

Canada's Bill C-26: Yet Another Government Power Grab

By [Mark E. Jeftovic](#)

Global Research, February 01, 2023
[easyDNS](#) 27 January 2023

Region: [Canada](#)

Theme: [Law and Justice](#), [Police State & Civil Rights](#)

All Global Research articles can be read in 51 languages by activating the Translate Website button below the author's name.

To receive Global Research's Daily Newsletter (selected articles), [click here](#).

Follow us on [Instagram](#) and [Twitter](#) and subscribe to our [Telegram Channel](#). Feel free to repost and share widely Global Research articles.

Another doozy from the Canadian government.

Following along several other bills winding their way along the Road to Serfdom...

- Bill C-11 regulates the internet under the CRTC and paves the way toward institutionalized content moderation, the requirement for licenses to publish online, and regulation of user generated content ([in Senate](#))
- Bill C-36 the Online Harms Bill sought to designate political dissent as "hate speech" and invoked penalties for criticizing politicians (not sure where this one is at the moment).
- Bill C-18 throws a funding lifeline to Canada's flailing agitprop industry (a.k.a the mainstream media), in that it will require tech platforms to pay licensing fees for content the media outlets post there ([passed third reading](#) in November). This bill [will reward big media conglomerates](#) like Bell, while freezing out small and independent organizations.

Here comes another one, [Bill C-36: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts](#), which passed first reading last June.

It's been largely flying under everybody's radar so far. The Canadian Civil Liberties Association has been actively raising awareness and Michael Geist had Brenda McPhail, their Director of the Privacy, Technology and Surveillance Program [on his podcast](#) last October.

We mentioned C-26 [in AxisOfEasy #273](#) citing Gowling WLG's [coverage of it by Brent Arnold](#) (Brent Arnold sits on the Internet Society Canada Chapter board, as do I, but I am writing this post from my role as easyDNS CEO, and not ISCC.)

The Government Hereby Grants Itself The Following Powers:

The new bill is ostensibly a cyber-security and critical infrastructure bill, but it is riddled with nebulous, open-ended terms, Kafka-esque secrecy provisions, onerous penalties and conspicuously absent of any semblance due process:

It effectively subjects Canada's telecom and internet sectors to the whim of unelected bureaucrats and political functionaries.

Am I being bombastic? You tell me: given that the legislation that grants them the power to order a telecommunications service provider "to do or stop doing *anything*".

"Part 1 amends the Telecommunications Act to add the promotion of the security of the Canadian telecommunications system as an objective of the Canadian telecommunications policy and to authorize the Governor in Council and the Minister of Industry to direct telecommunications service providers to do anything, or refrain from doing anything, that is necessary to secure the Canadian telecommunications system. It also establishes an administrative monetary penalty scheme to promote compliance with orders and regulations made by the Governor in Council and the Minister of Industry to secure the Canadian telecommunications system as well as rules for judicial review of those orders and regulations."

I guess it all comes down to what you mean by "anything".

Speaking of anything, the government can deem "any" service or system a vital service or system - which then makes that entity subject to requirements, that...

- (a) authorizes the Governor in Council to designate any service or system as a vital service or vital system;
- (b) authorizes the Governor in Council to establish classes of operators in respect of a vital service or vital system;
- (c) requires designated operators to, among other things, establish and implement cyber security programs, mitigate supply-chain and third-party risks, report cyber security incidents and comply with cyber security directions;
- (d) provides for the exchange of information between relevant parties; and
- (e) authorizes the enforcement of the obligations under the Act and imposes consequences for non-compliance.

Each one of these bullet points opens a can of worms unto itself, combined they have the potential to effectively nationalize Canada's information infrastructure.

The penalties for non-compliance are onerous: \$1 million *per day* for individuals and \$15 million /day for any other entity.

But wait, there's more:

Under C-26, orders are filed in secret, telecommunications service providers (TSPs) can be ordered to cut off any user (including another TSP) while being barred from even informing the entity that it's happening, let alone why.

The contents of said orders are secret and not even divulged to the target. I recommend listening to the Michael Geist / Brenda McPhail podcast above to understand the threat to Canadians' *privacy*.

Me, sitting here with my easyDNS hat on, running an internet service provider, I'm dialled in on the *due process* aspects.

More accurately, the complete *absence* of due process. We've got twenty-five years experience of being told by various governments and their agencies to forgo due process and do things that would otherwise disrupt businesses, individual rights and even the network itself if we listened to them.

Being told to *do* or *stop doing* "*anything*" seems overly broad.

It gets worse:

Similar to previous legislation, there are provisions for warrantless entry into places of business, or private homes, to search, copy or remove anything they deem relevant - including documents or telecommunications equipment.

C-26 also permits the government to share data with *foreign entities*. Again, this is all done without any of the privacy safeguards most citizens *think* they have as a constitutional right, because this bill, and this government, mostly ignores that those rights exist.

Non-Hypothetical Example

Last year, around this time, the same government that is introducing this bill arbitrarily enacted bank account seizures, not only against protestors, but also targeting [crowdfunded contributions](#) to their fundraisers.

This was done under the aegis of the Emergencies Act, however the seizures started before the EA was even ratified in Parliament, and the list of fundraising contributors was largely sourced from a third-party spreadsheet that was hacked from a foreign crowdfunding platform.

Nevermind that the entire thing went away within a week - rationalized as "mission accomplished" (the reality was the measure [sparked a run on banks](#) and nearly blew up the Canadian financial system)

Five major Canadian banks mysteriously go offline in hours-long outage



Jordan Major

STOCKS Feb 17, 2022

+390
 Share

A range of investment tools and advice to help you worry less and sleep more.

Learn more

Not much mention of this in the MSM, oddly...

The 2022 invocation of the Emergencies Act made it clear that our government is perfectly willing to act unilaterally, without due process, in contravention of basic human rights to unbank people at whim.

Bill C-26 will give them a veneer of Soviet-era legislation to unperson you in the online realm.

What Can You Do?

While I said I'm not speaking with my ISCC hat on today, the Internet Society Canada Chapter is one of the civil society bodies that does its level best to bring informed, rational commentary and input to the policy making process. Membership includes a couple ex-CRTC commissioners and even a recent appointee to the Order of Canada.

Consider [signing up as a member today](#) and help us bring a clue to the process, or alternatively, get behind [the Canadian Civil Liberties Association](#).

You can also make your views known to your MP. They don't care if they get your vote or not, so don't even bother telling them you won't vote for them. You have speak their language, e.g

"I know you don't care about my vote – but I feel strongly enough about this issue to make the maximum allowable personal contribution to your opponent, and fund raise for them wherever I can".

In my case they at least started replying to my emails after that.

*

Note to readers: Please click the share buttons above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image: Technocracy – a 1933 cartoon by Winsor McCay.

The original source of this article is [easyDNS](#)
Copyright © [Mark E. Jeftovic](#), [easyDNS](#), 2023

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Mark E. Jeftovic](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca