December 10, 2024

Hon Mélanie Joly
Minister of Foreign Affairs
House of Commons
Ottawa, ON K1A 0A6

Hon Dominic LeBlanc
Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs
House of Commons
Ottawa, ON K1A 0A6

Hon Arif Virani
Minister of Justice & Attorney General of Canada
House of Commons
Ottawa, ON K1A 0A6

To the **Hon Mélanie Joly**, Minister of Foreign Affairs, the **Hon Dominic LeBlanc**, Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, and the **Hon Arif Virani,** Minister of Justice and Attorney General of Canada

CC: **Philippe Dufresne**, Privacy Commissioner of Canada

We, the undersigned organizations and individual experts, write to urge you to reject adoption of the United Nations draft Convention against Cybercrime (A/AC.291/L.15) once it is opened for signatures in Hanoi next year.

The treaty requires states to adopt a number of criminal offences, intrusive surveillance powers, and exceedingly broad cross-border law enforcement cooperation mechanisms. Accompanying these requirements are weak safeguards that too frequently defer to national preference and generally lack any meaningful operational mechanisms.

The draft treaty is deeply flawed in multiple ways that will have a lasting detrimental impact on human rights at a global scale. It will also undermine cybersecurity, constrain Canada's ability to act in its own interest and the interest of its citizens and people in Canada when faced with information sharing requests from other states, and place Canadians, including our diaspora communities, at greater risk of harm from extraterritorial human rights abuses.

The draft Convention is generally detrimental to human rights globally and in Canada

Negotiations of this treaty confirmed that deep divisions remain among states regarding the scope of their human rights obligations. It is irresponsible in this context to adopt a powerful instrument of this nature without including sufficiently robust safeguards that include effective operational mechanisms to implement them in practice.

The draft Convention has been criticized by human rights groups, the Office of the UN High Commissioner for Human Rights (OHCHR), media freedom organizations, members of the United States Senate, leading security researchers, large tech companies, and industry associations and initiatives. This sea of criticism should come as no surprise, as the draft Convention raises numerous significant threats to human rights, including to the rights of children, gender-based harm, and threats to LGBT communities, human rights defenders, political dissidents, whistleblowers, journalists and security researchers, among others. It is poised to expand threats of mercenary spyware abuses, and democratic and security threats including threats to internet freedom and security tools such as encryption and VPNs.

The draft Convention also fails to clearly articulate the core harm it seeks to address, giving license to a problematic trend where states use cybercrime regimes to label any online conduct a "cybercrime", resulting in repression of online dissent and interactions between LGBT people. It is particularly concerning that, in addition to already including a vague and open-ended criminalization provision (Article 4), an

additional protocol that will expand the Convention's existing list of enumerated cybercrimes is already contemplated. Without a principled definition of cybercrime, there are no limits to what further offences might be included in this additional protocol.

The draft Convention will expose people in Canada, and around the world, to increased dangers of foreign interference and transnational repression

A paramount concern raised by the chorus of opposition to the draft Convention is the danger that the treaty will be abused and leveraged by foreign governments to engage in domestic and transnational repression.

Given the draft Convention's expansive scope, it is on course to become a powerful tool for authoritarian governments that would abuse its expansive surveillance and cross-border cooperation mechanisms to expand their targeting, intimidation, and silencing of political opposition, activists, and human rights defenders including through specious allegations of wrongdoing—a dangerous pattern that already plagues other international cooperation mechanisms like INTERPOL's Red Notice program. It could also be mis-used to aid prosecutions under repressive criminal laws that are specifically designed to clamp down on Internet freedom and political dissent.

Safeguarding protections for online expressive activity and political dissent should be an imperative for Canada. Canada is particularly vulnerable to the effects of foreign interference and transnational repression. More than one out of every five people living in Canada was born in another country. Canada is home to many refugees from around the world, and has welcomed over a million refugees since 1980. Canada has an obligation to anticipate risks and protect people in Canada—including refugees, human rights defenders, activists, and journalists—from the rights violations caused by foreign interference and transnational repression.

Already, human rights activists, civil society, and political figures in Canada have been targeted by foreign governments through monitoring, harassment and intimidation, violence and murder, and targeted spyware attacks on Canadian soil. The Government of Canada has stated that it takes the issue of foreign interference seriously, including the need for ensuring that Canada's laws are responsive to the new and evolving foreign interference threats.

National security review bodies and institutions like the National Security and Intelligence Committee of Parliamentarians (NSICOP) and David Vigneault, the then-Director of CSIS, have also recognized the critical importance of addressing foreign interference, including the vulnerability of ethnocultural communities living in Canada. Both Global Affairs Canada and NSICOP have observed that certain governments are increasingly monitoring and harassing human rights defenders in Canada, and that this activity, designed to silence human rights-based criticism of foreign states, "has a chilling effect on human rights activism and freedom of expression."

Historically, Canada has learned hard lessons from past failures to adequately heed the danger of cooperation with foreign governments without taking adequate measures to safeguard human rights. Canadian authorities have witnessed first-hand the tragic and horrific consequences that inappropriate data sharing with foreign authorities can inflict on innocent persons. Even the informal sharing of inappropriate or inaccurate information can lead to the rendition and torture of innocent persons, as in the case of Maher Arar—a Canadian citizen who was arrested in the United States, and rendered to Syria where he was subjected to torture and inhumane treatment.

In a 2022 Special Report on the role of transnational repression in Canada, Freedom House reported that "in the past, Canadian authorities have made agreements to cooperate with governments that perpetrate transnational repression, granting them access to people living in the country in exchange for short-term policy benefits." The report emphasized that it is positive that "Canadian authorities have demonstrated a high level of awareness of the threat posed by foreign governments to specific ethnic communities, political exiles, and diasporas living in the country." However, the report concluded that there continues to be a need for authorities to do more to protect the specific harm of transnational repression for individuals and communities in Canada.

The Government of Canada has taken increasingly proactive steps in recent years. In 2020, the Government of Canada announced that it would be suspending its extradition agreement with Hong Kong in response to repressive new national security laws imposed by the Standing Committee of the National People's Congress of China—laws that were only made more severe in 2024. Canada has expressed serious concern about erosion of respect for human rights and freedoms under the legal regime.

In short, there is a long history of known risks and reported harms that people in Canada have suffered through foreign interference and transnational repression. Canada has also previously been subjected to pressure campaigns, such as from Saudi Arabia—including Interpol Red Notice requests and extradition requests—which Canada refused citing the absence of an extradition agreement with Saudi Arabia. Freedom House additionally reports that extradition requests from countries such as Saudi Arabia, Iran, China, and Mexico have been denied because they were found to be political in nature. Canada also routinely receives extradition requests and mutual assistance requests from India, including reportedly an Interpol Red Notice request and extradition request in relation to Canadian citizen and Sikh activist Hardeep Singh Nijjar—which Canada also refused. Mr. Nijjar was ultimately murdered on Canadian soil in 2023. Prime Minister Trudeau publicly stated that Government of India agents are credibly alleged to have been directly responsible in Nijjar's killing and that subsequent investigations have garnered compelling evidence that the Government of India has engaged in "clandestine information gathering techniques, coercive behaviour targeting South Asian Canadians, and involvement in over a dozen threatening and violent acts, including murder."

Against this backdrop, there are many ways in which people in Canada are poised to be negatively impacted by abuse of this treaty. Given the broad scope of the Convention—with information sharing obligations applicable to digital information associated with all serious domestic criminal offences—it is expected to flood already overloaded legal cooperation channels with low-priority or abusive police requests for digital information. This is problematic, in itself, as overloaded screening mechanisms in international cooperation regimes have been shown to be abused over and over. Personal information and private data accessible to police agencies and in police records are also of significant interest to authoritarian governments. Recent reporting, for example, revealed that agents of the Rwandan government were implicated in attempts to obtain information from police records in the possession of the RCMP, adding to growing concerns from activists from the Rwandan diaspora in Canada about how the Rwandan government has been surveilling its critics in Canada. The revelations are another example of the concerning trend around regarding potential for abuse of information sharing channels between police agencies around the world.

In 2022, the House of Commons Standing Committee on Justice and Human Rights embarked on a comprehensive study of Canada's extradition systems, and received testimony, for example, on the broader context surrounding India's targeting of Sikh activists in Canada. Among many recommendations, the report

found that Canada needs to "modernize outdated treaties and withdraw from treaties with partners that seriously contravene international human rights standards." The draft Convention, however, will push Canada in entirely the opposite direction. Through a single, sweeping instrument, the Convention would force Canada's hand into cooperation agreements with authoritarian governments around the world and countries with rights-violating laws. This would include, for example, obliging Canada to renew extradition obligations with Hong Kong for offences covered by the draft Convention, and to enter into new extradition agreements with respect to those offences with other signatories where Canada has historically not agreed to an extradition treaty (such as with China, Saudi Arabia, Rwanda, Russia, and others). As will be detailed later in this letter, it will also impact Canada's ability to protect human rights in the context of existing cooperation agreements, such as those with India. All of these obligations would be particularly concerning given the absence of an obligation to refuse extradition for political offences in the draft Convention.

Human rights defenders, civil society, political figures, and government officials in Canada and elsewhere would also be more vulnerable to state-sponsored espionage, given the draft Convention is also poised to become a vehicle for complicity in the global mercenary spy trade. Technology companies based in Canada would also become more vulnerable to becoming conscripted into repressive surveillance systems and prosecutions, when countries and law enforcement agencies around the world knock on Canada's door for personal information and data located in Canada.

We recognize that Article 6(2) of the draft Convention nominally excludes acts that suppress fundamental human rights from the Convention. But the draft Convention fails to adopt any of the mechanisms necessary to effectively operationalize this nominal safeguard. And many elements of the draft Convention actively undermine any prospect that the intent of Article 6(2) will be realized, including the breadth of the Convention's criminalization provisions and significant shortcomings in the draft Convention's framework for international cooperation (discussed below).

In the face of these shortcomings, Canada should reject a treaty that would undermine human rights around the world, and expose people living in Canada, their families abroad, and most of the world's population to an expanding array of dangers involving surveillance and repression.

The draft convention will undermine cybersecurity while impeding vital social media platform & AI research

Elements of the draft Convention on cybercrime will have the adverse effect of making information and communication systems less secure.

Article 28(4) of the draft convention can be used to compel service provider employees to disclose information about security safeguards in their products, be they Internet Service Providers, social media platforms or secure messaging services. Employees may be pressured to disclose security vulnerabilities, information regarding encryption protocols, and even passwords. While these demands must respect international human rights law including the principle of proportionality (Article 24(1)), the draft Convention does not require individual notification, permits gag orders (Article 40(20)) and grants states discretion as to whether information disclosure requirements should be premised on judicial authorization (Article 24(2)).

Once this security vulnerability information is obtained in the context of a specific investigation, nothing in the draft Convention prevents states from reusing it for other purposes or even sharing it with mercenary commercial spyware providers.

The draft Convention's core cybercrime provisions are exceedingly broad and fail to address well-documented problems arising from their Budapest Convention counterparts. These provisions, which have been used to prosecute whistleblowers and security researchers, threaten to criminalize basic conduct simply for violating a company or employer's terms of use. The unacceptable risk posed by this broad scope of criminalization eventually prompted the United States Department of Justice to adopt a "do not prosecute" policy with respect to good faith security research, a safeguard absent from the draft Convention.

Indeed, over 120 of the world's leading security researchers have decried the draft Convention and the risks it poses to their important work. Concerns over the negative impact the same criminal paradigm is having on good-faith AI (including Generative AI) and social media platform research have prompted calls for similar legal protections, citing the significant prevailing chill these broad criminal prohibitions are having on any independent scrutiny.

The draft Convention's jurisdiction clause (Article 22) further requires states to take jurisdiction over any crime committed against or by a national of that state, or against the state itself, placing Canadian cybersecurity researchers, including members of diaspora communities, at risk of cross-border investigations or even extradition proceedings. The resulting chill on legitimate research could undermine cybersecurity on a global scale, while deterring essential independent scrutiny of AI systems and content dissemination on social media platforms.

The draft Convention adopts a powerful cross-border surveillance tool that jeopardizes international human rights & subverts existing safeguards

The draft Convention's international cooperation chapter adopts a powerful multilateral tool for cross-border policing that requires mutual legal assistance without adopting reasonable safeguards to ensure compliance with human rights. This framework places Canada's ability to comply with its *Charter* and international human rights obligations at jeopardy.

The draft Convention obligates states to provide each other with the widest measure of mutual legal assistance in the collection of electronic evidence regarding any serious crime. Attempts to include privacy and human rights safeguards in the draft Convention's international cooperation chapter met with severe resistance from many negotiating parties, resulting in a framework that is significantly deficient and subject to severe abuse. These safeguards fall short in a number of ways, and have been heavily criticized by human rights authorities at the United Nations and experts. For example, the draft Convention fails to impose any specific data protection requirements on the processing of requests for international cooperation, relying instead on existing national or international obligations (Article 36). However, Canada's outdated data protection law does not provide an adequate level of protection,[1] while Canada has yet to adopt crucial international data protection instruments such as Convention 108+. Canadian officials therefore have limited tools they can use to protect the privacy of Canadians when processing requests for assistance. Numerous states around the world provide even weaker data protection while some limit the availability of data protection rights to residents.

Under a framework set by the Supreme Court of Canada, Canadian government officials cannot issue an international cooperation request to another state if the state's practices violate international human rights

[1] *Union of Canadian Correctional Officers v Attorney General of Canada*, 2016 FC 1289, para 139-141 (aff'd 2019 FCA 212, paras 38-42).

obligations.[2] Unfortunately, the draft Convention's international cooperation framework fails to ensure that states will respect international human rights obligations when responding to requests. In fact, it strongly suggests they will not do so, creating instead a mechanism that is prone to abuse. In particular, the draft Convention's failure to explicitly include the principle of proportionality as an overarching requirement for its cross-border policing mechanisms will lead to violations of the right to privacy. Reasonably foreseeable privacy violations include situations where a requested state provides Canada with evidence obtained through the use of commercial spyware or through measures that bypass encryption—each in violation of international human rights law. Many states also fail to require prior judicial authorization when conducting surveillance or obtaining metadata and subscriber data in response to requests for mutual legal assistance.

By operation of the *Mutual Legal Assistance in Criminal Matters Act*, the draft Convention would also subvert numerous existing safeguards in Canada's broader framework for processing mutual legal assistance. For example:

- The *MLCMA* is premised on the assumption that the government will enter into agreements with safeguards tailored to the particular criminal justice systems of specific countries or subsets of countries and, as a result, imposes few default safeguards that would apply across all agreements. The draft Convention subverts this approach by creating an agreement with all countries in relation to any electronic evidence of a serious crime (Articles 35 and 40).
- Under the general *MLCMA* approach, Canada has the option of suspending any given bilateral agreement with any country that exhibits systematic human rights or rule of law failures. There is no option to do so once the draft Convention is adopted, as Canada would need to repudiate the entire agreement and could not do so with respect to any specific signatory of the agreement, even if that signatory has a demonstrable record of systemic rule of law and human rights failures.
- The draft Convention lacks a political crimes exception, even though this exception is present in numerous other bilateral or regional agreements that Canada has adopted. Article 40(22), for its part, provides some protection but sets an exceedingly high bar and lacks any mechanisms to ensure it is respected in practice such as a requirement for judicial determination and inclusion in national law.
- The *MLCMA* imposes a dual criminality obligation for any legal assistance request that falls outside the scope of an existing agreement.[3] Since the draft Convention requires legal assistance in relation to all states and treats dual criminality as an option to be exercised in national law (Article 40(8)), it renders this central *MLCMA* safeguard effectively inoperative.

The draft Convention will also undermine safeguards in future negotiated agreements while subverting those already adopted in existing agreements. States that have already accepted more rigorous safeguards in bilateral agreements with Canada could repudiate those and rely on the more permissive draft Convention instead. At the same time, Canada has failed to update many MLAT agreements with states where respect for rule of law and human rights is rapidly devolving. Once the draft Convention is adopted, renegotiating or

---

[2] *Canada (Justice) v Khadr*, 2008 SCC 28 at para 2 and 18, citing *R v Hape*, 2007 SCC 26 at para 52, 51, 101, and 56. Note that this framework for addressing international cooperation should be seen as establishing a floor, not a ceiling, in terms of the Charter obligations it imposes on Canadian officials in an increasingly interconnected world: *R v McGregor*, 2023 SCC 4 at para 68 [Karakatsanis & Martin]. See also: Leah West, "Canada Stands Alone: A Comparative Analysis of the Extraterritorial Reach of State Human Rights Obligations" (2022) 55:3 *UBC L Rev* 845.

[3] *MLCMA*, sub-sections 6(1) and (2).

even repudiating such agreements in the face of further devolution will not be possible given that any state will be able to rely on the draft Convention in lieu of any bilateral agreement with robust safeguards.

Put plainly, the draft Convention undermines Canada's discretionary bargaining power and imposes broad, mandatory obligations while undermining our government's ability to protect the human rights of Canadians.

Canada's mutual legal assistance relationship with Hong Kong is illustrative of the challenges that adopting this draft Convention would create. Canada's Mutual Legal Assistance Treaty was suspended in 2020 by Hong Kong following a diplomatic dispute triggered by the latter's adoption of an oppressive set of national security laws, discussed above. Under the draft Convention, Hong Kong would be able to request investigative assistance regarding political dissidents living in Canada and to do so without a number of core safeguards that were included in the now defunct bilateral treaty, which remains suspended. These safeguards included mandatory requirements to refuse any request that would impair Canada's essential interests, would relate to any offence under military law or to a political crime, or would violate the principle of dual criminality. The lack of these safeguards is particularly concerning given the extra-territorial reach of Hong Kong's growing arsenal of abusive national security laws.

Under the *MLCMA*, the draft Convention's provisions on mutual legal assistance will have direct legal effect soon after the draft Convention is adopted by Canada and comes into force.[4] We know from our experience with other international cooperation mechanisms such as INTERPOL's notice systems that the combination of weak safeguards and overloaded screening processes is a recipe for abuse. This draft Convention replicates that recipe. Given this high potential for subverting international human rights and core safeguards in Canada's framework for mutual legal assistance, Canada must reject this Convention.

Conclusion

Canada would lose more than it would gain as a signatory to the draft Convention. To avoid exposing people in Canada and around the world to increased threats of transnational repression and human rights violations, undermining proportionate and rights-respecting efforts to address cybercrime, and producing significant risks to Internet users globally, we urge Canada to refuse signing the draft UN Convention against Cybercrime following its adoption by the UN General Assembly and to use its mandate to encourage other countries to do the same.

Endorsed by the following organizations and individual experts:

Organizations

- **Amnesty International Canada – English Section**
- **Amnesty International Canada – Francophone Section**
- **Centre for Free Expression**
- **Centre for Law and Democracy**
- **Criminal Lawyers' Association**
- **International Civil Liberties Monitoring Group**
- **OpenMedia**
- **PEN Canada**
- **Privacy & Access Council of Canada**

[4] *MLCMA*, paragraph 2(1)(a).

Individual Experts

- **Noura Aljizawi**, Senior Researcher at the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
- **Colin Bennett**, Professor Emeritus, University of Victoria
- **Andrew Clement**, Professor Emeritus, Faculty of Information, University of Toronto
- **Ron Deibert**, Professor of Political Science and Director of the Citizen Lab at the University of Toronto
- **Tamir Israel**, Technology and Human Rights Lawyer
- **Brenda McPhail**, Director, Executive Education and Professor of Practice, McMaster University
- **Adam Molnar**, Assistant Professor, Sociology & Legal Studies, University of Waterloo
- **Alex Neve**, Visiting and Adjunct Professor of International Human Rights Law, University of Ottawa
- **Jonathan Penney**, Citizen Lab Fellow and Associate Professor at Osgoode Hall Law School, York University
- **Kate Robertson**, Senior Research Associate at the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
- **Jim L. Turk**, Director, Centre for Free Expression, Toronto Metropolitan University