The Right To Not Be Collected

A Privacy First framework for the data extraction age

July- 2026

DEMOCRATIC GOVERNANCE | 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.

Most people still talk about privacy as if the problem begins after data has been collected.

Was it stored securely?

Was it breached?

Was it shared without consent?

Was the privacy policy clear enough?

Those questions matter. But they are not the first question we should be asking.

The first question should be much simpler:

Why was anyone allowed to collect this data in the first place?

Personal data has become one of the central engines of modern power. It is used to profile us, price us, track us, sort us, target us, manipulate us, deny us, sell to us, scam us, and increasingly, to train systems that will make decisions about us long after we have forgotten we ever handed the information over.

That is the part too many laws still fail to address.

We are living under a data-first model. Businesses, platforms, employers, governments, landlords, insurers, schools, apps, devices, and service providers collect first, justify later, and protect only after the fact. Privacy becomes a setting, a policy link, a consent box, or a damage-control exercise after something goes wrong.

But once personal data exists, control has already been lost.

It can be copied, scraped, purchased, sold, inferred from, combined with other datasets, transferred across borders, accessed by governments, breached by criminals, or repurposed for technologies and uses that did not exist when it was collected.

And the people collecting it often understand its future value long before the rest of us understand the future risk.

That is why we need to reverse the model.

Not better consent boxes.

Not longer privacy policies.

Not another promise that our data will be kept safe after it has already been taken.

We need a Privacy First approach. A model that begins with restraint.

A model that treats personal data not as a corporate asset, government convenience, or inevitable byproduct of modern life, but as something powerful enough to damage freedom, dignity, fairness, safety, democracy, and personal autonomy.

The question should no longer be: How do we protect the data once it has been collected?

The question should be: Why was collection allowed at all?

What follows is a draft policy proposal for a Privacy First Act — a framework built around one simple principle:

The right is not only to protect personal data after it is taken. The right is not to be unnecessarily collected in the first place.

1. Purpose

The purpose of this policy is to reverse the current data-first approach to personal information and establish privacy as the default condition of participation in modern society.

Personal data is no longer a passive record of a person's interaction with a service. It has become a source of power. It can be used to profile, manipulate, scam, defraud, exclude, surveil, price-discriminate, train artificial intelligence systems, influence political behaviour, evaluate risk, limit access to services, and create permanent records that follow people across institutions, borders, platforms, employers, governments, and markets.

For decades, data collection carried natural limits. Storage was expensive. Processing was limited. Access was restricted. Most organizations collected what they needed because collecting everything was impractical.

That world no longer exists.

Today, personal data can be collected constantly, invisibly, cheaply, and at scale. It can be scraped, copied, purchased, inferred, combined with other datasets, transferred across borders, breached, subpoenaed, monetized, or repurposed for uses that did not exist when the data was first gathered.

The central failure of modern data law is that it often treats privacy as something to be protected after data has already been taken. This policy begins from the opposite position.

The question should not be: How do we protect the data once it has been collected?

The first question should be: Why was anyone allowed to collect it in the first place?

2. Core Principle

Privacy shall be the default.

No person, business, platform, employer, contractor, service provider, public body, government agency, institution, landlord, insurer, financial entity, educational body, health-related service provider, or data processor shall collect, retain, generate, infer, purchase, sell, share, transfer, or use personal data unless the collection or use is demonstrably necessary for a specific lawful purpose, proportionate to that purpose, limited to the minimum data required, and incapable of being reasonably achieved through less intrusive means.

Personal data shall not be collected merely because it is useful, profitable, convenient, customary, technologically possible, or potentially valuable in the future.

3. The Right Not To Be Collected

Every person shall have a right not to be unnecessarily collected, tracked, profiled, identified, recorded, inferred, analyzed, monetized, or subjected to data extraction as a condition of ordinary life.

Access to employment, housing, health care, education, public services, transportation, financial services, commerce, communication, legal services, social support, public spaces, or digital platforms shall not be made conditional on unnecessary personal data collection.

Privacy is not a luxury feature, a subscription option, a buried setting, or a right that exists only after a person has surrendered their information.

Privacy is a condition of freedom.

4. Definitions

For the purpose of this policy:

Personal data means any information, record, identifier, signal, image, sound, biometric marker, behavioural pattern, device marker, location trace, transaction record, communication record, health-related information, employment information, financial information, demographic information, or inferred information that identifies, relates to, describes, predicts, profiles, or can reasonably be associated with a person.

Inferred data means information created, predicted, derived, assumed, classified, scored, or generated about a person based on other data, including behavioural predictions, risk scores, eligibility scores, productivity scores, health assumptions, political assumptions, financial assumptions, purchasing likelihood, vulnerability indicators, or emotional state analysis.

Sensitive personal data includes, but is not limited to, health information, biometric data, precise location data, government identification, financial data, children's data, immigration or citizenship information, employment status, disability-related information, education records, legal records, sexual or intimate information, religious or political information, and data that may expose a person to discrimination, targeting, coercion, fraud, harassment, or exclusion.

Data collection includes direct collection, passive collection, purchase, scraping, recording, observation, tracking, device capture, form submission, account creation, background monitoring, third-party transfer, data matching, behavioural analysis, automated inference, or any other method by which personal data is acquired or generated.

Secondary use means any use of personal data beyond the specific purpose for which it was lawfully and expressly collected.

Data processor means any person, corporation, contractor, platform, public body, artificial intelligence system operator, vendor, broker, analytics provider, cloud provider, software provider, or other entity that collects, stores, accesses, analyzes, transfers, processes, infers from, or uses personal data on behalf of itself or another party.

5. Data Minimization as a Legal Requirement

All personal data collection shall be governed by the principle of strict minimization.

A collecting entity must prove that:

- The data is necessary for a specific lawful purpose.
- The same purpose cannot reasonably be achieved without collecting the data.
- Less intrusive data would not be sufficient.
- The amount of data collected is the minimum required.
- The data will be retained only for the minimum period required.
- The data will not be used for unrelated secondary purposes.
- The person affected can understand what is being collected and why.
- The collection does not create disproportionate future-use risk.

Where an entity cannot meet this standard, collection shall be prohibited.

6. Prohibited Data Practices

The following practices shall be prohibited unless expressly authorized by law and subject to independent oversight:

- Collecting personal data for speculative, undefined, future, or "service improvement" purposes that are not clearly necessary.
- Requiring personal data unrelated to the service being provided.
- Bundling unnecessary data collection into terms of service or employment conditions.
- Denying essential services because a person refuses unnecessary data collection.
- Using consent to justify collection where there is a clear power imbalance.
- Selling, licensing, renting, trading, or transferring personal data to third parties without a specific legal basis.
- Combining datasets to create profiles beyond the original purpose of collection.
- Using personal data for price discrimination without explicit disclosure and regulatory approval.
- Using behavioural data to manipulate vulnerability, addiction, fear, urgency, political belief, financial insecurity, or emotional state.
- Creating inferred profiles for eligibility, access, employment, insurance, credit, housing, health care, education, or public services without meaningful review and appeal.
- Scraping personal data from public or semi-public sources for profiling, resale, artificial intelligence training, or behavioural analysis.
- Collecting children's data for advertising, profiling, prediction, monetization, or future behavioural analysis.

- Using personal data collected for one purpose to train artificial intelligence systems without separate lawful authority.
- Retaining personal data after the original lawful purpose has ended.
- Transferring personal data into foreign jurisdictions where legal protections are weaker, unclear, or incompatible with the rights established under this policy.

7. Sensitive Data Protection

Sensitive personal data shall receive the highest level of protection.

Sensitive personal data may only be collected where it is strictly necessary, directly connected to the service or legal purpose, proportionate, time-limited, and subject to enhanced safeguards.

Entities collecting sensitive personal data must provide a clear explanation of:

- Why the data is required.
- What law or specific operational need authorizes collection.
- Who will access it.
- Where it will be stored.
- Whether it will leave the jurisdiction.
- How long it will be retained.
- Whether it will be shared, processed, inferred from, or used by automated systems.
- How the person can challenge collection or request deletion.
- What harm may result from breach, misuse, transfer, or future repurposing.

No sensitive personal data shall be used for advertising, behavioural manipulation, unrelated profiling, commercial resale, or artificial intelligence training unless expressly permitted by law and subject to independent public-interest review.

8. Future-Use Risk Assessment

Every collection of personal data shall be assessed not only according to its stated present purpose, but according to reasonably foreseeable future-use risks.

This assessment must consider:

- Whether the data could be combined with other datasets.
- Whether the data could be used to identify, track, or profile a person.
- Whether the data could expose a person to fraud, manipulation, discrimination, coercion, harassment, or exclusion.
- Whether the data could be transferred to another jurisdiction.

- Whether the data could be accessed by governments, law enforcement, foreign entities, data brokers, contractors, or unauthorized parties.
- Whether the data could be used to train artificial intelligence or automated decision systems.
- Whether future technologies could make the data more revealing than it appears at the time of collection.
- Whether retention of the data creates more risk than benefit.

Where future-use risk is high, collection shall be prohibited unless a compelling public interest can be demonstrated.

9. Consent Is Not Enough

Consent shall not be treated as valid where a person has no meaningful ability to refuse.

Consent shall not be sufficient where access to employment, housing, health care, education, public services, financial services, essential commerce, government services, transportation, or communication depends on accepting unnecessary data collection.

Consent shall not legalize collection that is unnecessary, disproportionate, deceptive, coercive, overly broad, bundled, or unrelated to the service being provided.

A person cannot meaningfully consent to unknown future uses, undisclosed data transfers, artificial intelligence training, behavioural profiling, or risks that are not clearly explained.

10. No Privacy Penalty

A person shall not be punished, charged more, denied access, placed in a slower service stream, refused employment, refused housing, or treated less favourably because they exercise their privacy rights.

Where a service can reasonably be provided with less data, a privacy-protective option must be available without additional cost, reduced quality, unreasonable delay, or exclusion.

Privacy shall not become a premium product available only to those who can afford it.

11. Ban on Unnecessary Identity Collection

Government-issued identification, health numbers, social insurance numbers, citizenship information, driver's licence information, biometric data, and similar identifiers shall not be collected unless specifically required by law or strictly necessary for the service being provided.

Where age, eligibility, residency, status, or identity must be confirmed, the least intrusive method shall be used.

For example:

- If age confirmation is sufficient, a birthdate shall not be collected.
- If residency confirmation is sufficient, full identity documents shall not be copied.
- If eligibility can be verified without retaining documents, documents shall not be retained.
- If a person can prove identity in person, no additional digital profile shall be created unless necessary.
- If a one-time verification is sufficient, permanent storage shall be prohibited.

12. Limits on Data Retention

Personal data shall not be retained indefinitely.

Every collecting entity must establish a fixed deletion schedule before collection occurs.

- Personal data shall be deleted when:
- The original purpose has been fulfilled.
- The legal retention period has expired.
- The person withdraws consent where consent is the legal basis.
- The data is no longer necessary.
- The data was collected unlawfully.

The future-use risk outweighs the need for retention.

Data retained "just in case," "for analytics," "for future development," "for service improvement," or "because it may become useful" shall be considered unlawfully retained unless a specific lawful purpose is proven.

13. Limits on Inferred Data

Inferred data shall be treated as personal data.

A person shall have the right to know when significant decisions or profiles are created using inferred data.

No person shall be denied employment, housing, credit, insurance, health care, education, public services, social support, financial services, or other significant opportunities based on inferred data without:

- Clear notice.
- Access to the basis of the inference.
- A meaningful explanation.

- The right to correct inaccurate information.
- The right to challenge the decision.
- Human review.
- Independent auditability.

Secret scoring systems shall not be used to determine access to essential services.

14. Artificial Intelligence and Automated Systems

Personal data shall not be used to train, tune, test, improve, or operate artificial intelligence systems unless the use is specifically authorized, necessary, proportionate, disclosed, and subject to meaningful oversight.

Publicly accessible data shall not be presumed to be freely available for artificial intelligence training.

The fact that information can be scraped, copied, or accessed does not mean it may lawfully be used.

Artificial intelligence systems that rely on personal data must be subject to:

- Data minimization requirements.
- Source documentation.
- Bias and harm assessment.
- Future-use risk assessment.
- Independent audit.
- Public reporting where public services are affected.
- Clear appeal rights where people are impacted.
- Deletion and correction mechanisms where feasible.

No artificial intelligence system shall be deployed in a way that requires broad, unnecessary, or involuntary personal data extraction from the public.

15. Children and Vulnerable Persons

Children's data shall not be collected for profiling, advertising, behavioural prediction, commercial manipulation, or future monetization.

Institutions serving children, seniors, patients, disabled persons, unhoused persons, people accessing social supports, workers in precarious employment, or other vulnerable groups shall be subject to heightened obligations.

A power imbalance shall be presumed where the person affected depends on the collecting entity for care, income, housing, education, safety, benefits, legal status, or essential services.

In these cases, consent alone shall not be sufficient.

16. Public Bodies and Government Data

Government bodies shall be held to the highest standard under this policy.

The state shall not collect, centralize, link, or repurpose personal data across programs unless expressly authorized by law, necessary for a defined public purpose, proportionate, publicly disclosed, independently reviewed, and subject to strict limits.

Government convenience shall not be treated as sufficient justification for mass data collection.

Public bodies shall not create centralized identity systems, cross-program databases, automated eligibility systems, or surveillance-linked service platforms without public notice, legislative authority, privacy impact assessment, and independent oversight.

Data collected for one public service shall not be used for unrelated enforcement, surveillance, eligibility reduction, immigration action, policing, debt collection, or benefit denial unless clearly authorized by law and subject to judicial or independent review.

17. Employers and Workplace Data

Employers shall not collect more personal data than is necessary to administer employment, safety, payroll, benefits, legal compliance, or legitimate workplace operations.

The following shall be prohibited unless strictly necessary and independently justified:

- Continuous worker surveillance.
- Keystroke logging.
- Productivity scoring unrelated to actual job requirements.
- Biometric monitoring.
- Location tracking beyond working necessity.
- Audio or video monitoring in non-public work areas.
- Emotional analysis or attention tracking.
- Health-related inferences unrelated to accommodation or safety.
- Automated discipline based on opaque scoring systems.
- Use of personal devices to collect workplace data without clear limits.

Workers shall have the right to know what data is collected, how it is used, who has access, and how long it is retained.

18. Data Brokers and Secondary Markets

The sale, resale, licensing, transfer, aggregation, or commercial exchange of personal data shall be prohibited unless specifically authorized by law and subject to strict oversight.

Data brokers shall not collect, purchase, scrape, infer, package, sell, or distribute personal data without a specific legal basis and clear rights for the person affected.

Every person shall have the right to know whether a data broker holds information about them, what information is held, where it came from, who it was sold to, and how to require deletion.

A public registry of data brokers shall be established.

Failure to register shall be an offence.

19. Transparency and Public Accountability

Entities collecting personal data must provide plain-language notice before collection.

This notice must state:

- What data is being collected.
- Why it is necessary.
- What less intrusive alternatives were considered.
- Whether collection is required by law or optional.
- Who will access the data.
- Whether it will be shared.
- Whether it will be transferred outside the jurisdiction.
- Whether it will be used for automated decision-making.
- Whether it will be used for artificial intelligence training.
- How long it will be retained.
- How the person can access, correct, challenge, or delete it.
- What consequences, if any, result from refusal.

Privacy notices shall not be buried in long terms of service, bundled consent forms, vague policies, or unreadable legal language.

20. Independent Privacy Impact Assessments

Before launching any program, system, device, platform, database, artificial intelligence tool, surveillance tool, public service integration, or large-scale data collection practice involving personal data, the collecting entity must complete a Privacy First Impact Assessment.

The assessment must determine:

- Whether the data is necessary.
- Whether the purpose can be achieved without collecting personal data.
- Whether less sensitive data can be used.
- Whether the data creates future-use risk.
- Whether the data will be linked to other datasets.
- Whether automated systems will use the data.
- Whether the data could be used against the person in future.
- Whether vulnerable people are affected.
- Whether a power imbalance exists.
- Whether deletion is possible and enforceable.
- Whether public reporting is required.
- Whether collection should be prohibited.

For public bodies and high-risk private systems, the assessment shall be filed with the privacy regulator and made public, with limited redactions only where strictly necessary for security or lawful confidentiality.

21. Right of Access, Correction, Deletion, and Explanation

Every person shall have the right to:

- Know what personal data is held about them.
- Know the source of that data.
- Know who has accessed it.
- Know who it has been shared with.
- Correct inaccurate data.
- Delete data that is unnecessary, expired, unlawfully collected, or no longer justified.
- Challenge inferred data.
- Receive a meaningful explanation of automated decisions.
- Object to secondary use.
- Withdraw consent where consent is the legal basis.
- Seek compensation for misuse, overcollection, breach, or unlawful retention.

These rights shall be easy to exercise and shall not require legal assistance, excessive fees, unnecessary identification, or unreasonable delay.

22. Enforcement

A Privacy First Commissioner shall be established or empowered to enforce this policy.

The Commissioner shall have authority to:

- Investigate complaints.
- Conduct audits.
- Order deletion of unlawfully collected data.
- Suspend data collection practices.
- Prohibit high-risk systems.
- Issue binding orders.
- Require public reporting.
- Impose administrative penalties.
- Refer serious violations for prosecution.
- Require compensation or remediation for affected persons.
- Audit artificial intelligence and automated decision systems.
- Inspect data broker activity.
- Require proof that collection is necessary.

The burden of proof shall rest on the collecting entity.

A person shall not be required to prove harm before unlawful collection can be stopped.

23. Penalties

Penalties shall be proportionate to the seriousness of the violation, the sensitivity of the data, the number of people affected, the financial benefit obtained, the degree of negligence or intent, and whether vulnerable persons were affected.

Penalties may include:

- Fines.
- Deletion orders.
- Suspension of data processing.
- Public notice requirements.
- Compensation to affected persons.
- Loss of public contracts.
- Loss of licences or regulatory approvals.
- Director and officer liability in cases of reckless or intentional misuse.
- Criminal penalties for knowing misuse, concealment, trafficking, or unlawful sale of sensitive personal data.

Repeated unlawful collection shall be treated as a serious offence.

24. Public Procurement Conditions

No public money shall be used to purchase, license, operate, subsidize, or support systems that violate Privacy First principles.

Any vendor seeking public contracts involving personal data must demonstrate:

- Data minimization.
- No unnecessary secondary use.
- No unauthorized artificial intelligence training.
- No undisclosed subcontracting.
- No foreign transfer without approval.
- No sale or commercial reuse of public data.
- Deletion at the end of the contract.
- Audit rights for the public body and privacy regulator.
- Compliance with this policy.

Public data shall not become a private asset.

25. Exceptions

This policy shall not prohibit necessary data collection for legitimate purposes, including health care, emergency response, legal compliance, public safety, fraud prevention, payroll, taxation, benefits administration, contractual performance, education administration, or other lawful and necessary purposes.

However, all exceptions must remain subject to necessity, proportionality, minimization, purpose limitation, retention limits, security safeguards, oversight, and future-use risk assessment.

An exception shall not become a loophole for broad data extraction.

26. Implementation

This policy should be implemented in stages.

Stage One: Public Sector Compliance

All government departments, agencies, Crown corporations, public schools, public health bodies, municipalities, and publicly funded programs shall complete data collection inventories and identify unnecessary collection, retention, sharing, and cross-program linkage.

Stage Two: High-Risk Private Sector Compliance

High-risk sectors, including finance, insurance, employment platforms, housing platforms, health-related services, education technology, data brokers, artificial intelligence firms, surveillance vendors, telecommunications, and large digital platforms shall be subject to mandatory Privacy First Impact Assessments.

Stage Three: General Data Minimization

All organizations collecting personal data shall be required to justify collection, reduce retention, eliminate unnecessary data fields, and provide privacy-protective alternatives.

Stage Four: Enforcement and Public Reporting

The Privacy First Commissioner shall publish annual reports identifying systemic risks, enforcement actions, high-risk sectors, data broker activity, artificial intelligence concerns, and recommendations for legislative updates.

27. Guiding Standard

The guiding standard of this policy is simple: If a person cannot reasonably participate in society without surrendering unnecessary personal data, then privacy has already failed.

A free society cannot be built on constant extraction.

A fair market cannot exist when people are profiled, scored, manipulated, and priced according to hidden data systems.

A democratic government cannot justify collecting more information than it needs merely because technology makes it possible.

A person should not have to become a dataset in order to work, learn, travel, shop, communicate, receive care, access benefits, rent a home, enter a building, use a service, or live an ordinary life.

Privacy First means collection is the exception.

The person is the starting point.

The burden belongs to the collector.

The right is not only to protect data after it is taken.

The right is not to be unnecessarily collected at all.

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/

Website
lawrencenault.me

Policy proposals
lawrencenault.me/policy/

Research
lawrencenault.me/research-policy/

Social
Threads: @mountainhermitauthor
Bluesky: @mountainhermit.bsky.social