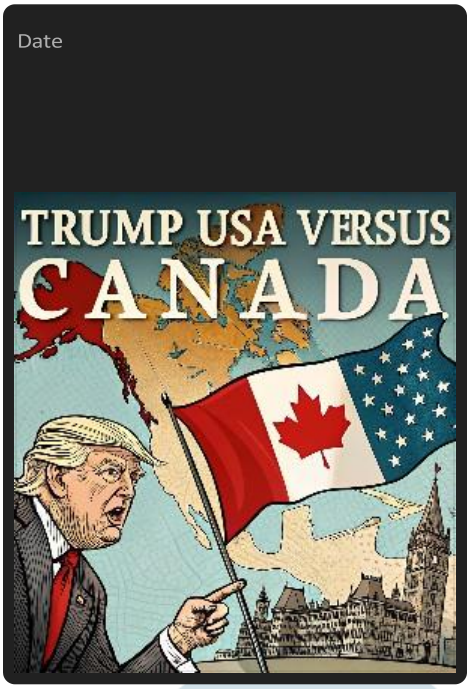
Date



AI ETHICS & SOVEREIGN SECURITY POLITICS

Identification-Consent: an expression of Canadian sovereignty

As Trump doubles down on Canada's Statehood, he uses veiled threats "Attacking Canada Highly Unlikely".

Followed by misinformation;

"I'll always talk about that. You know why? We subsidize Canada to the tune of $200 billion a year," Trump added, reiterating his false claim over the U.S. trade deficit with Canada. (cbc.ca)

This is clearly an attack on Canada's sovereignty wielding misinformation to attack Canada sovereignty. A feat that would not of been possible before the unregulated team up of politics and social media in the US.

Behind the friendly logos and seamless user interfaces, a secret surveillance architecture has quietly been taking shape.

In the context of a web service session, whether it's in person or online the burden of notice is on the Service, to inform the individual. Not on the individual to opt-in to a contract of terms for use. This is a problem that ad tech companies like Google have created through web browser design. It has taken this long for international standard, and international Treaty for data governance, Convention 108+, to come to International market. It takes time to legislate, but once 38 countries implement it legislation to come into effect. To officially be the global standard privacy policy.

The deception of Ad-Tech, self proclaimed 'Internet Industry' has a ethical challenge at its core that is damaging to digital culture, rights and society as it grows.

The impacts are now observable, with un-regulated AI, taking everyone's data with by pretending redefined transparency, permission and consent

An issue that rots the core of Ethics in AI, hides the rapacious theft of data to create commercially unregulated knowledge banks. It's not just copyright theft, it's a violation of data sovereignty. It's essentially a digital war over unregulated surveillance of your data. A war that can be won by requiring scope of disclosure online.

🧠 The Silent Invasion of Data Sovereignty

When you sign into a cloud service, post a message, save a file, or make a transaction, you might assume you own your data because you have access to it. However, most likely, you are transferring your data across the internet to a service located in another legal jurisdiction that does not recognize the same laws or regulations. The traditional concept of 'privacy' has not only been disregarded but has been systematically stuck in analogue privacy by internet tech companies unregulated in the US, who are able to build their systems around security and privacy laws of other countries like Canada.

Access to your data is not equivalent to ownership or control, nor is it subject to common rules.

Access is merely borrowed, while ownership signifies control. The normalization of services requiring individuals to repeatedly submit their personal data is framed as a protective measure.

Behind every login, every "agree to terms" checkbox, and every SSL certificate issued on your behalf, **you were unknowingly surrendering the keys.**

- Your emails were readable.
- Your sessions were tokenized and resold.
- Your behaviors were segmented and auctioned. Browsers would automatically send your data internationally.
- Your identity was profiled and packaged not as *you*, but as *a pattern* for sale, without your knowledge or consent, beyond the sovereignty of your country, to a location where your data holds no rights.

The invasion of your sovereignty did not occur in a single moment. It has been slowly and silently eroded, one internet session at a time, under terms and conditions that offer outdated privacy options.

⚠ The Selling of Trust

Google didn't need to "steal" your data. The Chrome browser is designed so **they own your data by default**, while pretending to care and adhere to the rules.

They didn't need hackers to breach your data. **They manipulated your consent** through legal fictions and behavioral nudges, using dark patterns to circumvent laws and regulations.

Every time you clicked "Log in with LinkedIn," "Accept Terms and Conditions," or "Allow Access to Contacts," another piece of your sovereignty was dissolved.

Now, as standards for digital privacy, transparency, and consent become enforceable, the deceptive practices of big tech regarding personal data are becoming clear. This is evident with the latest advancements in digital privacy transparency and consent security and compliance technologies.

A new generation of Controller identification assurance technologies is emerging to implement digital privacy (zero trust) solutions which don't require passing user information across the internet. Consented surveillance to access services online addressing these ad- tech security challenges.

What Consent looks like Online

Consent looks like asking permission before surveillance, like placing digital identification receipts (aka Cookies) on your device. It requires being transparent about what is being tracked, and when online (not in person) this means identifying who will be in control of your data before, and if it is leaving your location and country. In Quebec the
@Law 25 Transparency Obligation refers to a user interface that is equivalent to turning identification on like a switch. At 0PN we work on the digital technology to see if consent, security and permissions are mutual.

This is why we know that currently there is a lot of mis-information in the design of online surveillance based services, which hide the digital surveillance with deception by default. In the context of Canadian (Law of the Commons derived) Consent: 'Services that use, access, or create identifiers connected to a human being are technically and legally considered the 'users' of personal data. Subject to the permission and control of the individual, your consent.

This is not only a matter of being polite, this means that in Commons based internet law @Convention 108+ a notice of who the Data (or PII) Controller is, is compulsory, **prior** to collecting personally identifiable data. In addition, as you would expect when being polite, a notice of risks involved when transferring data internationally is required, especially to the USA, whose internet companies hold Canadians data hostage for profit.

Asking permission before tracking with digital surveillance people is not just polite, it's a matter of national security, which is why regulation is needed. But, instead of just regulating internet companies, Canada needs to regulate the scope Canadian information disclosure and make rapacious data practices, that are clearly harming children to stop.

How can consent work online?

Consent is all about authority of the state which extends (some identerati may say delegated) by the state to the individual, this includes online when the individual is in the location where the self-sovereign right of consent is provided.

Notice and consent can be Embedded with Standards used to Upgrade Cookies to Digital Privacy Capable - With Scope of Data Disclosure Policy

Introducing Scope of Data Disclosure as a mechanism to build in networked privacy by default

A simple rule: All services (aka identification controllers) are required to be transparent about their identity and services, ensuring that the individual using the service can choose the scope of disclosure when creating a digital identifier. Users must have control over the permissions for its use, in accordance with the service's purpose.

Transparency is the straightforward human governance solution, especially regarding the semantics and technical definitions of terms used by the digital surveillance industry. Scope of Disclosure

Make standard digital identification transparency a rule that applies to everybody equally to implement digital privacy law. A simple digital transparency rule, an international transparency code of conduct that is open digital as well as legally, as open source. Digital transparency upgrades cookie receipts to digital notice and consent receipts, that set people free, embeds trust directly in data flows. Stand up a policy that dictates that online gateway services must disclose their identity and data sovereignty prior to generating identifiers, profiling, and transferring data internationally. (Make them upgrade cookies to receipts).

To check what your transparency performance rating is, sign up at 0PN.ORG for the beta test, and get a confidential WHiSSPR (white hat identity surveillance privacy risk report) to see your digital privacy transparency risk.(only from May 5th to May 24th, 2025)