

Public Use of Camera-Capable Wearable Technology and Personal Data Protection 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/

The companion policy proposal, companion to this one, looked at what happens when businesses, public bodies, employers, contractors, institutions, and service providers use camera-capable wearable technology in places where people are asked to expose sensitive information.

This companion proposal looks at the other side of the same problem: ordinary individuals.

Smart glasses, body-worn cameras, wearable AI, and similar devices do not only create risks when they are used by staff behind a counter. They also create risks when they are worn by the person behind you in line, beside you in a waiting room, near you at a service desk, standing beside you at a payment terminal, or sitting across from you while your documents, screen, card, or ID are visible.

A person's private information does not become public simply because it is briefly exposed in a public or semi-public place.

This proposal starts from a simple principle: just because someone can wear a camera does not mean they should be allowed to record your life.

Your ID, bank card, health card, passport, phone screen, medical documents, legal papers, government forms, employment records, and private information should not become someone else's image file, AI input, searchable record, or social media post.

1. Purpose

The purpose of this policy is to protect individuals from the unauthorized capture, storage, sharing, analysis, upload, or misuse of sensitive personal information by private individuals using camera-capable wearable technology.

This policy is intended to apply where a person who is not acting on behalf of a business, employer, government body, public institution, contractor, or organization uses smart glasses, wearable cameras, body-worn devices, wearable AI systems, or similar technologies to capture another person's identity documents, payment cards, screens, records, forms, images, biometric information, or other sensitive information.

This policy recognizes that modern camera-capable wearable technology allows ordinary individuals to capture information that was previously difficult or impossible to record without being noticed.

The public should not be required to accept silent recording, background capture, concealed recording, or AI analysis of their sensitive information simply because camera technology has become small, wearable, and socially normalized.

2. Relationship to Companion Legislation

This policy is intended to operate alongside the Camera-Capable Wearable Technology and Sensitive Information Protection Act.

That companion policy focuses primarily on organizations, businesses, public bodies, employers, contractors, institutions, and controlled settings where people are required or expected to expose sensitive information.

This policy focuses on the conduct of private individuals, bystanders, patrons, visitors, customers, attendees, passengers, students, patients, applicants, observers, and members of the public who may use camera-capable wearable technology to capture another person's sensitive information.

Together, the two policies recognize that sensitive information can now be captured both by institutions and by ordinary individuals using increasingly powerful wearable technology.

Privacy protection must apply both to the organizations that require people to expose sensitive information and to the individuals who may exploit that exposure.

3. Core Principle

No person has the right to use wearable camera technology to capture another person's ID, bank card, credit card, health card, passport, document, phone screen, form, signature, face, biometric information, or other sensitive information without lawful authority or clear consent.

The fact that a person is in a public or semi-public place does not give others permission to capture, store, upload, analyze, or share their sensitive information.

A person's sensitive information does not become public simply because it is briefly visible.

4. Definition: Camera-Capable Wearable Technology

For the purposes of this policy, camera-capable wearable technology means any device worn on the body, face, head, clothing, uniform, helmet, eyewear, badge, lanyard, jewellery, or accessories that is capable of capturing, recording, storing, transmitting, analyzing, scanning, processing, or interpreting images, video, audio, biometric information, text, documents, screens, cards, or identifying information.

This includes, but is not limited to:

- Smart glasses.
- Camera-enabled eyewear.
- Body cameras.
- Wearable AI devices.
- Button cameras.
- Badge cameras.
- Head-mounted cameras.
- Augmented reality devices.
- Hidden wearable cameras.
- Camera-enabled accessories.
- Devices capable of facial recognition.
- Devices capable of text recognition.
- Devices capable of document capture.
- Devices capable of payment card capture.
- Devices capable of background image, video, or audio capture.
- Any similar device capable of recording, scanning, storing, transmitting, or analyzing information while worn by a person.

A device does not need to be actively recording to fall under this policy if it is technically capable of capturing, buffering, scanning, analyzing, storing, or transmitting information in the relevant setting.

5. Definition: Sensitive Personal Information

For the purposes of this policy, sensitive personal information means any information that could reasonably be used to identify, locate, track, impersonate, profile, discriminate against, financially harm, expose, exploit, intimidate, or target a person.

This includes, but is not limited to:

- Driver's licences.
- Health cards.
- Passports.
- Birth certificates.
- Citizenship or immigration documents.
- Social insurance numbers.
- Banking information.
- Credit cards.
- Debit cards.
- Security codes.
- Expiry dates.
- Signatures.
- Home addresses.
- Phone numbers.
- Email addresses.
- Medical documents.
- Legal documents.
- Employment documents.
- Student records.
- Government benefit documents.
- Tax documents.
- Insurance documents.
- Rental applications.
- Employment applications.
- Phone screens.
- Computer screens.
- Payment terminals.
- Login credentials.
- QR codes or barcodes connected to identity, payment, health, employment, education, government services, or access systems.
- Facial images connected to identity, health, employment, education, housing, income support, immigration, policing, or public services.
- Biometric information.

- Any document, card, screen, form, record, or image containing information that could reasonably be used for identity theft, fraud, stalking, discrimination, harassment, doxxing, surveillance, profiling, or exploitation.

6. Definition: Public and Semi-Public Spaces

For the purposes of this policy, public and semi-public spaces include places where members of the public, customers, clients, patients, students, tenants, passengers, voters, applicants, or service users may reasonably be present.

This includes, but is not limited to:

- Lineups.
- Waiting rooms.
- Bars.
- Restaurants.
- Clinics.
- Hospitals.
- Pharmacies.
- Schools.
- Colleges and universities.
- Government offices.
- Voting places.
- Banks.
- Airports.
- Transit stations.
- Buses, trains, taxis, rideshare vehicles, and other transportation settings.
- Courthouses.
- Libraries.
- Social service offices.
- Shelters.
- Employment centres.
- Landlord and tenant offices.
- Retail stores.
- Hotels.
- Service counters.
- Payment areas.
- Security checkpoints.
- Public events.

- Private businesses open to the public.
- Any place where people may be required or expected to present sensitive personal information.

7. Prohibited Capture of Sensitive Personal Information

No person may knowingly, recklessly, or negligently use camera-capable wearable technology to capture, record, scan, store, transmit, analyze, or share another person's sensitive personal information without lawful authority or clear consent.

This prohibition applies to:

- Recording another person's ID.
- Recording another person's bank card.
- Recording another person's credit card or debit card.
- Recording another person's health card.
- Recording another person's passport.
- Recording another person's documents.
- Recording another person's phone screen.
- Recording another person's computer screen.
- Recording another person's payment terminal.
- Recording another person's signature.
- Recording another person's medical, legal, employment, education, housing, immigration, or government documents.
- Recording another person's forms while they are being completed, reviewed, signed, submitted, or presented.
- Recording information that is briefly visible during a transaction, application, appointment, service interaction, or public process.

A person may violate this policy even if the sensitive information is only partially captured.

A person may also violate this policy if the information is captured incidentally but then stored, shared, reviewed, uploaded, analyzed, or used.

8. No Consent by Public Presence

A person does not consent to the capture of sensitive personal information simply by being present in a public or semi-public space.

A person does not consent to the capture of sensitive personal information by:

- Standing in a lineup.

- Sitting in a waiting room.
- Entering a business.
- Attending school.
- Visiting a clinic.
- Voting.
- Paying for goods or services.
- Showing ID to staff.
- Filling out a form.
- Using a payment terminal.
- Holding a document.
- Looking at a phone screen.
- Accessing social supports.
- Applying for employment.
- Seeking housing.
- Seeking medical care.
- Participating in a government process.

Sensitive information remains private even when it is briefly visible to others.

9. High-Risk Public and Semi-Public Settings

The use of camera-capable wearable technology by private individuals should be restricted or prohibited in high-risk settings where sensitive information is commonly exposed.

These settings include, but are not limited to:

- Lineups where IDs are checked.
- Waiting rooms where medical, legal, financial, or government documents are handled.
- Bars and clubs where IDs are presented.
- Clinics and hospitals.
- Pharmacies.
- Schools and child care settings.
- Government offices.
- Voting places.
- Banks and financial institutions.
- Airports and security checkpoints.
- Social service offices.
- Shelters and income support offices.
- Employment centres.

- Landlord and tenant offices.
- Payment counters.
- Any location where children, vulnerable people, victims, patients, or people accessing social supports may be present.

Restrictions may include requiring camera-capable wearable technology to be removed, turned off, covered, placed away, or kept out of sensitive information areas.

10. Protection of Children and Vulnerable Persons

Enhanced protections shall apply where camera-capable wearable technology is used to capture, record, scan, analyze, store, or share images or information involving:

- Children.
- Youth.
- Elderly people.
- Patients.
- Victims of crime.
- Survivors of abuse.
- People experiencing homelessness.
- People accessing social supports.
- People accessing food banks or shelters.
- People accessing disability supports.
- People receiving medical care.
- People receiving mental health care.
- People involved in legal, immigration, family, custody, or protection proceedings.
- People whose identity, location, health, status, or circumstances could expose them to harm.

Capturing sensitive personal information involving these individuals shall be treated as an aggravated violation unless clearly authorized by law or necessary to prevent immediate harm.

A person must not use camera-capable wearable technology to record a child's documents, face, location, school information, medical information, or identity information for posting, sharing, AI processing, surveillance, mockery, harassment, or personal use.

11. Recording Documents Held by Another Person

No person may use camera-capable wearable technology to record, photograph, scan, magnify, zoom in on, or otherwise capture documents, cards, screens, forms, or records being held, completed, reviewed, carried, displayed, or presented by another person without lawful authority or clear consent.

This includes documents held:

- In a person's hand.
- On a counter.
- At a service desk.
- At a payment terminal.
- In a waiting room.
- In a lineup.
- At a voting place.
- At a clinic.
- At a school.
- At a bank.
- At a government office.
- In a workplace.
- On public transportation.
- In any public or semi-public setting.

The fact that a document is momentarily visible does not make it available for capture.

12. Screens and Digital Displays

No person may use camera-capable wearable technology to capture, record, scan, store, transmit, or analyze another person's phone screen, laptop screen, tablet screen, payment screen, work screen, school screen, medical screen, government service screen, or other digital display where sensitive personal information may be visible.

This includes:

- Banking apps.
- Payment apps.
- Health apps.
- Government service portals.
- Employment applications.
- Housing applications.
- School portals.
- Medical records.
- Legal documents.
- Email or messaging apps.
- Login credentials.
- QR codes.

- Authentication codes.
- Two-factor authentication screens.
- Personal photos or documents.
- Any screen displaying sensitive personal information.

A person may violate this policy even if they claim the screen was visible in a public place.

13. Uploading to AI Tools, Cloud Services, or Third-Party Platforms

No person may upload, submit, process, analyze, store, or share another person's sensitive personal information through:

- Artificial intelligence tools.
- Chatbots.
- Image recognition tools.
- Facial recognition tools.
- Optical character recognition tools.
- Translation tools.
- Document conversion tools.
- Cloud storage services.
- Social media platforms.
- Data broker services.
- Background search tools.
- People-search services.
- Public databases.
- Private group chats.
- Messaging apps.
- Any third-party system that can retain, analyze, train on, share, or repurpose the information.

This prohibition applies whether the image, document, card, screen, or information was captured intentionally, incidentally, secretly, or in the background.

A person must not upload images of strangers' documents, cards, faces, screens, or personal information to AI tools for identification, translation, enhancement, amusement, analysis, profiling, or any other purpose without lawful authority or clear consent.

14. Bystander Liability

A person may be liable under this policy if they capture, store, share, upload, analyze, or distribute another person's sensitive personal information while acting as a bystander.

A bystander does not avoid responsibility by claiming they were not part of the business, organization, service, event, or transaction where the information was exposed.

Bystander liability may apply where a person:

- Records another person's ID in a lineup.
- Records another person's payment card at a counter.
- Records another person's documents in a waiting room.
- Records another person's phone screen on public transportation.
- Records a person accessing social supports.
- Records a person at a clinic, shelter, voting place, school, bank, government office, or legal proceeding.
- Shares or uploads another person's sensitive information after capturing it.
- Uses wearable technology to zoom in on documents, screens, cards, or forms held by another person.

The absence of a direct relationship between the person recording and the person recorded shall not be a defence.

15. Concealed Recording

Concealed recording of sensitive personal information by camera-capable wearable technology shall be treated as an aggravated violation.

Concealed recording includes:

- Wearing hidden cameras.
- Disabling recording indicators.
- Covering recording indicators.
- Using camera-capable devices designed to appear inactive.
- Using camera-capable devices designed to resemble ordinary eyewear, accessories, clothing, jewellery, or badges.
- Recording while claiming the device is not active.
- Using software that captures information in the background while the device appears inactive.
- Using zoom, enhancement, AI analysis, or OCR to extract information not clearly visible to the human eye.

Where concealed recording occurs, the capture shall be presumed intentional unless the person responsible can prove otherwise.

16. Recording Indicators and Device Transparency

No person may disable, conceal, bypass, suppress, alter, or interfere with a recording indicator on camera-capable wearable technology when used in public or semi-public spaces.

A recording indicator includes any light, sound, icon, screen notice, haptic alert, software notification, system message, or other signal intended to show that image, video, audio, biometric, document, or data capture is occurring.

It shall be a serious violation to:

- Disable a recording light.
- Cover a recording light.
- Modify software to suppress a recording notice.
- Use third-party tools to hide recording.
- Use hardware modifications to conceal recording.
- Use a device known to provide misleading recording indicators.
- Use a device that captures information in the background without clear notice.

Disabling or concealing recording indicators shall trigger enhanced penalties.

17. Passive, Background, or Undisclosed Capture

No person may use camera-capable wearable technology in a way that allows passive, background, or undisclosed capture of sensitive personal information in public or semi-public settings.

This includes devices or software that:

- Temporarily buffer images, video, or audio.
- Store pre-recording footage.
- Scan text, cards, faces, documents, or screens in the background.
- Upload images, video, audio, or metadata to cloud services.
- Create OCR outputs.
- Create facial templates.
- Create object recognition data.
- Create searchable records.
- Use “always-on,” “context awareness,” “memory,” “assistant,” “scene understanding,” or similar functions.
- Retain information after the user believes the device is inactive.

- Make sensitive information available to a device manufacturer, software provider, AI system, advertiser, analytics vendor, or third party.

A person may be liable if they knowingly use a device in a setting where such background capture is reasonably foreseeable.

18. Sharing, Publishing, or Redistributing Captured Information

No person may share, publish, post, sell, trade, forward, distribute, upload, or otherwise disclose another person's sensitive personal information captured through camera-capable wearable technology.

This includes sharing through:

- Social media.
- Messaging apps.
- Group chats.
- Email.
- Cloud folders.
- AI tools.
- Search tools.
- Data broker platforms.
- Employer systems.
- Public websites.
- Private forums.
- Law enforcement tip lines, unless reporting an immediate and lawful concern.
- Media outlets, unless protected by a clear public interest exception.

Sharing captured sensitive personal information shall be treated as a separate violation from the original capture.

Each further disclosure may create additional liability.

19. Public Interest and Safety Exceptions

This policy is not intended to prohibit lawful recording where necessary to document immediate danger, violence, abuse, police misconduct, public corruption, environmental harm, threats to safety, or other matters of clear public interest.

However, even where recording is justified for public interest or safety reasons, the person recording must take reasonable steps to avoid capturing or sharing unrelated sensitive personal information.

Where possible, sensitive information should be blurred, cropped, redacted, or excluded before any sharing.

The public interest exception does not allow the unnecessary capture, publication, upload, or AI processing of IDs, bank cards, health cards, documents, children's information, medical information, immigration information, or other sensitive personal information unrelated to the public interest matter being documented.

20. Right to Object and Request Cessation

A person has the right to ask another individual to stop using camera-capable wearable technology where their sensitive personal information is visible or at risk of capture.

A person may ask that the device be:

- Turned away.
- Removed.
- Covered.
- Turned off.
- Placed away.
- Kept at a distance.
- Disabled for the duration of the sensitive interaction.

A refusal to comply may be considered evidence of intentional or reckless conduct where sensitive personal information is captured.

No person may threaten, harass, intimidate, retaliate against, or mock another person for objecting to the use of camera-capable wearable technology near sensitive personal information.

21. Civil Remedies

A person whose sensitive personal information is captured, stored, shared, uploaded, analyzed, or misused in violation of this policy may seek civil remedies.

Remedies may include:

- Statutory damages without requiring proof of financial loss.
- Compensation for actual financial loss.
- Compensation for emotional distress.
- Compensation for identity theft risk.
- Compensation for reputational harm.

- Compensation for safety risk.
- Injunctions preventing further use or disclosure.
- Orders requiring deletion.
- Orders requiring confirmation of deletion.
- Orders requiring removal from online platforms.
- Orders prohibiting further contact.
- Recovery of legal costs.
- Enhanced damages for intentional, concealed, repeated, exploitative, discriminatory, or AI-related misuse.

The absence of proven financial loss shall not prevent recovery.

Unauthorized capture of sensitive personal information is itself a harm.

22. Enhanced Penalties

Enhanced penalties shall apply where the violation involves:

- Children.
- Vulnerable people.
- Patients.
- Victims of crime.
- Survivors of abuse.
- People accessing social supports.
- People accessing shelters.
- People receiving medical care.
- People participating in legal proceedings.
- People voting.
- People showing government documents.
- People exposing banking or payment information.
- Concealed recording.
- Disabled recording indicators.
- Background capture.
- AI processing.
- Facial recognition.
- Uploading to third-party platforms.
- Public posting.
- Doxxing.
- Harassment.

- Discrimination.
- Identity theft.
- Fraud.
- Repeated conduct.
- Commercial exploitation.

Enhanced penalties may include higher statutory damages, punitive damages, device seizure where authorized by law, restrictions on future use of camera-capable wearable technology, and referral for criminal investigation where applicable.

23. Platform and AI Tool Duties

Platforms, AI tools, cloud services, and image-processing services should be required to provide a process for individuals to report the unauthorized upload or processing of sensitive personal information captured through camera-capable wearable technology.

Where a platform or AI tool receives notice that uploaded content contains another person's sensitive personal information captured without consent, it must take reasonable steps to:

- Remove the content.
- Stop further distribution.
- Prevent indexing.
- Prevent use for AI training.
- Prevent use for facial recognition.
- Prevent use for OCR or document analysis.
- Preserve evidence where required for legal process.
- Provide a reporting pathway for the affected person.

Repeated failure by platforms to respond to such reports may create regulatory liability.

24. Education and Public Awareness

Governments should establish public education campaigns explaining that camera-capable wearable technology creates privacy risks beyond ordinary photography.

Public education should explain:

- Sensitive information remains private even when briefly visible.
- Recording another person's ID, bank card, documents, or screen can cause serious harm.
- Smart glasses and wearable AI may capture more than the wearer realizes.
- Uploading images of strangers' documents or faces to AI tools can create lasting harm.
- Recording indicators may not be enough.

- People have the right to object when sensitive information is at risk.
- Children, patients, victims, and vulnerable people require heightened protection.

25. Review and Updating

Because camera-capable wearable technology, AI systems, biometric tools, and image-processing software are changing rapidly, this policy must be reviewed at least every two years.

The review must consider:

- New smart glasses.
- Wearable AI devices.
- Facial recognition systems.
- Document scanning tools.
- Payment card capture risks.
- Background recording functions.
- AI memory systems.
- Social media practices.
- Platform enforcement.
- Privacy commissioner findings.
- Civil claims.
- Public complaints.
- Whether penalties are sufficient to deter violations.

26. Plain-Language Summary

This policy is based on a simple idea:

Just because someone can wear a camera does not mean they should be allowed to record your life.

Your ID, bank card, health card, passport, phone screen, medical documents, legal papers, government forms, employment records, and private information do not become public property because they are briefly visible in a lineup, waiting room, clinic, school, bank, government office, bar, airport, or payment area.

Smart glasses, body-worn cameras, wearable AI, and similar devices make it easier for ordinary people to capture sensitive information without being noticed.

That does not make it acceptable.

Privacy law must recognize that harm can come not only from institutions collecting data, but also from individuals capturing, sharing, uploading, or exploiting the sensitive information of strangers.

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

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