Hi ,

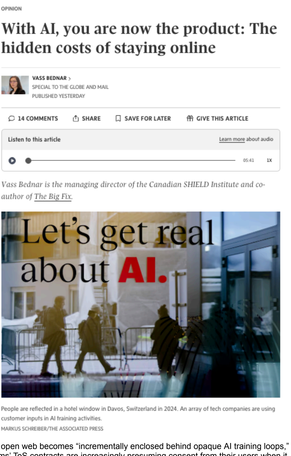
Do you mind if we use all of your newsletter interactions to make an AI model we can profit off of?

I mean, just kidding. But if you are reading this from your Gmail inbox, here's how to turn Google's AI training function off. Wired has an excellent piece explaining How to Stop Your Data From Being Used to Train AI. But why is this happening by default in the first place?

If you haven't noticed, you aren't supposed to.

Many technology platforms are making AI training the price of participation. And because they assume consent, it's sort of a (very subtle) shakedown. Our posts, drafts, clicks and swipes inform algorithmic models tech firms can monetize. This forced AI-consent turns everyday digital life into raw material for companies' balance sheets. We don't need to accept this as the new normal. We can use public policy to turn it off.

This week, I wrote an op-ed in the Globe and Mail's Report on Business that spotlights how accessing essential platforms now comes bundled with coerced AI training. The piece points to companies like **Anthropic**, **LinkedIn** and **Reddit**, which have all moved towards terms of service (ToS) that include "extractive" AI-training elements.



OPINION

With AI, you are now the product: The hidden costs of staying online

VASS BEDNAR
SPECIAL TO THE GLOBE AND MAIL
PUBLISHED YESTERDAY

14 COMMENTS SHARE SAVE FOR LATER GIVE THIS ARTICLE

Listen to this article — Learn more about audio — 05:41 — 1X

Vass Bednar is the managing director of the Canadian SHIELD Institute and co-author of The Big Fix.

People are reflected in a hotel window in Davos, Switzerland in 2024. An array of tech companies are using customer inputs in AI training activities.
MARKUS SCHREIBER/THE ASSOCIATED PRESS

As the open web becomes "incrementally enclosed behind opaque AI training loops," platforms' ToS contracts are increasingly presuming consent from their users when it comes to training AI off their data.

And there are even *more* examples!

In late 2023 and again in early 2024, **Grammarly** — a popular online writing assistant — added a new "Product Improvement and Training" setting that defaults many individual accounts into allowing their written content to train Grammarly's AI models unless manually switched off — effectively turning everyday documents, drafts and emails into training data by default.

Last year, **Hubspot** revised its customer ToS to state that user data "may be used to train HubSpot AI models" and customers would "instruct" Hubspot to do so unless they sent an email opting out.

Slack quietly updated its privacy principles last spring to clarify that customer messages, files and interactions would be automatically included in its machine-learning training unless a workspace admin emailed to opt out. This shift effectively defaulted millions of users into training Slack's internal AI systems without explicit consent.

In June 2024, **Figma** launched new AI terms and introduced a "Content Training" toggle that was switched on by default for many account tiers, meaning users' design files could be used to train Figma's AI unless administrators discovered and disabled the setting — a move that sparked pushback from professional designers and privacy advocates.

Over at X (**Twitter**), updated ToS and privacy terms outline that user content may be used to train AI, while interactions with Grok are also used for model training. Plus, the platform also lets other companies train on your data.

In other instances, better controls exist: Auttomatic-owned Tumblr and Wordpress both added "prevent third-party sharing" toggles that restrict posts from being shared with external AI companies. While this gives users some control, it still formalizes the default assumption that your content is in scope for AI unless you explicitly turn it off.

Public pushback has worked — but where's our government?

In many cases, high-profile companies have found themselves walking back changes to how they treat AI training in their ToS after blowback from their userbase. **Zoom**'s 2023 ToS update was widely read as allowing the company to train AI on audio, video, facial data and chat content without an opt-out, prompting a public outcry and a subsequent clarification that the company would not use customer content to train generative models without consent. In 2024, small changes in **Adobe**'s ToS sparked panic among creators who feared their work could be swept into AI training, leading Adobe to update the terms to explicitly state that neither local nor cloud-stored content — outside of Adobe Stock submissions — would be used for that purpose. And in 2025, **WeTransfer** triggered similar backlash when new language suggested user-uploaded files might be used to "improve machine-learning models." After criticism from creatives, the company rewrote the clause and clarified that files are not — and never have been — used for AI training.

Together, these examples show how "we might use your content for AI" has become a kind of default legal boilerplate, narrowed only when people push back.

Under current Canadian privacy laws, the standard is clear: companies must obtain consent for new uses of personal information, and that consent must be specific, informed and freely given. Companies are often already collecting the information that they are using for AI training, but it is the new use — for AI model training — they must obtain consent for use.

The Office of the Privacy Commissioner (OPC) has explained that, under PIPEDA, users "cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service – they must be given a choice."

AI training is certainly not "necessary" for the above companies to continue to provide the services their users are already working with. This means, according to the privacy watchdog's guidance, companies must be obtaining Canadians' consent.

As increasingly sophisticated platforms extract increasingly sophisticated levels of sensitive personal information from Canadians online, such as details about our identity and behaviour, we should be given the choice to opt into the increasingly sophisticated ways that information is used — like AI training. Tucking broad training rights into a legal update is not meaningful consent — not for individuals, not for creators and not for workers whose internal communications run through enterprise tools.

Currently, Canadian privacy law's notice and consent requirements are not sufficient to regulate this emerging area of concern because they may not protect all the pieces of information that companies feed into AI training, such as creator or website content.

And the privacy law only dictates rules for platforms' use of "personal information," the legal definition of which may not encompass all of the information generated by users or creators. That allows tech companies wiggle room for when they have to obtain meaningful consent.

It will ultimately be up to our regulators, the OPC and the Competition Bureau, to investigate and assess whether the use of collected user information in training bespoke AI models runs counter to Canadian law.

The policy question that remains: is Canadian law, as it stands, effectively protecting users, creators and digital businesses from the coerced use of their data for building AI models that will enrich online platforms and tech giants? It does not appear to be, though a refresh is coming. This is an opportunity to introduce robust transparency and consent obligations on companies that are otherwise surreptitiously slurping up all sorts of data.

Right now, various technology companies have been quietly rewriting the rules of participation online by cowardly refreshing their ToS. This is all hiding in plain sight. Our regulators have the authority and the obligation to draw a hard line between using a service and being conscripted into training its AI. It's time to enforce it.

Until next time,

Vass Bednar

Two New SHIELD Sovereignty Scores

The SHIELD Sovereignty Score is a practical framework we created to turn policy promises into testable choices, reinforcing SHIELD's goal of Sovereignty by Design. The score reveals if and how a policy decision shifts control, competition or value toward Canada.

We published two scores this week:

1. The Algoma Steel Loan (6/10)

The federal government recently finalized a $400-million loan to Algoma Steel (with Ontario kicking in another another $100-million), keeping Canada's only independent steelmaker operating, securing jobs and supporting the government's emerging Buy Canadian industrial strategy. Our analysis finds the loan *does* stabilize Canada's last Canadian-controlled steelmaker during severe tariff pressure — but misses key opportunities to lock in long-term sovereignty benefits, such as stronger innovation and IP requirements, on-going Canadian ownership or deeper value capture.

2. The 2024 Cohere Cash Injection (2/10)

Our evaluation of the federal government's $240-million payment to Cohere gives the policy a 2/10 on sovereignty and economic transformation. The funding flowed entirely to a foreign firm for activities it was already planning, created no new jobs, did not broaden Canada's skills base, and did not reduce reliance on foreign supply chains or prevent further market concentration. While it may have slowed a potential relocation, the deal did not secure any guarantees that Cohere's ownership, IP or economic value would remain in Canada.

SHIELD In the News

Bloomberg Tax - US Tech Firms Urge End to Canada Tax Laws in Trade Deal Review

Offering comment in this story, SHIELD noted that Canada should expand taxation of digital economic activity without relying on a new standalone digital services tax. Instead, Canada could modernize its definition of "permanent establishment" to capture digital businesses, allowing existing tax laws to apply to foreign platforms.

CBC The National - U.K. government to ban ticket resales above face value

Vass Bednar offered policy context for the UK's decision, building on a previous op-ed. The interview was also clipped for CBC's As It Happens.

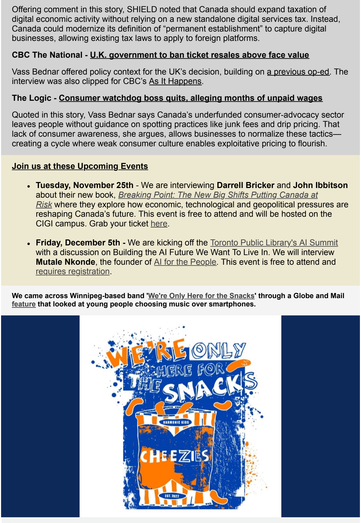
The Logic - Consumer watchdog boss quits, alleging months of unpaid wages

Quoted in this story, Vass Bednar says Canada's underfunded consumer-advocacy sector leaves people without guidance on spotting practices like junk fees and drip pricing. That lack of consumer awareness, she argues, allows businesses to normalize these tactics—creating a cycle where weak consumer culture enables exploitative pricing to flourish.

Join us at these Upcoming Events

- **Tuesday, November 25th** - We are interviewing **Darrell Bricker** and **John Ibbitson** about their new book, *Breaking Point: The New Big Shifts Putting Canada at Risk* where they explore how economic, technological and geopolitical pressures are reshaping Canada's future. This event is free to attend and will be hosted on the CIGI campus. Grab your ticket here.
- **Friday, December 5th -** We are kicking off the Toronto Public Library's AI Summit with a discussion on Building the AI Future We Want To Live In. We will interview **Mutale Nkonde**, the founder of AI for the People. This event is free to attend and requires registration.

We came across Winnipeg-based band 'We're Only Here for the Snacks' through a Globe and Mail feature that looked at young people choosing music over smartphones.



SEND TO A FRIEND