparency reports.
- Provide applicants with access to platform-level data policies.
- Prevent scraping or unauthorized resale of applicant data.
- Clearly disclose whether the platform itself uses applicant data for analytics, AI training, advertising, or commercial data products.

A platform that profits from job advertising should share responsibility for the integrity of that advertising.

## 17. Posting Record Requirement

Employers, recruiters, and platforms must retain records of public job postings for a defined period.

Records should include:

- Original posting.
- Posting classification.
- Date posted.
- Date removed.
- Compensation range.
- Job location.

- Hiring timeline.
- Number of applicants.
- Whether interviews occurred.
- Whether the role was filled.
- Whether the successful candidate was internal or external.
- Whether the role was cancelled.
- Applicant data retention settings.
- Third parties that received applicant data.

These records should be available to regulators during audits or investigations.

## 18. Labour-Market Data Integrity

Governments should not treat all job postings as equal evidence of labour demand.

Public labour-market reporting should distinguish between:

- Active vacancies.
- Talent pool postings.
- Evergreen postings.
- Conditional postings.
- Internal/preferred-candidate postings.
- Cancelled postings.
- Reposted positions.
- Duplicate postings.
- Third-party recruiter duplicates.
- Platform-generated duplicates.

Government agencies using job-posting data should adjust for ghost jobs, recycled listings, and inactive postings before making claims about labour shortages, skills gaps, employment demand, or regional economic conditions.

No government should rely on unverified job-posting volume as the sole basis for labour policy, immigration planning, training subsidies, education funding, or corporate subsidy decisions.

## 19. Public Funding and Subsidy Conditions

Any employer receiving public funding, tax credits, grants, procurement contracts, wage subsidies, training subsidies, or economic development support should be subject to stricter job-posting rules.

Publicly supported employers must disclose:

- How many jobs were promised.
- How many jobs were posted.
- How many were active vacancies.
- How many were filled.
- Whether jobs were filled locally.
- Whether postings were conditional.
- Whether postings were cancelled.
- Whether applicant data was shared with third parties.
- Whether AI or automated screening was used.

A company should not be allowed to use ghost postings to exaggerate job creation connected to public subsidies.

## 20. Applicant Rights

Applicants should have the right to:

- Know whether a job is real, active, conditional, evergreen, or a talent pool.
- Know how their data will be used before applying.
- Apply without consenting to unrelated data use.
- Request deletion of their applicant data.
- Withdraw from consideration.
- Know whether AI or automated screening was used.
- Request human review of automated rejection.
- Know whether their information was shared with third parties.
- File a complaint about deceptive postings.
- File a complaint about misuse of applicant data.
- Receive notice if the hiring process is cancelled.
- Receive notice if their data is affected by a breach.

## 21. Employer Rights and Safe Harbours

This framework should not punish honest employers for ordinary hiring changes.

An employer should not be penalized simply because:

- A budget is unexpectedly cut.

- A candidate declines an offer.
- Hiring is paused for legitimate reasons.
- A project is delayed.
- A role changes during recruitment.
- No suitable candidate is found.
- Business conditions change.

However, the employer must update the posting, notify applicants where appropriate, and avoid presenting inactive or uncertain roles as active vacancies.

A safe harbour may apply where the employer can show:

- The posting was accurate when published.
- The employer had a genuine intention to hire.
- The employer updated the posting when circumstances changed.
- Applicant data was handled according to the stated policy.
- Applicants were not misled for data-harvesting purposes.

## 22. Enforcement

Enforcement could be handled through employment standards offices, privacy commissioners, consumer protection agencies, or a dedicated labour-market integrity office.

Regulators should have the power to:

- Investigate complaints.
- Audit employers and platforms.
- Require posting records.
- Require applicant data records.
- Order correction of misleading postings.
- Order deletion of improperly collected applicant data.
- Suspend deceptive postings.
- Penalize repeat offenders.
- Publish names of serious violators.
- Restrict access to public job boards.
- Restrict eligibility for public funding or procurement.
- Refer serious privacy violations to privacy regulators.
- Refer fraud-like conduct for further legal action where appropriate.

## 23. Penalties

Penalties should be scaled based on severity, intent, size of employer, number of applicants affected, and whether the violation was repeated.

Possible penalties include:

- Warning for first minor violation.
- Mandatory correction.
- Applicant notification order.
- Data deletion order.
- Administrative monetary penalty.
- Higher penalty for repeat violations.
- Higher penalty for deliberate ghost postings.
- Higher penalty for selling or transferring applicant data without consent.
- Temporary ban from public job boards.
- Loss of eligibility for public hiring subsidies.
- Loss of eligibility for government contracts.
- Public listing of serious violators.

Where applicant data has been sold, transferred, or used for unauthorized AI training, penalties should reflect the seriousness of the loss of control.

Once applicant data has entered external databases, data-broker systems, or AI training pipelines, the harm may be impossible to fully reverse.

## 24. Transparency Reports

Large employers, recruitment firms, and job platforms should publish annual transparency reports.

Reports should include:

- Number of job postings.
- Number of active vacancies.
- Number of talent pool postings.
- Number of evergreen postings.
- Number of conditional postings.
- Number of cancelled postings.
- Number of reposted roles.
- Number of roles filled.



- Average hiring timeline.
- Use of AI screening tools.
- Applicant data retention practices.
- Number of deletion requests.
- Number of complaints received.
- Number of confirmed deceptive postings.
- Number of postings removed for misrepresentation.
- Third-party data-sharing categories.

These reports would help applicants, governments, researchers, and regulators understand whether job postings reflect real employment opportunities.

## 25. Public Job Board Standards

Government-run or publicly funded job boards should meet the highest standard.

They should:

- Require job classification labels.
- Require compensation ranges.
- Require hiring timelines.
- Require applicant data notices.
- Remove expired postings.
- Flag reposted roles.
- Ban repeat ghost-job offenders.
- Prevent duplicate postings from distorting labour-market data.
- Publish aggregate statistics by job classification.
- Refuse postings that do not disclose applicant data practices.

A public job board should not become a public résumé-harvesting tool.

## 26. Special Rules for Recruiters and Staffing Agencies

Recruiters and staffing agencies must disclose whether they are hiring for:

- A specific employer.
- A confidential employer.
- A talent pool.
- A possible future contract.

- A general recruitment database.
- A role that is contingent on client approval.

If the employer is confidential, the recruiter must still disclose:

- Whether the vacancy is active.
- Whether the position is funded.
- Whether the client has authorized recruitment.
- Whether applicant data will be shared with one employer or many.
- How long the data will be retained.
- Whether the applicant will be contacted before being submitted to any employer.

Recruiters should not be allowed to collect résumés under the appearance of a specific job when no specific job exists.

## 27. Special Rules for Public-Sector Hiring

Public-sector employers should be required to disclose when a posting is:

- Open competition.
- Internal competition.
- External posting with internal candidate.
- Expression of interest.
- Talent inventory.
- Conditional on funding.
- Conditional on project approval.

Public-sector hiring should not invite external applicants into a process that is effectively predetermined without disclosure.

Where public-sector postings are used to satisfy procedural requirements, the posting should state that clearly.

## 28. Data Breach and Security Requirements

Applicant data must be protected with appropriate security safeguards.

Employers, platforms, recruiters, and vendors must protect applicant data against:

- Unauthorized access.

- Data scraping.
- Unapproved sharing.
- Employee misuse.
- Vendor misuse.
- Data breaches.
- Unsecured storage.
- Indefinite retention.
- Unauthorized AI training.
- Unauthorized transfer to third countries.

Applicants must be notified if their information is compromised.

Because job applications often contain enough information for identity theft, fraud, profiling, discrimination, and long-term employment harm, applicant data should be treated as sensitive personal information.

## 29. Deletion and Withdrawal Process

Every applicant must have access to a simple deletion and withdrawal process.

This process must allow the applicant to:

- Withdraw from the hiring process.
- Request deletion of application materials.
- Request deletion from a talent pool.
- Revoke consent for future use.
- Request a list of third parties who received the information.
- Request confirmation that deletion has occurred.

Deletion requests should be completed within a defined period, such as 30 days, unless a specific legal obligation requires retention.

If data cannot be deleted because it has already been transferred, anonymized, aggregated, or used in AI training, that must be disclosed to the applicant.

## 30. Anti-Retaliation Protection

Employers, recruiters, and platforms must not penalize, blacklist, or disadvantage applicants for:

- Asking whether a job is active.

- Asking how their data will be used.
- Refusing unrelated data consent.
- Requesting deletion.
- Filing a complaint.
- Reporting a suspected ghost job.
- Requesting human review of automated screening.

Applicants should not have to choose between privacy and employability.

### 31. Implementation Timeline

A phased implementation model could be used.

#### *Phase 1: Disclosure*

Require job classification labels, hiring timelines, compensation ranges, and applicant data notices.

#### *Phase 2: Retention and Consent*

Create standard retention limits, deletion rights, consent rules, and restrictions on secondary use.

#### *Phase 3: Platform Accountability*

Require job boards and platforms to verify postings, preserve records, remove misleading listings, and publish transparency reports.

#### *Phase 4: Enforcement and Audits*

Introduce penalties, audits, public reporting, and stricter rules for publicly funded employers.

### 32. Model Posting Disclosure

Every job posting should include a disclosure similar to the following:

**Job Status:** Active vacancy

**Hiring Timeline:** Applications close June 30. Interviews expected July 8–19. Hiring decision expected by July 31.

**Applicant Data Use:** Your application will be used only for this hiring process unless you separately consent to future consideration.

**Retention Period:** Unsuccessful applications will be deleted within 12 months.

**Third-Party Access:** Applications will be processed through [platform/vendor name]. Data will not be sold or used for AI training.

**Automated Screening:** Automated screening will / will not be used.

**Deletion Requests:** Applicants may request deletion by contacting [contact information].

### 33. Rationale

Job seekers are often required to submit detailed personal information before they know whether a job is real, whether hiring is active, or what will happen to their data.

This creates several harms.

First, ghost jobs waste applicant time and emotional energy. Applying for work is labour. It requires tailoring résumés, writing cover letters, preparing portfolios, completing forms, answering screening questions, and sometimes doing unpaid assessments. When the job does not exist, that labour has been extracted under false pretenses.

Second, ghost jobs distort the labour market. They can make it appear that employers are hiring when they are not. This can mislead workers, governments, schools, training providers, immigration planners, and economic development agencies.

Third, job applications contain valuable personal data. Résumés reveal employment history, education, location, skills, salary expectations, career movement, references, and sometimes sensitive personal information. Without clear rules, this data can be retained indefinitely, shared widely, sold, analyzed, or used to train automated systems.

Fourth, deceptive job postings can benefit employers and platforms while applicants carry the cost. Employers can test wages, build databases, signal growth, satisfy internal optics, or gather market intelligence. Platforms can increase listing volume and collect user data. Applicants receive little transparency in return.

A fair labour market requires honest job advertising.

A fair privacy system requires meaningful control over applicant data.

This framework recognizes that a job application is not just a document. It is a transfer of personal information, trust, time, and hope. That transfer should come with legal obligations.

### 34. Core Policy Statement

No employer, recruiter, platform, or third-party hiring service should advertise a job in a manner that misleads applicants about whether the job exists, whether hiring is active, or how applicant data will be collected, retained, used, shared, sold, or analyzed.

Job seekers deserve truth before they apply.

They deserve control over their data.

They deserve a labour market where advertised opportunities are not allowed to become traps for personal information.

---

### ***About the Author***

Lawrence Nault is a Canadian author, filmmaker, and independent researcher based in Alberta's Badlands and Rockies. He writes speculative fiction and YA fantasy, directs documentary film, hosts the podcast *Stone & Signal*, and publishes academic research and policy proposals on digital infrastructure, occupational health, and environmental governance. His work asks hard questions about ecology, technology, and what it means to be human.

#### **Contact**

[lawrencenault.me/contact/](http://lawrencenault.me/contact/)

#### **Website**

[lawrencenault.me](http://lawrencenault.me)

#### **Policy proposals**

[lawrencenault.me/policy/](http://lawrencenault.me/policy/)

#### **Research**

[lawrencenault.me/research-policy/](http://lawrencenault.me/research-policy/)

#### **Social**

Threads: [@mountainhermitauthor](https://www.threads.net/@mountainhermitauthor)

Bluesky: [@mountainhermit.bsky.social](https://bsky.app/profile/@mountainhermit.bsky.social)