

# The AI Upload Consent and Data Authority Act

July- 2026

## 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 day, people upload documents, artwork, manuscripts, contracts, school assignments, client files, images, and private records into online tools without knowing where those files go next.

Sometimes those tools are obvious AI systems. Sometimes they are not. They may be file converters, AI detectors, plagiarism checkers, résumé scanners, transcription tools, PDF editors, image enhancers, or workplace productivity platforms. But once a file is uploaded, control over that material may be lost.

This policy proposal is built around one simple principle:

If it is not yours, and you do not have permission or legal authority, you should not be able to upload it into an AI or AI-adjacent system.

The law should not require artists, writers, students, workers, clients, patients, businesses, or communities to prove exactly how much harm was caused after their work or private material was uploaded without consent. In many cases, that harm cannot be properly measured. The loss of control is the harm.

The AI Upload Consent and Data Authority Act is a proposal to create clear rules, visible warnings, meaningful consent, platform accountability, and enforceable consequences before people hand someone else's work or private documents to systems that may store, share, analyze, or train on them.

## Purpose

The purpose of this Act is to prevent individuals, companies, institutions, contractors, employees, students, clients, or third parties from uploading artwork, documents, images, writing, contracts, records, research, schoolwork, business files, personal files, or other protected material into artificial intelligence systems or AI-adjacent digital tools unless they have the legal ownership, consent, licence, employment authority, contractual authority, or copyright permission to do so.

This Act recognizes that many online tools now collect, process, retain, analyze, share, or use uploaded content in ways that are not obvious to the person uploading the file. These tools may include, but are not limited to:

- AI writing tools.
- AI image tools.
- AI detectors.
- Plagiarism checkers.
- File converters.
- OCR tools.
- PDF tools.
- Transcription tools.
- Résumé scanners.
- Contract-review tools.
- Image-enhancement tools.
- Cloud-based editing tools.
- Educational technology platforms.
- Business productivity tools.
- Any service that uses uploaded material to train, improve, fine-tune, evaluate, benchmark, or develop artificial intelligence systems.

The central principle is simple: No person should be allowed to upload someone else's work, private material, confidential document, copyrighted content, creative file, or personal data into an AI or AI-adjacent system unless they have clear lawful authority to do so.

## Core Requirement

Any digital service that allows users to upload files, documents, images, artwork, audio, video, code, writing, educational material, professional material, or other user-submitted content must provide a clear, visible, plain-language notice before upload.

This notice must not be hidden in the terms of service, privacy policy, footer, account settings, or secondary menu.

The notice must appear at the point of upload.

## Required Upload Warning

Before accepting an uploaded file, the service must display a warning substantially similar to the following:

- By uploading this file, you confirm that you own this material or have the legal authority, consent, licence, workplace authorization, contractual permission, or copyright permission required to upload it to this service.
- Do not upload artwork, documents, images, writing, contracts, records, private files, confidential files, schoolwork, professional work, or copyrighted material that you do not own or have authority to submit.
- Unauthorized uploading of protected, private, confidential, or copyrighted material may result in legal liability, penalties, civil claims, regulatory enforcement, or charges under applicable law.

The user must actively confirm this statement before the upload proceeds.

Pre-checked boxes, implied consent, passive acceptance, or blanket terms of service are not sufficient.

## Service Disclosure Requirements

Any service that accepts uploaded material must clearly disclose, before upload:

- Whether uploaded files are stored.
- How long uploaded files are retained.
- Whether uploaded files are reviewed by humans.
- Whether uploaded files are shared with third parties.
- Whether uploaded files are used to train, fine-tune, evaluate, improve, benchmark, or develop AI systems.
- Whether metadata is collected from uploaded files.
- Whether uploaded files may be used for product development.
- Whether uploaded files may be transferred outside the user's jurisdiction.
- Whether users can permanently delete uploaded files.
- Whether the service claims any licence over uploaded material.

These disclosures must be short, plain-language, and visible before upload.

A company may not rely only on a general terms of service agreement to obtain consent for AI training, model improvement, data sharing, or secondary use of uploaded content.

# Prohibited Conduct

It shall be prohibited for a person to knowingly upload material into an AI or AI-adjacent system if they do not have lawful authority to do so.

This includes, but is not limited to:

- Uploading an artist's work without permission.
- Uploading an author's unpublished manuscript without permission.
- Uploading a student's work without permission.
- Uploading a client's file without permission.
- Uploading an employee's work product outside authorized workplace use.
- Uploading a confidential business document without authority.
- Uploading legal, medical, financial, educational, or government records without authority.
- Uploading private family photos without consent from the appropriate rights holder.
- Uploading Indigenous cultural material, ceremonial material, community records, or traditional knowledge without proper community authority.
- Uploading copyrighted books, articles, images, music, scripts, photographs, designs, or other works without permission.
- Uploading documents obtained through employment, contracting, volunteering, caregiving, education, public service, or professional access for purposes not authorized by the owner, client, employer, institution, or rights holder.

# Duties of AI and Digital Tool Providers

Any service that accepts uploaded material must take reasonable steps to prevent misuse.

These duties include:

- Clear upload warnings.
- Plain-language data-use disclosures.
- Active uploader confirmation.
- Accessible deletion tools.
- A public policy on AI training use.
- A process for rights holders to report unauthorized uploads.
- A process for removal, deletion, and confirmation of deletion.
- Retention logs for uploaded files where legally appropriate.
- Audit records for high-risk or commercial services.
- Special protections for minors, students, patients, clients, employees, and vulnerable persons.
- Special protections for confidential, professional, legal, medical, educational, cultural, and government records.

Where a service uses uploaded material for AI training or model improvement, it must obtain specific, informed, opt-in consent from the lawful rights holder or authorized representative.

Consent from the uploader alone is not valid if the uploader does not own or control the uploaded material.

## No Hidden AI Training Consent

A company must not treat upload as automatic consent for AI training.

A company must not bury AI-training permission in a general terms of service.

A company must not use vague language such as "service improvement," "product development," "analytics," "quality assurance," or "machine learning enhancement" as a substitute for clear disclosure.

If uploaded material may be used to train, improve, test, evaluate, or develop an AI system, the service must say so plainly before upload.

## Rights Holder Remedies

Rights holders must have the right to:

- Request confirmation of whether their material was uploaded.
- Request deletion of unauthorized material.
- Request information about whether the material was used for AI training or model improvement.
- Request information about third-party sharing.
- File a regulatory complaint.
- Seek damages where harm has occurred.
- Seek penalties for repeated, commercial, reckless, or intentional misuse.
- Require platforms to preserve records where a legal claim is pending.

Where material has already been used for AI training, the service must be required to disclose what remedial steps are technically possible, what steps will be taken, and why any requested remedy cannot be fully completed.

## Enforcement

Enforcement under this Act should recognize that unauthorized uploading is not a minor or reversible act.

Once a document, image, artwork, manuscript, contract, record, private file, cultural material, school assignment, client file, business document, or creative work is uploaded into an AI or AI-adjacent system, the original rights holder may lose meaningful control over it.

The harm may not be easy to measure.

The harm may not be visible immediately.

The harm may not be monetized in any simple way.

The rights holder may never know whether the file was stored, copied, analyzed, shared, reviewed, transferred, used for AI training, used for product development, or retained in a dataset.

For that reason, enforcement should not depend only on proving financial loss, market damage, or malicious intent.

The unauthorized upload itself should be recognized as a legally significant harm.

## Strict Liability for Unauthorized Uploads

Where a person uploads protected, private, confidential, copyrighted, proprietary, cultural, professional, educational, medical, legal, employment, government, or personal material without lawful authority, the act of unauthorized upload should be sufficient to trigger liability.

The burden should not fall entirely on the rights holder to prove what happened after the upload.

The uploader should bear responsibility for confirming that they had the authority to upload the material before doing so.

Intent may still matter when determining the severity of penalties, but lack of malicious intent should not erase liability.

A person who uploads material without authority may be liable even if they did not understand the full consequences of the upload.

## Penalty Factors

Penalties should consider:

- Whether the uploaded material belonged to someone else.
- Whether the uploader had lawful authority.
- Whether the material was private, confidential, unpublished, sensitive, cultural, commercial, professional, educational, legal, medical, or personal.

- Whether the upload involved a minor, student, client, patient, employee, artist, author, contractor, Indigenous community, or vulnerable person.
- Whether the service used uploaded material for AI training, model improvement, product development, human review, sharing, resale, or third-party processing.
- Whether the uploader ignored a clear warning.
- Whether the uploader acted in a personal, institutional, professional, commercial, reckless, or repeated capacity.
- Whether the uploader gained or attempted to gain benefit from the upload.
- Whether the upload exposed the rights holder to privacy, reputational, professional, financial, creative, cultural, legal, or safety risks.
- Whether deletion, containment, or confirmation of non-use is possible.

## No Requirement to Prove Exact Monetary Harm

A rights holder should not be required to prove exact financial damage in order for the law to apply.

Many harms caused by unauthorized AI uploads cannot be properly monetized.

These may include:

- Loss of control over unpublished work.
- Loss of control over private records.
- Loss of control over confidential documents.
- Loss of control over cultural material.
- Loss of control over student work.
- Loss of control over client files.
- Loss of control over creative style, voice, image, likeness, or process.
- Loss of first-publication rights.
- Loss of trust.
- Loss of privacy.
- Loss of professional confidentiality.
- Loss of negotiating power.
- Risk of future misuse.
- Risk of model training or dataset retention.
- Risk of downstream copying.
- Risk of unknown third-party access.

Because these harms are difficult or impossible to calculate, the Act should allow statutory penalties, presumed damages, regulatory fines, deletion orders, audit orders, and other remedies without requiring the rights holder to prove a precise dollar value.

## Platform and Service Provider Liability

Services that accept uploads must not escape responsibility by saying the uploader clicked "agree."

Where a service accepts uploaded material, it must provide clear warnings, clear data-use disclosures, meaningful consent options, deletion mechanisms, and rights-holder complaint procedures.

If a service fails to clearly warn users that unauthorized uploading may be unlawful, fails to disclose retention or AI-training practices, or uses uploaded material beyond the lawful authority of the uploader, the service may also be liable.

Services should face heightened penalties where they:

- Hide AI-training permissions in terms of service.
- Use vague consent language.
- Retain uploaded material without clear disclosure.
- Use uploaded material for training without rights-holder consent.
- Share uploaded material with third parties without clear disclosure.
- Fail to delete unauthorized material when notified.
- Fail to maintain records of upload, retention, deletion, and use.
- Mislead users about whether uploaded material is stored, reviewed, or used.
- Rely on uploader consent when the uploader did not own or control the material.

## Required Remedies

Where unauthorized upload has occurred, regulators or courts should be able to order:

- Immediate deletion of the uploaded material.
- Confirmation of whether the material was stored, copied, reviewed, shared, or used for AI training.
- Disclosure of all third parties that received the material.
- Preservation of records for investigation.
- Deletion from active systems where technically possible.
- Removal from training datasets where technically possible.
- A statement explaining whether the material has already been used in model training or product development.
- A statement explaining what remediation is technically possible and what is not.
- Notice to affected rights holders.
- Administrative penalties.
- Statutory damages.
- Civil damages.

- Institutional discipline or professional consequences where appropriate.
- Procurement bans or licence restrictions for repeat-offending service providers.

## Aggravated Violations

Higher penalties should apply where unauthorized upload involves:

- Unpublished creative work.
- Confidential legal, medical, financial, educational, or employment records.
- Student work.
- A minor's personal information or creative work.
- Indigenous cultural material, community records, traditional knowledge, or ceremonial material.
- Private family photos or personal records.
- Trade secrets or proprietary business information.
- Client, patient, student, or employee files.
- Repeated conduct.
- Commercial use.
- Institutional use.
- Deceptive use.
- Retaliatory use.
- Malicious use.
- Upload after a clear warning.
- Upload into a system known to retain, share, or train on submitted material.

## Core Enforcement Principle

The law should not ask rights holders to prove the impossible.

Once unauthorized material enters an AI or AI-adjacent system, the damage may be unknown, untraceable, irreversible, or impossible to fully price.

Therefore, the law should treat unauthorized upload as the actionable harm.

Intent may affect the penalty.

But the absence of intent should not erase the violation.

## Public Institutions

Public institutions, schools, universities, libraries, health systems, courts, municipalities, police services, correctional systems, and government departments must not upload public records, student

records, patient records, legal records, government documents, Indigenous records, personal information, or copyrighted material into AI systems unless they have explicit legal authority and the service has been approved through a public procurement, privacy, security, and data-governance review.

Public institutions must maintain a public registry of approved AI and upload-based tools.

## Workplace Protections

Employers must clearly inform workers which AI tools are approved for workplace use.

Workers must not be required to upload client files, confidential documents, creative work, personal information, or copyrighted material into AI systems unless the employer has confirmed that the use is lawful, authorized, secure, and compliant with this Act.

Employees should not be personally liable for uploads made under direct employer instruction unless the employee knowingly violated the law or acted outside authorized duties.

Employers, contractors, vendors, and institutions should bear responsibility for the tools they require workers to use.

## Education Protections

Schools, colleges, universities, teachers, professors, administrators, and education technology vendors must not upload student work into AI detectors, grading tools, plagiarism tools, writing tools, or assessment systems unless students and, where appropriate, parents or guardians have been clearly informed of:

- What tool is being used.
- What data is uploaded.
- Whether the material is retained.
- Whether it is used for AI training.
- Whether it is shared with third parties.
- How long it is kept.
- How deletion can be requested.
- What alternatives exist.

Student work should not become training data simply because a school, teacher, or platform used an AI-related tool.

## Exceptions

This Act should not prevent lawful uses where proper authority exists.

Exceptions may include:

- Material uploaded by the copyright owner.
- Material uploaded with clear permission from the rights holder.
- Material uploaded under a valid licence.
- Material uploaded under a valid employment or institutional policy.
- Material uploaded under court order or statutory authority.
- Material uploaded for accessibility purposes where no data is retained or used for training.
- Material uploaded for security scanning where no secondary use occurs.
- Material uploaded for private personal use where the uploader owns the material or has lawful authority.
- Material in the public domain.
- Material covered by a lawful exception, provided the upload does not create unauthorized retention, sharing, commercial exploitation, or AI-training use.

## Guiding Principle

This Act is not intended to stop people from using technology.

It is intended to stop people, companies, schools, employers, institutions, and governments from quietly transferring other people's work, private records, confidential material, or copyrighted content into AI systems without consent, authority, or accountability.

The rule should be simple enough for everyone to understand:

If it is not yours, and you do not have permission or legal authority, you cannot upload it into AI.

---

### *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/](https://lawrencenault.me/contact/)

#### **Website**

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

#### **Policy proposals**

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