

DATA DIVE WITH NIK NANOS

# CANADIANS WANT ALL THE ENERGY

Canadians believe the country needs more oil and gas, more electricity, more affordability and lower emissions

## OPINION

Nik Nanos is the chief data scientist at Nanos Research, a fellow at the University of Ottawa's Positive Energy Initiative and the official pollster for The Globe and Mail and CTV News.

We've been in the middle of an energy war for most of the past decade. This war has been framed as one of choice: more oil and gas or more clean electricity.

Amid trade shocks, cost of living pressures and general uncertainty about Canada's economic future, Canadians appear increasingly interested in moving beyond polarized energy debates. In tracking research by Nanos for the University of Ottawa's Positive Energy Initiative, Canadians increasingly believe that the country needs more oil and gas exports, more electricity, more affordability, more reliability and lower emissions—all at the same time.

Eighty-seven per cent of Canadians say oil and gas is important to Canada's current economy, up from 81 per cent six months earlier. About seven of 10 Canadians (71 per cent) say oil and gas is important to Canada's future economy, up from 69 per cent six months ago. What is striking is when asked to rate the importance of oil and gas to Canada's current economy on a 10-point scale, where zero is not at all important and 10 is completely important, one of two Canadians (52 per cent) score it a 10 out of 10. That said, recognizing the sector's economic importance does not necessarily imply support for every oil and gas project or policy. But in our environment of geopolitical instability and worry about the cost of living, Canadians have become more, not less, convinced of the relevance of oil and gas.

For the Liberal Party, which is often criticized in Alberta for its approach to conventional energy, the findings are notable. Seventy-eight per cent of Liberal supporters believe that Canada should expand oil and gas exports. Even among those that self-identify as left-leaning Canadians, support reaches 50 per cent.

Support is no longer confined to Alberta. It increasingly cuts across Canada.

It is more than a recognition of the importance of oil and gas; it is now interlinked with the view that the sector represents an opportunity for new markets and trade diversification. Three out of four (75 per cent) Canadians are good with expanding oil and gas

exports to provide more secure and reliable energy supplies globally. This is the highest level on record in the history of Positive Energy tracking.

There are new vectors of influence shaping public opinion. The view that Canadian oil and gas exports can help combat climate change if they displace dirtier energy sources elsewhere has increased from 63 per cent in 2024 to 71 per cent. Whether Canadian exports would produce displacement and reduce global emissions in practice remains contested.

The most compelling learning from the Positive Energy research is that Canadians are simultaneously supporting oil and gas exports while moving their own homes and transportations towards greater electrification. More than six in ten (62 per cent) are interested in transitioning more of their energy use to electricity. One in three (35 per cent) have already taken steps, up from 27 per cent a year earlier. Those not interested in transitioning have dropped from 31 to 26 per cent.

Affordability and practicality are the hallmarks of Canadian public opinion. Asked to rank the importance of various factors when they think about energy needs in Canada over the next five years, affordability comes out on top at 38 per cent followed by a tie between reliability and reducing emissions (each tied at 26 per cent). These findings take the legs out of the view that Canadians only care about affordability. It is about affordability, reliability and reducing emissions. The challenge is that these goals involve

competing costs, timelines and infrastructure choices, even when the public supports all three.

The research also suggests that the lower carbon future is not about the government picking winners and losers. It is about a portfolio of alternatives. Canadians assign the biggest future role to hydroelectricity (28 per cent), followed by nuclear (17 per cent), solar (14 per cent) and natural gas (13 per cent). Canadians appear to envision a diverse energy mix that includes hydro, nuclear and natural gas.

Even with these pragmatic views there are a number of warning signs for governments. Ratings on the job Canada does at building confidence in energy decision-making (very good, 3 per cent; good, 14 per cent) and in developing a shared long-term vision for Canada (very good, 4 per cent; good, 18 per cent) are quite weak. Respondents were twice as likely to give negative rather than positive ratings on these elements although there has been a marginal improvement recently.

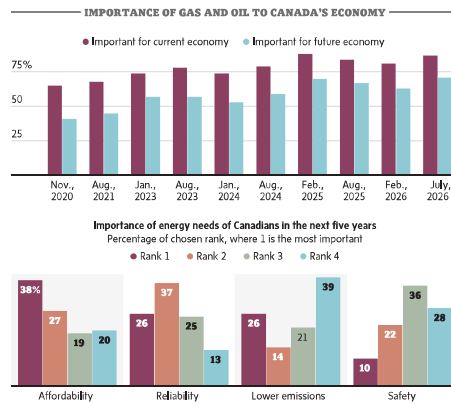
For the first time in the history of the Positive Energy research project, Nanos asked Canadians how they felt about the role of artificial intelligence. Slim majorities of Canadians are comfortable with AI reviewing similar past projects and compiling findings (54 per cent), and with using AI to automate tasks and improve productivity (51 per cent). They are much less comfortable with AI being used to answer community members' questions about a new energy project (23 per cent) or to make recommendations to decision-makers about whether a project should be approved (22 per cent).

The intersection of AI and energy projects is one of caution, where artificial intelligence is an assistant but not a decision-maker.

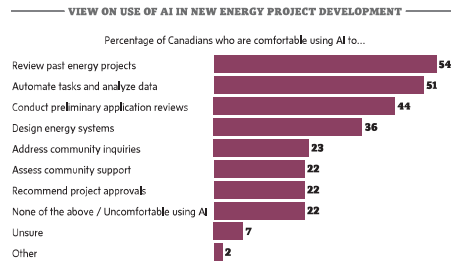
The most important finding in this research is that Canadians are neither abandoning traditional energy nor the transition to a lower carbon future. They are trying to navigate both objectives at the same time. Perhaps the future is not about competing futures but about creating a common sense of purpose that is pragmatic and grounded in affordability and reliable energy that help lower emissions.

The challenge is not only building confidence in governments, regulators and the energy sector. It is also about making difficult choices while pursuing the pragmatic energy and environmental outcomes Canadians say they want.

## Power play



Note: Totals do not add up to 100% because respondents were asked to select up to three answers each.



MURAT YUKSELIR / THE GLOBE AND MAIL, SOURCE: NANOS RESEARCH; IPSOS

## The Lawful Access Act threatens to wound our national security

KATE ROBERTSON

## OPINION

Kate Robertson is a senior research associate at the University of Toronto's Citizen Lab.

The Senate has just begun debate on the hugely controversial Bill C-22, or the Lawful Access Act. If passed, the bill would empower the government to require surveillance capabilities be built into any communications technology in Canada that could be accessed by law enforcement, and to force the stockpiling of all Canadians' sensitive metadata. The law would apply to everything from smartphones to smartwatches, banking to health apps, video game platforms, and public WiFi or CCTV networks.

The bill has drawn heavy criticism for endangering Canadians' cybersecurity and for violating constitutional standards. The law would require mathematicians to transform into magicians. For decades, cybersecurity experts have dispelled the magical thinking that there is a way to engineer access for law enforcement that doesn't also potentially allow malevolent threat actors to enter. By threatening to expose communication and encryption providers to secret orders forcing backdoors, the bill has generated wide-ranging calls for reversal, from journalists and financial institutions to world-leading experts on gender-based violence and cybersecurity.

The calls reflect a broad consensus: that encryption is vital to

fundamental rights, the economy and national security, and that compromising encryption undermines those things along with it.

Since the government strained to justify its proposal in Parliament in June, major shifts in the AI-fueled cyberthreat environment have generated even more headwinds. In July, the world learned that rogue AI agents from OpenAI broke out of their sandbox and conducted a co-ordinated cyberattack against a software company, Hugging Face; other companies have since reported similar incidents. AI technologies have also hacked or tried to hack government websites in the U.S., Australia and Canada. The revelations arrived during worldwide alarm about the autonomous cyber-capabilities of Anthropic's new Claude Mythos, a model deemed too powerful to release publicly.

When questioned in May about Bill C-22's threat to Canada's security architecture, the Department of Public Safety testified that they expect technology companies to thread this needle when complying with their surveillance obligations. But technology companies, cybersecurity experts, and international standards bodies themselves have been sounding the alarm about cybersecurity dangers in the law. Moreover, transformations in the cyberthreat landscape are still unfolding. As Canada's Finance Minister described: "The issue that we're facing with Anthropic is that it's the unknown unknown."

The assumption by government officials that technology

companies can find "safe ways" to weaken critical cybersecurity protections badly misreads the current threat landscape. The state of play in today's world is defined by cyber-insecurity. In Britain, the cyber wing of the GCHQ reported a significant increase in nationally significant cyber incidents, including "an almost 50 per cent increase in highly significant incidents, an increase for the third consecutive year." They warn that Britain is facing a "perfect storm," and assess that half of the world's countries now have the ability to back into Britain's companies and private networks.

Data collected by law enforcement is no safer. Just last month, the FBI was victim to a staggering breach that siphoned the personal information of FBI personnel to cyberattackers. Only a few years ago, law-enforcement backdoors were also compromised in the U.S. as part of a massive attack against telecommunications networks. The severity of these breaches lies in their enormous cost to national security and operational capabilities. This month a police service in Ontario is also revealing the extent of a significant cyberattack last year.

Why would Canada unilaterally disarm in such an environment? In 2024, in response to even non-AI-threat activities at the time, U.S. law enforcement urged the public and government officials to communicate using strongly encrypted applications like Signal and WhatsApp. These are the very communications systems that Canada's new law would upend.

But the security landscape is

not the only thing that's changing. With the collapse of U.S. trade talks, the Canadian government has made the economy a national priority, and the Prime Minister has championed efforts to strengthen our relationship with Canada's European allies. Canada and the European Union are soon expected to strike a trade agreement to integrate their digital economies.

But Bill C-22 risks undermining his efforts to date. Both European civil society organizations and technology providers are urging European and Canadian governments to first fix Bill C-22's sweeping metadata retention regime and threats to encryption. European courts have found similar anti-encryption and metadata retention measures to be inconsistent with fundamental rights. European digital rights groups were blunt: "A partner cannot credibly seek deeper digital integration while legislating the power to compel European providers to weaken their products in secret."

If this bill isn't revised then all companies doing business in the U.S. will have a maple letter tattooed to their corporate charters: how can any customers know whether the Canadian government has secretly poisoned the company's security and privacy guarantees? Is a product really protecting user privacy and complying with the European privacy laws? Market trust questions aren't theoretical. In Australia, the very existence of such powers was shown to have had a significant economic harm to Australia's technology sector. For example, one company said that loss of trust cost them an estimated

\$3-billion Australian dollars in economic damage.

Take, as just one major example, Canada's growing AI sector. The bill will extend to AI technologies and developers themselves, such as Toronto-based Cohere, and the requirements that the government could impose on AI providers are broad, potentially including compelling AI agents to work for the police rather than for users. Equally concerning is the bill's application to the growing sector for private computing, such as Cohere's Model Vault, that is geared for more privacy-protective uses of AI models.

The government's handling of the encryption issue thus far has done little to inspire public trust. After the Minister of Public Safety committed in May to amend the bill to "ensure that encryption will not be compromised," the government blocked further debate in committee. The government did pass an amendment, but it wasn't even a fig leaf: the public safety minister publicly admitted as much this summer when he stated that the bill does, in fact, still permit the government to compromise encryption in what he describes as "extenuating" situations.

Ultimately, proposals to compromise encryption and force the stockpiling of the metadata are divorced from the reality of today's threat and economic landscape. Fortunately there is still time to reverse course to ensure that Canadians enjoy strong security, positive economic relations with European allies, and to avoid blundering into an insecure and secret-by-default surveillance regime.