

Camera-Capable Wearable Technology and Sensitive Information 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/

Smart glasses, body cameras, wearable AI devices, and similar technologies are changing what it means to hand someone, or even just show, your ID, bank card, credit card, health card, or private documents.

This is no longer just a question of whether a business scans your information. It is also a question of who may be silently recording it, where that data goes, whether software is capturing images in the background, and whether the public has any meaningful way to know.

The Camera-Capable Wearable Technology and Sensitive Information Protection Act is a proposed policy standard for places where people are asked to expose sensitive information. Bars, banks, clinics, hotels, government offices, hiring desks, schools, service counters, and payment terminals all create moments where private data can be captured in seconds.

This proposal starts from a simple principle: if an organization requires you to show sensitive information, it has a duty to protect that information from unnecessary recording, whether by staff, contractors, wearable devices, background software, or nearby third parties.

Privacy cannot depend on whether someone notices a tiny light on a pair of glasses.

1. Purpose

The purpose of this policy is to protect members of the public from the unauthorized capture, storage, transmission, sale, analysis, or misuse of personal, financial, medical, immigration, identity, or other sensitive information through camera-capable wearable technology.

This policy applies in situations where a person, employee, contractor, agent, volunteer, security worker, doorman, server, cashier, receptionist, clerk, inspector, service provider, or representative is handling, viewing, scanning, verifying, accepting, processing, or standing in viewing proximity of sensitive documents, identity cards, payment cards, or other records.

The policy recognizes that modern camera technology, including smart glasses and similar devices, may allow images, video, audio, biometric information, payment information, and document information to be captured without the clear awareness or consent of the person whose information is exposed.

2. Core Principle

No person should be required to expose identification, banking information, credit card information, debit card information, medical information, immigration status, citizenship status, address information, employment records, or other sensitive personal data to an individual wearing camera-capable technology unless strict privacy safeguards are in place.

Public access to services, venues, employment, housing, health care, education, transportation, retail transactions, financial transactions, or government services must not depend on a person accepting unnecessary visual or audio recording of their sensitive information.

The public should not have to guess whether their ID, health card, citizenship status, bank card, private documents, signature, address, or financial information is being silently recorded.

3. 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, badge, helmet, lanyard, eyewear, or accessories that is capable of capturing, recording, storing, transmitting, analyzing, scanning, processing, or interpreting images, video, audio, biometric information, text, documents, payment information, or identifying information.

This includes, but is not limited to:

- Smart glasses.
- Camera-enabled eyewear.
- Body cameras.
- Button cameras.

- Badge cameras.
- Wearable AI devices.
- Head-mounted cameras.
- Augmented reality devices.
- Devices capable of facial recognition.
- Devices capable of text recognition.
- Devices capable of document capture.
- Devices capable of payment card capture.
- Devices capable of biometric analysis.
- Devices capable of background image, video, or audio capture.
- Any similar device capable of visual, audio, biometric, or document recording, whether visible or concealed.

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

4. Definition: Sensitive Information

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

This includes, but is not limited to:

- Driver's licence numbers.
- Health card numbers.
- Citizenship status.
- Immigration status.
- Passport information.
- Birth certificates.
- Social insurance numbers.
- Banking information.
- Credit card numbers.
- Debit card numbers.
- Security codes.
- Expiry dates.
- Signatures.
- Home addresses.
- Phone numbers.

- Email addresses.
- Employment records.
- Medical information.
- Insurance information.
- Student records.
- Legal documents.
- Tax documents.
- Government benefit documents.
- Facial images connected to identity documents.
- Licence plates.
- Access cards.
- Security badges.
- Login credentials.
- QR codes or barcodes connected to identity, payment, access, health, employment, education, or government records.
- Any document, card, form, record, screen, or image containing information that could be used for identity theft, financial fraud, stalking, discrimination, unauthorized surveillance, profiling, impersonation, harassment, or targeted exploitation.

5. Clarifying “Misuse”

For the purposes of this policy, misuse means any collection, capture, retention, copying, transmission, analysis, sale, sharing, indexing, scanning, profiling, or use of sensitive information beyond what is strictly necessary for the immediate purpose for which the information was provided.

Misuse includes, but is not limited to:

- Capturing an image of a person’s ID without clear lawful authority.
- Recording payment cards during a transaction.
- Capturing medical, legal, government, financial, housing, or employment documents without lawful authority.
- Capturing documents for personal, business, training, marketing, surveillance, analytics, or AI-related purposes.
- Storing images or video of sensitive documents after the immediate transaction is complete.
- Uploading captured information to third-party platforms, cloud services, AI tools, facial recognition tools, analytics systems, or data brokers.
- Sharing captured information with employers, contractors, advertisers, insurers, landlords, law enforcement, political organizations, or other third parties without lawful authority.

- Using captured information to profile a person's citizenship, health status, age, disability, income, address, employment status, race, ethnicity, religion, gender, immigration status, political activity, financial status, or other personal characteristics.
- Using captured information for harassment, fraud, blackmail, intimidation, discrimination, doxxing, identity theft, financial theft, commercial targeting, or surveillance.

Misuse does not require proof that harm has already occurred. Unauthorized capture, retention, transmission, or analysis of sensitive information is itself a privacy harm.

6. Prohibited Use in Sensitive Information Settings

A person may not wear or operate camera-capable wearable technology while handling, inspecting, viewing, verifying, accepting, processing, or standing in close viewing proximity to sensitive information unless the device is:

- Required by law or public safety regulation.
- Clearly disclosed to the person whose information is visible.
- Necessary for the specific service being provided.
- Subject to strict retention, deletion, access, and audit controls.
- Incapable of storing or transmitting sensitive information beyond the immediate lawful purpose.
- Configured to prevent background image, video, audio, biometric, text, or document capture.
- Subject to meaningful oversight by the organization responsible for its use.

Where these conditions are not met, the device must be removed, turned off, covered, disabled, stored away, or replaced with a non-recording alternative before the person's sensitive information is presented.

7. Viewing Proximity Standard

This policy applies not only when a person directly handles sensitive information, but also when they are in viewing proximity of it.

A person is in viewing proximity when they are close enough that a camera-capable device could reasonably capture, magnify, scan, record, buffer, transmit, or process information from:

- An ID card.
- A driver's licence.
- A health card.
- A passport.
- A credit card.

- A debit card.
- A phone screen.
- A paper document.
- A payment terminal.
- A government form.
- A medical document.
- A legal document.
- A customer file.
- A personnel file.
- A student file.
- A delivery record.
- A rental application.
- An employment application.
- A benefits application.
- Any document containing sensitive information.

This applies even if the person claims they did not personally look at the information.

If a camera-capable device could capture the information, the duty exists.

8. Business and Employer Duties

Any business, public body, non-profit, contractor, venue, institution, or organization whose workers interact with sensitive information must establish a written policy governing camera-capable wearable technology.

That policy must include:

- A ban on personal smart glasses or similar recording devices in sensitive information areas.
- Clear signage where recording-capable devices are used.
- A requirement that customers, clients, patients, students, applicants, tenants, employees, or members of the public be informed before sensitive information is exposed.
- A non-recording alternative for identity verification or payment processing.
- A process for immediate complaint and review.
- A requirement to delete any unauthorized capture immediately.
- A requirement to report privacy breaches to the affected person and the appropriate privacy authority.
- Disciplinary consequences for employees or contractors who violate the policy.
- A ban on using captured sensitive information for AI training, facial recognition, marketing, analytics, profiling, resale, or unrelated business purposes.

- A requirement that workers be trained on the privacy risks of wearable camera technology.
- A requirement that managers actively enforce the policy.

Employers may not avoid responsibility by claiming that a device belonged to a worker personally.

If a business allows, ignores, encourages, or fails to prevent the use of camera-capable wearable technology in sensitive information settings, the business is responsible for resulting privacy violations.

9. No Consent by Entry

Consent must not be assumed simply because a person enters a venue, store, office, workplace, school, clinic, hotel, bar, restaurant, government office, event, service counter, or public facility.

General signage stating “recording may occur” is not sufficient consent for the capture of IDs, payment cards, medical documents, immigration documents, banking documents, employment documents, legal documents, or other sensitive information.

Consent must be specific, informed, voluntary, and connected to the immediate purpose for which the information is being provided.

A person must be told when camera-capable wearable technology is being used before they are asked to expose sensitive information.

10. Right to a Non-Recording Alternative

A person must have the right to request that camera-capable wearable technology be removed, disabled, covered, turned away, placed out of view, or replaced before they present sensitive information.

A person must not be denied service, entry, employment consideration, housing consideration, medical assistance, education access, public service access, financial service access, or the ability to complete a lawful transaction solely because they object to unnecessary recording or potential recording of their sensitive information.

Exceptions may apply only where recording is specifically required by law, court order, or established public safety regulation.

Third-Party Recording Risk in Sensitive Information Areas

Where an organization requires, requests, or permits a person to expose sensitive information, the organization has a duty to take reasonable steps to prevent unauthorized capture of that information by third parties present in the same area.

This includes other customers, patrons, visitors, applicants, patients, students, tenants, contractors, bystanders, delivery workers, service providers, or members of the public who are wearing or using camera-capable technology.

An organization must not treat the risk of third-party recording as outside its responsibility where the organization has created, required, or controlled the setting in which sensitive information is exposed.

Organizations must establish privacy-protected areas for the handling, viewing, scanning, verification, payment, signing, or presentation of sensitive information. These areas must be designed or managed to reduce the risk that sensitive information can be captured by unrelated individuals.

Reasonable safeguards may include:

- Positioning service counters so IDs, payment cards, documents, and screens are not visible to others.
- Providing privacy screens, document shields, or payment shields.
- Creating separate verification areas.
- Creating distance between lineups and counters where sensitive information is handled.
- Prohibiting camera-capable wearable technology in sensitive information zones.
- Requiring smart glasses or similar devices to be removed, covered, turned away, or disabled before entering sensitive information areas.
- Allowing people to request a more private location before presenting sensitive documents.
- Training staff to recognize and respond when third parties may be recording sensitive information.
- Posting clear notices that recording IDs, payment cards, documents, screens, signatures, or another person's sensitive information is prohibited.

Where a person reports that another individual may be using camera-capable technology to capture sensitive information, the organization must take reasonable steps to respond immediately. This may include pausing the transaction, shielding the information, moving the person to a private area, asking the third party to stop recording, requiring the third party to move away, or refusing service to a person who continues to create a privacy risk.

An organization shall not be liable for every unforeseeable act by an unrelated person, but it may be liable where the risk was reasonably foreseeable and no meaningful safeguards were provided.

The presence of camera-capable wearable technology in an area where sensitive information is routinely exposed shall be considered a foreseeable privacy risk.

11. High-Risk Settings

This policy should apply with heightened restrictions in settings where sensitive information is commonly exposed.

These include, but are not limited to:

- Bars, clubs, and age-restricted venues checking ID.
- Liquor and cannabis retailers.
- Hotels and short-term rentals.
- Banks and financial institutions.
- Government service offices.
- Medical clinics and hospitals.
- Pharmacies.
- Schools and post-secondary institutions.
- Child care facilities.
- Employment and hiring offices.
- Landlord and tenant offices.
- Car rental agencies.
- Insurance offices.
- Courthouses and legal offices.
- Security checkpoints.
- Retail counters where payment cards are handled.
- Restaurants, bars, and service counters where payment cards are handed to staff.
- Delivery and courier services handling identity or signature documents.
- Public benefits offices.
- Immigration, citizenship, and licensing offices.
- Any workplace where customer, client, patient, student, employee, or applicant records are visible.

In high-risk settings, camera-capable wearable technology should be prohibited unless expressly authorized, necessary, disclosed, and subject to strict oversight.

12. AI, Facial Recognition, and Automated Analysis Ban

Sensitive information captured through camera-capable wearable technology must not be processed through:

- Artificial intelligence systems.
- Facial recognition tools.
- Optical character recognition systems.
- Biometric identification systems.

- Behavioural profiling systems.
- Marketing analytics systems.
- Customer scoring systems.
- Employment screening systems.
- Immigration or citizenship profiling tools.
- Insurance risk tools.
- Predictive policing systems.
- Automated decision-making systems.
- Law enforcement databases, unless required by law.

No sensitive information captured in these settings may be used to train, fine-tune, test, improve, evaluate, or develop AI systems.

The prohibition applies even where the information was captured incidentally, temporarily, passively, or unintentionally.

13. Data Retention and Deletion

Where recording is legally permitted and necessary, only the minimum amount of information required may be captured.

Organizations must establish:

- A clear retention period.
- A deletion schedule.
- Access logs.
- Encryption requirements.
- Limits on who may view the data.
- A ban on copying data to personal devices.
- A ban on uploading data to unauthorized third-party services.
- A process for affected individuals to request access, correction, and deletion.
- A process to verify that deletion has occurred.
- A process to report unauthorized access, capture, transmission, or retention.

Unauthorized recordings must be deleted immediately, but deletion does not erase the violation.

The fact that data was later deleted does not remove responsibility for the original unauthorized capture.

14. Personal Devices

Employees, contractors, security staff, venue staff, delivery workers, clerks, servers, cashiers, receptionists, inspectors, health workers, government workers, and other workers must not use personal camera-capable wearable technology while performing duties that involve sensitive information.

This includes personal smart glasses, body cameras, wearable AI devices, camera-enabled earbuds, hidden cameras, and any other recording-capable device worn on the body.

Employers may not avoid responsibility by claiming the device was not owned, issued, or controlled by the organization.

If a worker uses a personal device in a sensitive information setting, the worker may be personally liable and the organization may also be liable if it failed to prevent or address the conduct.

15. Public Notice Requirement

Where camera-capable wearable technology is used in a setting open to the public, the organization must provide clear notice before sensitive information is requested.

The notice must state:

- What device is being used.
- Whether it can record.
- Whether it is recording.
- Whether it can capture information in the background.
- What information may be captured.
- Why the capture is necessary.
- How long the information will be retained.
- Who can access it.
- Whether it will be shared with any third party.
- Whether it will be processed by AI, facial recognition, OCR, analytics, or cloud services.
- How the person may request a non-recording alternative.

A small indicator light, icon, sound, or manufacturer-provided signal is not sufficient notice.

16. Tampering With, Disabling, or Concealing Recording Indicators

Any person, business, employer, contractor, device manufacturer, software provider, or third-party service provider who disables, removes, covers, alters, bypasses, masks, suppresses, or otherwise interferes with a recording indicator on camera-capable wearable technology shall be subject to enhanced penalties.

For the purposes of this policy, a recording indicator includes any light, sound, icon, screen notice, haptic alert, software notification, system message, device signal, or other feature intended to notify nearby people that image, video, audio, biometric, document, or data capture is occurring.

It shall be a serious violation to:

- Disable a recording light.
- Cover or obscure a recording light.
- Modify software to prevent a recording indicator from activating.
- Use third-party software to suppress a recording notice.
- Use hardware modifications to conceal recording.
- Use a device whose recording indicator is known to be inaccurate, unreliable, disabled, or misleading.
- Market, sell, distribute, or promote tools designed to defeat recording indicators.
- Require, encourage, or knowingly permit workers to use devices with disabled or concealed recording indicators.
- Continue using a device after becoming aware that its recording indicators are inaccurate, unreliable, disabled, concealed, or misleading.

Where a recording indicator has been disabled, concealed, bypassed, suppressed, or made misleading, any recording or capture of sensitive information shall be presumed to be intentional unless the person or organization responsible can prove otherwise.

Penalties for this violation shall be significantly higher than ordinary privacy violations and may include:

- Mandatory breach notification to all affected individuals.
- Statutory damages without requiring proof of financial loss.
- Administrative fines against both the individual operator and the responsible organization.
- Suspension or cancellation of business, security, liquor, cannabis, professional, or operating licences where applicable.
- Civil liability for any resulting harm.
- Personal liability for managers or supervisors who authorized, ignored, or failed to prevent the conduct.
- Prohibition from using camera-capable wearable technology in sensitive information settings.
- Referral for criminal investigation where fraud, identity theft, stalking, harassment, extortion, voyeurism, blackmail, or intentional concealment is involved.

A manufacturer's default design, software setting, or device limitation shall not be a defence if the organization knowingly deploys the device in a setting where sensitive information is likely to be visible.

17. Passive, Background, or Undisclosed Capture by Device Systems or Software

No camera-capable wearable technology, software system, operating system, application, cloud service, artificial intelligence tool, analytics platform, or third-party service may capture, buffer, store, transmit, analyze, index, scan, interpret, or retain images, video, audio, biometric information, payment information, text, or document information from sensitive information settings unless the operator has knowingly activated recording and the affected person has been provided with clear notice where required by this policy.

This clause applies even where the human operator did not manually press record.

A system shall be considered to have captured information if it:

- Temporarily buffers images, video, or audio.
- Stores pre-recording footage.
- Captures images for AI analysis.
- Scans text, numbers, faces, cards, documents, screens, barcodes, QR codes, or payment terminals in the background.
- Uploads visual, audio, biometric, text, or document data to a cloud service.
- Creates thumbnails, metadata, transcripts, OCR outputs, facial templates, object recognition data, searchable records, or machine-readable records.
- Uses “always-on,” “wake-word,” “context awareness,” “scene understanding,” “memory,” “assistant,” “safety,” “quality improvement,” or similar features to process information in the background.
- Retains information after the operator believes the device is inactive.
- Makes sensitive information available to the device manufacturer, software provider, employer, advertiser, AI model, analytics vendor, or any third party.

The fact that the operator did not knowingly activate recording shall not excuse the business, employer, manufacturer, software provider, or service provider if the device or system was designed, configured, or permitted to capture information in the background.

Any device or software used in sensitive information settings must be configured so that:

- Recording is off by default.
- Background image, video, audio, biometric, OCR, and AI processing are disabled.
- Pre-recording buffers are disabled.

- Cloud syncing is disabled unless legally required and disclosed.
- No sensitive information is retained without express lawful authority.
- The operator and affected person can clearly determine when capture is occurring.
- The device cannot silently collect sensitive information while appearing inactive.
- The device cannot process sensitive information through AI, OCR, facial recognition, biometric analysis, or analytics tools without lawful authority and clear notice.

A violation of this clause shall be treated as a serious privacy breach, whether or not the captured information was later viewed by a human being.

Enhanced penalties shall apply where a manufacturer, software provider, employer, or organization knew or ought to have known that the technology could capture sensitive information without active recording by the operator.

18. Manufacturer and Software Provider Responsibility

Manufacturers, software providers, app developers, cloud service providers, AI system providers, and third-party technology vendors must not design, sell, license, deploy, or enable camera-capable wearable technology for use in sensitive information settings unless the technology includes meaningful privacy protections.

These protections must include:

- Recording indicators that cannot be disabled by ordinary users.
- Clear notice when recording, capture, scanning, buffering, or AI processing is occurring.
- Default settings that prevent background capture.
- Controls to disable cloud uploads.
- Controls to disable AI analysis.
- Controls to disable OCR and document scanning.
- Audit logs where capture is legally permitted.
- Security protections against unauthorized access.
- Clear documentation of what the device captures, stores, transmits, or analyzes.
- A means for organizations to verify that recording and background capture features are disabled.

A manufacturer or software provider may be liable where its design, default settings, marketing, or lack of safeguards makes unauthorized capture of sensitive information reasonably foreseeable.

19. Anti-Retaliation Clause

No person may be punished, refused service, removed, reported, denied entry, denied employment consideration, denied housing consideration, denied medical assistance, denied education access,

denied government service, or treated adversely for asking that camera-capable technology not be used while their sensitive information is visible.

A person may also not be punished for asking whether a device is recording, whether it can record, whether it captures information in the background, whether information is stored, or whether a non-recording alternative is available.

20. Public Sector Standard

Government bodies and publicly funded organizations must meet the highest standard under this policy.

No public body may require a person to expose sensitive documents to camera-capable wearable technology unless the collection is expressly authorized, necessary, proportionate, disclosed, and subject to independent privacy oversight.

Public bodies must also ensure that contractors, security firms, service providers, technology vendors, and third-party operators comply with this policy.

Public bodies must not use camera-capable wearable technology to capture, analyze, or retain information related to citizenship, immigration status, health status, disability, income support, employment status, education status, housing status, or identity documents unless expressly authorized by law.

21. Enforcement

Violations may result in:

- Mandatory deletion of captured information.
- Written notice to affected individuals.
- Mandatory breach reporting.
- Administrative fines.
- Statutory damages without requiring proof of financial loss.
- Suspension of licences or permits.
- Civil liability.
- Personal liability for individuals who intentionally capture or misuse sensitive information.
- Organizational liability for employers who fail to prevent, investigate, or report violations.
- Enhanced penalties where information is used for fraud, harassment, discrimination, surveillance, AI training, resale, identity theft, profiling, blackmail, or intimidation.
- Enhanced penalties where recording indicators are disabled, concealed, bypassed, or made misleading.

- Enhanced penalties where devices or software capture sensitive information in the background without active recording by the operator.
- Referral to law enforcement where conduct may constitute a criminal offence.

Penalties should be significant enough that unauthorized capture of sensitive information is not treated as a minor cost of doing business.

22. Complaint and Investigation Rights

Any person who believes their sensitive information may have been captured by camera-capable wearable technology must have the right to file a complaint with the responsible organization and the appropriate privacy authority.

The organization must provide:

- Confirmation of whether camera-capable technology was in use.
- Confirmation of whether the device was capable of recording.
- Confirmation of whether recording, buffering, scanning, AI processing, or cloud transmission occurred.
- The identity of the organization responsible for the device.
- The retention period for any captured information.
- The steps taken to delete or secure the information.
- The names or categories of third parties who had access to the information.
- The steps taken to prevent recurrence.

Failure to provide this information shall be treated as a separate violation.

23. Minimum Safeguards for Lawful Use

Where camera-capable wearable technology is lawfully used in sensitive information settings, the following minimum safeguards must apply:

- The device must be issued or approved by the organization.
- The device must be configured to minimize capture.
- Personal devices must be prohibited.
- Recording must be off by default.
- Background capture must be disabled.
- AI processing must be disabled unless expressly authorized.
- Cloud syncing must be disabled unless expressly required and disclosed.
- Recording indicators must remain visible and functional.
- Workers must be trained.

- Access must be logged.
- Retention must be limited.
- Deletion must be verifiable.
- Complaints must be investigated.
- Breaches must be reported.

If these safeguards cannot be met, the technology must not be used in that setting.

24. Review and Updating

Because camera, wearable, biometric, payment, document-scanning, and AI technologies are changing rapidly, this policy must be reviewed at least every two years.

The review must consider:

- New wearable devices.
- Facial recognition technology.
- AI document scanning.
- Payment card capture risks.
- Identity theft risks.
- Background capture functions.
- Recording indicator reliability.
- Smart glasses and augmented reality systems.
- Privacy commissioner findings.
- Public complaints.
- Enforcement outcomes.
- Whether additional technologies should be restricted.
- Whether penalties are sufficient to deter violations.

25. Plain-Language Summary

If someone is checking your ID, handling your bank card, looking at your credit card, reviewing your medical forms, scanning your documents, or standing close enough to capture that information, they should not be wearing smart glasses or similar camera-capable technology unless there is a clear legal reason, clear notice, strict safeguards, and a non-recording option.

The public should not have to guess whether their ID, health card, citizenship status, bank card, signature, address, private documents, or financial information is being silently recorded.

Disabling a recording light, hiding a recording signal, or using software that captures images in the background should be treated as a serious privacy violation, not a technical mistake.

Sensitive information should not be captured just because technology now makes it easy to capture.

Note on Companion Legislation

This proposal is not intended to stand alone.

The Camera-Capable Wearable Technology and Sensitive Information Protection Act focuses primarily on organizations, businesses, public bodies, employers, contractors, institutions, and controlled settings where people are required or expected to expose sensitive information.

A companion policy should also be developed: the Public Use of Camera-Capable Wearable Technology and Personal Data Protection Act.

That companion policy would address the broader public use of camera-capable wearable technology by individuals who are not acting on behalf of a business, employer, government body, or organization.

It would deal with issues such as:

- Random individuals recording IDs, bank cards, documents, or screens.
- People wearing smart glasses in lineups, waiting rooms, bars, clinics, schools, government offices, voting places, banks, airports, and other public or semi-public spaces.
- Capturing children, vulnerable people, victims, patients, or people accessing social supports.
- Recording documents, cards, screens, or forms held by someone else.
- Uploading images of strangers' documents, cards, faces, or personal information to AI tools.
- Bystander liability for capturing or sharing another person's sensitive information.
- Concealed recording in public and semi-public spaces.
- Civil penalties even when the person responsible is not attached to a business, employer, government body, or organization.

Together, these two policies would recognize that sensitive information can now be captured not only by institutions, but also 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.

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)