International Civil Liberties Monitoring Group

MINUTES

SPRING 2024 GENERAL ASSEMBLY

May 29, 2024
9:45 am – 4pm EST
Hybrid format

Registrants: Khaled Alqazzaz (Canadian Muslim Public Affairs Council) Matthew Behrens (Campaign to Stop Secret Trials in Canada/Homes not Bombs), Rima Berns-McGown (IJV), Elizabeth Block (Canadian Friends Service Committee), Mohamed Boudjenane (Canadian Arab Forum), Tricia Brown (Unifor), Dawn Burns (CXCU), Maryève Boyer (COPE), Kelti Cameron (CUPE), Lina Chaker (Canadian Muslim Lawyers' Association), Xan Dagenais-Guertin (ICLMG Coordinator, Communications and Research), Mehjabeen Elahi (Islamic Relief Canada), Souhaila El Filali (Human Concern International), Martine Eloy (Ligue des droits et libertés), Pam Foster (Canadian Association of University Teachers), Rasha Hilal Al-Baiyatti (Inter Pares), Nadia Ibrahim (NUPGE), Hilary Homes (Amnesty International), Mahmuda Khan (Human Concern International), Kevin Malseed (Friend), Diana Martin (Mining Watch Canada), Tim McSorley (ICLMG Coordinator), Brian Murphy (Friend), Dominique Peschard (Ligue des droits et libertés), Roch Tassé (friend), James Turk (Centre for Free Expression), Sandra Wiens (Canadian Friends Service Committee)

Acknowledgement

We would like to begin by acknowledging that the land on which we gather is the unceded territory of the Anishinaabe Omàmiwinini (Algonquin people). We pay respect to the Anishinaabe Omàmiwinini, who are the original guardians of this land. We thank them for their stewardship of the land. We acknowledge their longstanding relationship with this territory, which remains unceded. We pay respect to all Indigenous people in this region, from all nations across Canada, who call this land home. We acknowledge the traditional knowledge keepers, both young and old. And we honour their courageous leaders: past, present, and future. We welcome the resistance and resurgence of Indigenous Peoples as part of the decolonizing process.

Welcome & go around

Rasha Co-Chairs first half of the assembly

1. **Welcome**
2. **Approval of the agenda**

Moved: Kevin
Seconded: Pam
Agenda approved.

3. Approval of the minutes from June 8, 2023, and November 29, 2023, Assemblies

June 8, 2023, minutes: changes requested at prior assembly have been made.
Moved to approve: Roch
Seconded: Kevin
June 8, 2023, minutes approved.

Moved to approve: Roch
Seconded: Rasha
November 29, 2023, minutes approved.

Point of clarification
Sameer Zuberi is a Montreal Liberal MP and long-time supporter of the ICLMG, formerly representing the Canadian Muslim Lawyers Association. He asked if we would be comfortable with him attending part of the meeting, but our process is that observers need to be approved not only by the steering committee in advance but also by the assembly. It appeared he would only be there for part of lunch and the activity report, which is public information, but not for strategy sessions.

Motion: Invite Sameer Zuberi to attend part of the assembly.
Moved: Corey
Seconded: Pam
Motion Passed.

4. Introductions and Member Updates
Nadia Ibrahim, staff at National Union of Public and General Employees, responsible for international solidarity work. Gaza has been all consuming. Another area of interest is related to artificial intelligence and its impacts on rights and civil liberties in the context of organizing in the workplace.

Souhaila El Filali, Executive Manager, Human Concern International, we are working on the situation in Gaza, working on humanitarian aid. Over 40 years in Canada and in more than 40 countries globally. Our CEO has joined online as well, Mahmuda Khan. Since October 7 advocating for rights of Palestinians to receive aid, and we were audited and suspended for one year. Working on the targeting of faith based, mainly Muslim, organizations by CRA

Elizabeth Block attends Quaker meeting and represents CFSC, which has a small committee to work on Middle East. A statement came out of Vancouver Monthly Meeting with a suggestion we ask Canada to recognize Palestine as a state, and also that we look at removing tax exempt status for charities aiding Israeli apartheid here in Canada.

Sarah, policy and legal research, Canadian Muslim Public Affairs Council, national organization dedicated to social justice, equity, inclusion, do policy, lobbying, research against Islamophobia, also a lot of grass roots efforts on community empowerment, support services, educational work, collaborating with civil society. Our executive director Khaled will join shortly.

Pam Foster**,** CAUT, doing a lot of work on the crackdown on campus encampments and freedom of expression. Also involved in on-line harms work

Mehjabeen Elahi, recently joined the Islamic Relief team as a government relations specialist. Eyes on Bill C41 as well as Gaza and more recently, we have a sponsorship program to sponsor orphans in Gaza—117 of our orphaned foster children have died in the war, the youngest being five, and that is only in the south, we don't even have statistics for North Gaza, yet which speaks to the dire situation there.

Corey Balsam, National Coordinator, Independent Jewish Voices, based in Montreal with 24 chapters. Our focus on Gaza and the backlash here against Palestine solidarity. Also involved in four injunctions, three related to encampments (McGill, UQAM, University of Toronto) and before that the injunction that prohibits

demonstrations in front of 24 Jewish institutions in Montreal. Regarding antisemitism, we have been working to prepare a response to the handbooks coming out about antisemitism and Islamophobia. I was surprised that I was allowed to see in advance the antisemitism pamphlet at Global Affairs Canada, but I could not take notes. It is very concerning, with a lot of focus on universities (concerning in light of recent interrogations of university presidents), recommendations for integrating IHRA the International Holocaust Remembrance Association, which has a problematic definition that equates antisemitism with critiques of Israel), law enforcement. Also concerned about the Justice Committee study on anti-semitism and potential recommendations that could impact on civil liberties, perhaps expanding what is already in the handbook.

Hilary Homes, Amnesty International, working on litigation connected to Gaza, apartheid, student encampments on right to protest, which is part of an international campaign that touches on Iran, Colombia, Peru, Russia, Sri Lanka, where anti-terrorism legislation is used to justify crackdowns. We released a report recently on China and transnational repression in academia, immigration detention, online harms act as well

Dominique Peschard, Ligue, a human rights group founded in 1963
In Quebec, published a journal on surveillance capitalism, intervening on a series of privacy and surveillance bills regarding the sharing of personal data, Quebec passed a special law on the management and sharing of health information. There is also a proposal to have a numerical identity which we will intervene on. Regarding protests at Quebec campuses, we are watching what is happening on the police side of things, including a quite violent response against a group of students who went outside of the campus and demonstrate din the streets. We denounced that brutality. We are part of coalition regarding Gaza genocide.

Martine Eloy: La Ligue joined with 46 other groups to form Quebec Coalition Emergency Palestine. La Ligue organized a press conference with Francesca Albanese, Special Rapporteur for Occupied Palestinian Territories and Joëlle Bedda (Al-Haq) for a group defending Human rights in Palestine. Albanese was clear about demanding sanctions against Israel. In addition to the main concern about the horrible crisis in Gaza, there are repercussions regarding right to free speech. We tried to print up position statements that we would pay for in newspapers to learn that anything that mentions Palestine has to go through the head leadership of the papers, and in one instance we had to share the tense of a verb. Every article seems to say October 7 was the beginning. Those supporting Palestine have been laid off. Coalition put out an appeal signed by hundreds of organizations and public personalities, and a second appeal has been distributed as well.

Sandra Wiens, new government relations for Canadian Friends Service Committee. We work on Indigenous human rights, peace and justice and ICLMG campaigns like Hassan Diab.

Roch Tasse, a friend and former national coordinator until Tim came on 8 years ago

Brian Murphy, a friend who was part of founding group of ICLMG and remains on the steering committee

Kevin Malseed, friend, was once with Inter Pares. I have been joining Ottawa demonstrations to shout into the open air instead of yelling at the TV. It's been a hard time and it is great to be here in person again.

Jim Sannes, Canadian Unitarians for Social Justice, Biggest concern now is animal agriculture pollution, Palestine and Israel, Indigenous rights. We do monthly webinars about current issues.

Rasha, Office and Finance Manager at Inter Pares. Civil liberties, human rights and social justice undergird all of our work, and we were a founding member of ICLMG. We believe the impact of all of our organizations together is more impactful than any of us working alone. We work with marginalized groups here and all over the world. The broad and vague nature of anti-terrorism legislation and heightened surveillance and policing provide

governments with tools to target and silence advocates and criminalize dissent under the excuse of maintaining national security and public order. One program we support involves reproductive rights and health in the Philippines and protecting our counterparts in the face of such regimes. The Filipino government introduced anti-terrorism legislation in 2020 that broadened the definition of terrorism and granted the authorities extensive powers to detain suspects without a warrant and increase surveillance. Since then women's rights and LGBTQ2+ advocates and our counterparts have faced increased harassment and threats and anti-terrorism rhetoric is being used to attack and discredit reproductive rights activists.

5. Financial update fundraising presentation

Fiscal year April 1 to March 31
Our revenue is in line with expectations, short by about $3,500. Some member and non-member contributions will come in later so those numbers will catch up.
Some new contributions are going toward our 20th anniversary publication.
Overall, we fell under expenses by about $2,000.
Salaries and benefits a bit higher given our health benefits. Last spring Steering Committee authorized additional national coordinator hours for 3 months.
Unrestricted funds at $17,130 and our reserve fund is now $33,000.

2024/25 Budget: adopted in late March by Steering Committee
Income is similar to last year's.
Expenses are higher, unsurprisingly. Largest is in salaries and benefits to address staff capacity issues. Xan will work 20 hours per week for 7 months and 25 hours the rest of the year timed to our busiest periods. Cost of living increase of 4% was approved.

There is a projected deficit of $6,156. We feel this is manageable. Xan will have more hours to send out fundraising appeals, and we have a new fundraising subcommittee with Pam Foster, Diana Martin, and Gavin Perryman, a longtime ICLMG supporter. We hope to make up the difference during the rest of the year.

Presently, we have $11,400 that have come in in the first couple of months of the fiscal year, with a $148 surplus.

Motion to approve budget
Moved: Brian
Seconded: Sandra
Approved.

6. Steering Committee Membership

Works to provide support and strategic advice in between assemblies. Right now, there are 13 people. Everyone in committee wishes to stay on with Rasha and Dominique as co-chairs. Thanks to Roch, Brian, Kevin, Pam, Hilary, Diana, Don, Fatima, Jim, Kevin (NCCM), Sima.

7. Activity Report

December 2023 – May 2024

1. **Legislative / Parliamentary work**

1.1 Bill C-20, *Public Complaints and Review Commission Act*

Bill C-20 would create a new, independent review agency for both the RCMP and CBSA. It would replace the current RCMP review body, and create the first ever independent review body for the CBSA. The creation of an independent review body for the CBSA has been a longstanding, key demand and advocacy priority of the ICLMG coalition.

Since the last assembly, ICLMG:

- Convened meetings with partner organizations and member groups to discuss the bill and coordinate strategy;
- Worked with colleagues to update proposed amendments following the House of Commons committee study of the bill;
- Sent a joint statement on recommendations to the Minister of Public Safety;
- Met with Senators Omidvar and Yussuff in January to discuss the upcoming Senate study of the bill;
- Met with NDP Public Safety critics Peter Julian and Alistair MacGregor to discuss further strategies for Third Reading and Senate study of the bill;
- Raised the lack of independent review with the UN Working Group on Arbitrary Detention.

1.2 Bill C-27, *Digital Charter Implementation Act, 2022*

Bill C-27 is the government's proposed update to Canada's private sector privacy law, namely the *Personal Information Protection and Electronic Documents Act*. It will also increase powers granted to the Privacy Commissioner, create a new tribunal, and enact a new *Artificial Intelligence and Data Act* (AIDA). While our primary focus is not on the private sector, there are key aspects of this bill that have an impact on national security, surveillance and privacy rights. AIDA will have more direct repercussions on our work, given the growing use of AI in surveillance capitalism and government surveillance.

Since the last assembly, ICLMG:

- Continued to organize meetings with partner organizations and privacy experts to discuss the content and advocacy strategy regarding the bill;
- Co-wrote, with the Right2YourFace Coalition, an open letter signed by 30 prominent groups and experts in December 2023 calling for a full public consultation on AIDA: https://iclmg.ca/public-consultation-for-aida/;
- Co-wrote an open letter signed by 60 prominent groups and experts in April 2024 calling for the withdrawal of AIDA from C-27: https://iclmg.ca/withdraw-aida/;
- Updated and promoted our letter-writing campaign calling for protection against facial recognition tech and surveillance: https://iclmg.ca/banfr/;
- Updated and promoted our letter writing campaign calling for the removal of the national security exemptions from C-27: https://iclmg.ca/action-c-27/;

1.3 Bill C-41, *An Act to amend the Criminal Code and to make consequential amendments to other Acts*

Humanitarian aid and international assistance generally is being hindered by Canada's anti-terrorism laws, particularly in Afghanistan – a risk ICLMG has long warned about. In Spring 2023, the government tabled Bill C-41 to ostensibly address the issue through amendments to the Criminal Code. Despite several remaining shortcomings, the bill received royal assent this past June.

Since our last assembly, ICLMG:

- Continued to participate in the informal C-41 legal working group to discuss implementation of Bill C-41 and the development of regulations;

- Participated in a Public Safety Canada briefing on the implementation of the provisions of Bill C-41and raised concerns around the proposed authorization process
- Raised concerns about the delays in the implementation of C-41with NDP Public Safety critic Alistair MacGregor
- Met with Asma Faizi, lawyer and president of the Afghan Women's Organization, for her study on the implementation of the provisions of Bill C-41

1.4 New "Online harms" legislation: Bill C-63

The federal government introduced Bill C-63 in February 2024. Known as the "Online Harms Act," it responds to many of our concerns with the government's original "online harms" proposal from 2021, but several aspects of the bill continue to raise serious concerns. Since our last assembly, ICLMG has:

- Continued participating in meetings of the "Online Harms Network";
- Read, analyzed and started to draft a brief on the bill;
- Met with a policy advisor to Justice Minister Virani about the bill in April;
- Signed onto a letter in May urging the Justice Minister to split Bill C-63 https://iclmg.ca/split-c-63-letter/.

1.5 New Foreign Interference legislation: Bill C-70

Although the federal inquiry into foreign interference continues its work, in May 2024 the government introduced new foreign interference legislation, Bill C-70. Much of it reflects proposals from a consultation held from December to February, but fails to respond to many of the concerns that we raised with the government. Since last assembly, we have:

- Participated in an online roundtable for the foreign interference consultation;
- Sent submissions in February to both Public Safety and Justice Canada for their respective consultations on legislative responses to foreign interference (which are now included in Bill C-70): https://iclmg.ca/foreign-interference-consultation/;
- Issued a press release with our preliminary reaction to the new foreign interference bill, which received coverage in several media outlets: https://iclmg.ca/foreign-interference-bill-release/;
- Started a thorough analysis of the bill to draft a more in-depth reaction and eventually a brief;
- Met with other Canadian and international civil society groups to discuss concerns with the bill;
- Participated in a technical briefing on the bill organized by the Special Rapporteur on Islamophobia;
- Continued to stay appraised of the commission and how we can offer our expertise of the impact on civil liberties which is severely lacking from the terms of reference.

1.6 Meetings with MPs & government officials and committee appearances

The ICLMG has continued to meet with various MPs, aids and government staff about the coalition's policies and priorities, including:

- Senator Ratna Omidvar regarding Bill C-20
- Senator Hassan Yussuff regarding Bill C-20
- NDP MP & Public Safety Critic Peter Julian regarding Bill C-20
- NDP MP & Public Safety Critic Alistair MacGregor regarding bills C-20, C-70 and other issues
- Dahlia James, Senior Policy Advisor to the Minister of Justice, regarding Bill C-63

More details on these meetings can be found in relevant sections of the Activity Report.

1.7 Concerns around meetings with Public Safety

Since July 2023, we have been unable to meet with officials from the Minister of Public Safety's office. Despite multiple attempts to meet with the new minister, the minister's chief of staff, the minister's director of policy, and the parliamentary secretary to the Minister of Public Safety, we have received one cursory response promising a future meeting. In late May, we finally received a response from Maja Kostic, Director of Policy to the Minister of Public Safety, to arrange a meeting with her and members of the policy team in the coming weeks.

2. Accountability and oversight

2.1 National Security and Intelligence Review Agency

As part of its work on accountability and review, the ICLMG continues to monitor and react to the work of the NSIRA. Since the last assembly this has included following up with NSIRA for details regarding their review of the CRA's anti-terrorism activities and recent review of CSIS' dataset regime.

2.2 Office of the Privacy Commissioner of Canada

ICLMG continues to engage with the Office of the Privacy Commissioner as part of our work on oversight and accountability. Since the last assembly:

- We participated in the OPC's quarterly civil society roundtable to discuss current privacy issues, including biometrics and Bill C-27;
- We participated in the OPC's consultation on guidance on the application of *PIPEDA* and the *Privacy Act* regarding biometrics. We shared our questions, concerns and recommendations with the OPC during an online meeting and in written responses to their online questionnaire.
- We read and reacted to the OPC report on the RCMP's "open source" internet surveillance under Project Wide Awake.

2.3 Parliamentary study of Transparency of the Department of National Defence

ICLMG was invited to appear at the House of Commons committee on National Defence's study on "Transparency of the Department of National Defence and Canadian Armed Forces." National Coordinator Tim McSorley spoke to:

- The Communications Security Establishment's problematic history of secrecy and evasion of accountability.
- The history of secrecy at the Department of National Defence, including in regard to the Afghan Detainee scandal and current concerns regarding defence intelligence activities

2.4 Review of national security legislation

Several pieces of national security legislation require mandatory review or renewal by Parliament. This year, three such pieces of legislation were supposed to be reviewed or renewed:

- National Security Act, 2017 (formerly Bill C-59) was meant to complete parliamentary review by June 2024
- National Security and Intelligence Committee of Parliamentarians (formerly Bill C-22) was also meant to be reviewed in 2023-24
- Section 83.3 of the Criminal Code which allows for preventative arrests if law enforcement suspect on reasonable grounds that it would prevent a terrorist activity, contains a sunset clause which expires in June 2024

ICLMG has worked to raise concerns about the lack of review with members of the Public Safety Committee, and has discussed strategy with the NDP around ensuring that clause 83.3 is not renewed.

3. Palestine and the right to dissent

The Israeli government, and its supporters, have attempted to justify their ongoing genocide against Gazans as "fighting terrorism," a view echoed by Canadian officials. ICLMG has continued to monitor the situation and take action. Since the last assembly, we have:

- Shared news, analysis, and joint letters calling for a ceasefire, an arms embargo and for Palestinian refugees to be let into Canada;
- We published a new statement and updated our original action calling on Canada to Oppose Genocide in Gaza and Defend Free Expression at Home: https://iclmg.ca/canada-must-oppose-genocide/;
- We published a new statement and accompanying action in May denouncing the conflation of criticism of Israel with terrorism and the accompanying calls and police actions to repress dissent, most recently against campus encampments: https://iclmg.ca/uphold-rights-at-encampments/;
- We participated in meetings of a new network of groups, convened by the BCCLA, working to address attacks on civil liberties in the context of support for Palestinian human rights.

4. Canadians detained abroad, torture & redress

4.1 Hassan Diab and Extradition

In April 2023, France proceeded with the trial of Dr. Hassan Diab, and in a miscarriage of justice, convicted him *in absentia* for the 1980 Rue Copernic bombing. We continue to advocate for Dr. Diab's rights to be protected and for reforms to the *Extradition Act*, including by:

- Sending a last-minute call to action to email Mélanie Joly on the eve of her diplomatic trip to France to urge her to advocate for justice for Dr. Diab;
- Updating and sharing our letter-writing campaign on the one-year anniversary of the unjust verdict;
- Sharing the new Parliamentary petition for Dr. Diab;
- Signing onto an open letter to the Justice Minister to commit to rejecting any second extradition request from France.

4.2 Canadians detained in Northeastern Syria

At least 17 Canadians, including 7 children, and three non-Canadian mothers remain indefinitely detained in camps and prisons in northeast Syria. In November, the Supreme Court of Canada declined to hear the appeal of four men challenging Canada's inaction in bringing them home.

Since our last assembly we have:

- Updated and promoted our letter-writing campaign in favour of repatriation of all: https://iclmg.ca/repatriate-all-canadians/;
- Supported and publicized the request that the Supreme Court reconsiders hearing the appeal of the families of four Canadian men detained in NE Syria;
- Raised the issue in a meeting with the UN Working Group on Arbitrary Detention.

5. Security certificates & inadmissibility

ICLMG has continued to work to eliminate security certificates, and defend the rights of those who are placed under one.

Since our last assembly this work has included:

- Updated and continued to push the Moe Harkat letter-writing campaign (as well as a holiday card campaign) on December 10 - the 21st "anniversary" of his arrest under a security certificate;
- Send a letter to the new Public Safety Minister for him to allow Moe to stay in Canada;
- Raised the ongoing issue of security certificates in a meeting with the UN Working Group on Arbitrary Detention.

6. Racism & Islamophobia

The ICLMG continues to oppose racial, religious and other forms of profiling and targeting by national security activities and laws, particularly that of Muslim and Arab communities and people of color. We are also aware of, and attempt to combat, the instrumentalization of acts of xenophobia, Islamophobia and racism to justify new or expanded use of national security laws. To that effect, since our last assembly we have:

- Highlighted the 7th "anniversary" of the Quebec Mosque shooting, which is also the National Day for Action Against Islamophobia, by remembering the victims and their families, and renewing our commitment to fighting islamophobia, including anti-Palestinian racism.
- Met with Amira Elghawaby, the federal Special Representative on Combatting Islamophobia, to discuss the rise of Islamophobia and anti-Palestinian racism in Canada following Israel's ongoing violence and attacks in Gaza
- Participated in a roundtable briefing on new foreign interference legislation organized by the Office of the Special Representative on Islamophobia;

7. Anti-terrorism, national security and international bodies

7.1 Canada's Universal Periodic Review (UPR)

We continue to engage in the process of Canada' 4th Universal Periodic Review at the UN Human Rights Council. Since the last assembly, we have:

- Participated in an online meeting with a consultation process organized by Equitas intended to gather the views of civil society regarding the state recommendations received by Canada at the United Nations on Nov 10, to help Canada formulate its response.
- We shared in writing which state recommendations Canada should prioritize, and which they should ignore: https://iclmg.ca/upr4-recommendations/. Our thoughts were heavily featured in Equitas final civil society report to the government of Canada.

7.2 Civil Society Coalition on Human Rights and Counterterrorism

The ICLMG continues to participate in the Civil Society Coalition on Human Rights and Counterterrorism. Since our last assembly this has included:

- Participation in quarterly coalition meetings to exchange information and strategize around impact of international counter-terrorism mechanisms on human rights in Canada and internationally
- Participation in quarterly working group meetings regarding impact of UN counter-terrorism activities on civil liberties and human rights

7.3 UN Counterterrorism Executive Directorate (CTED) Canada assessment

2023 year marked the second assessment of Canada's implementation of UN counterterrorism resolutions by CTED. Since then, we have continued efforts for the public release of their report on Canada. To that end we have:

- Remained in contact with CTED regarding the status of the report;
- Followed up with Global Affairs Canada on the status of the report and urging its release.

7.4 UN Cybersecurity Treaty

In January, we signed onto a joint statement with more than 100 groups calling for crucial changes to UN Cybercrime Treaty or to vote against it all together: https://iclmg.ca/amend-or-reject-100-groups-call-for-crucial-changes-to-un-cybercrime-treaty/

7.5 EU AI Convention

In February, we signed onto a joint letter with more than 115 other groups and experts urging the Canadian Government to Reject Private Sector Carve-Out in Council of Europe AI Convention Negotiations: https://onetreatyforall.com/

8. ICLMG Twentieth Anniversary publication

2022 marked the 20th anniversary the International Civil Liberties Monitoring Group. We are currently putting the final touches on a publication of short pieces that reflect on ICLMG's work and the challenges of defending civil liberties in the context of the War on Terror. The tentative publication/launch date is summer 2024.

9. Outreach, engagement and events

- Our social media accounts continue to increase in size and reach tens of thousands of people;
- We have published 10 editions of the News Digest since the last assembly;
- We sent and shared a fundraising appeal on Giving Tuesday at the end of November: https://iclmg.ca/giving-tuesday-2023/;
- In December, we sent out our biannual "What we've been up to" email: https://iclmg.ca/july-dec-2023/
- We sent another fundraising email (and posted on social media) in March after the introduction of Bill C-63 and all the work done and to be done around C-20, C-27 and foreign interference: https://iclmg.ca/help-us-expand-the-fight/
- We collaborated with the director and staff of the documentary, *Manufacturing the Threat*, to have ICLMG materials distributed at screenings, as well as sharing a discount code for ICLMG followers.
- In our last activity report we forgot to include that Tim spoke with the Confederation of Canadian Unions (CCU) on Artificial Intelligence at their Labour School the end of October 2023. The talk is online at: https://www.youtube.com/watch?v=63hcphjVkm0

10. Media & publications

Select media coverage and ICLMG publications since our last assembly:

10.1 Media coverage & interviews

"Licence to break the law: More Canadian spies get permission to commit crimes, memo shows," Chris Arsenault, CBC News, 6 December 2023: https://www.cbc.ca/news/canada/licence-to-break-the-law-more-canadian-spies-get-permission-to-commit-crimes-memo-shows-1.7043938

“Federal consultations on AI regulations heavily skewed toward businesses, industry groups, say critics,” Joe Castaldo, The Globe and Mail, 10 December 2023: https://www.theglobeandmail.com/business/article-canada-ai-law/

“Civil society groups call for AIDA to be considered separately from C-27,” The Wire Report, 14 December 2023: https://www.thewirereport.ca/2023/12/14/civil-society-groups-call-for-aida-to-be-considered-separately-from-c-27/

“Allow CSIS to share intelligence on security threats, business council asks Ottawa,” Jim Bronskill, The Canadian Press, 19 January 2024: https://www.ctvnews.ca/politics/allow-csis-to-share-intelligence-on-security-threats-business-council-asks-ottawa-1.6733127

“AI bill ‘democratically illegitimate’ and litigation ‘likely’ without proper consultations, say AFN, civil society orgs,” Stuart Benson, The Hill Times, 21 February 2024: https://www.hilltimes.com/story/2024/02/21/ai-bill-democratically-illegitimate-and-litigation-likely-without-proper-consultations-say-afn-civil-society-orgs/412203/

“Border agency eyes smartphone facial recognition system amid privacy concerns,” The Canadian Press, 24 April 2024: https://ca.news.yahoo.com/border-agency-eyes-smartphone-facial-184532765.html

“Feds advance ideas to fight foreign interference, prompting support and concern,” Jim Bronskill, The Canadian Press, 29 April 2024: https://www.cp24.com/news/feds-advance-ideas-to-fight-foreign-interference-prompting-support-and-concern-1.6866574

“Trudeau fait confiance aux universités pour gérer les manifestations sur leurs campus,” François Joly, Le Téléjournal, 3 mai 2024.

“Data privacy as a human right must be recognized by privacy and AI bill, say advocates,” Jesse Cnockaert, The Hill Times, 6 May 2024: https://www.hilltimes.com/story/2024/05/06/data-privacy-as-a-human-right-must-be-recognized-by-privacy-and-ai-bill-say-advocates/420721/

“Foreign influence registry among proposed tools in bill to counter interference,” Jim Bronskill, The Canadian Press, 6 May 2024: https://toronto.citynews.ca/2024/05/06/suite-of-legislative-measures-to-counter-foreign-interference-coming-today/

“Liberal foreign interference bill includes some 'good tools' for RCMP: commissioner,” Jim Bronskill, The Canadian Press, 7 May 2024: https://www.pentictonherald.ca/news/national_news/article_a4c5dd58-4961-561e-bcb7-674c7327a4aa.html

“Priorité au registre et au respect des droits,” Marie Vastel, Le Devoir, 21 mai 2024: https://www.ledevoir.com/opinion/editoriaux/813286/lutte-contre-ingerence-etrangere-priorite-registre-respect-droits

Check out all coverage of ICLMG in the media at https://iclmg.ca/about-us/iclmg-in-the-media-2/

10.2 Op-eds & online commentary

- We reacted to the news that the Trudeau government's use of Emergencies Act during 'Freedom Convoy' violated Canadians' Charter rights;

- We reacted to the news that Canadian spy agency's big data program is breaking the law according to a new NSIRA report;
- We reacted to the Office of the Privacy Commissioner of Canada's new report on the RCMP's "open source" internet surveillance under Project Wide Awake.
- We posted to mark the seventh anniversary of the Quebec Mosque shooting and the National Day for Action Against Islamophobia.

10.3 Press releases and statements

- Joint letter urges Justice Minister to split Bill C-63, May 7, 2024: https://iclmg.ca/split-c-63-letter/
- Provisions of new foreign interference bill will have much broader consequences on rights and freedoms in Canada, warns civil liberties coalition, May 7, 2024: https://iclmg.ca/foreign-interference-bill-release/
- Canadian coalition calls for urgent action to uphold civil liberties and Charter rights at protests and encampments across the country, May 3, 2024: https://iclmg.ca/uphold-rights-at-encampments/
- Key stakeholders call for withdrawal of controversial AI legislation, April 24, 2024: https://iclmg.ca/withdraw-aida/
- Advocates urge full public consultation on controversial AI legislation, December 14, 2023: https://iclmg.ca/public-consultation-for-aida/
- ICLMG statement: Canada Must Oppose Genocide in Gaza and Defend Free Expression at Home, December 8, 2023: https://iclmg.ca/canada-must-oppose-genocide/

11. Institutional and Governance matters

Since our last Assembly, ICLMG:

- Welcomed the Canadian Muslim Public Affairs Council as a new member!
- Held two Steering Committee meetings in January and March;
- Carried out annual membership fundraising activities;
- Worked with CAUT staff to update our accounting process
- Established a new fundraising subcommittee with Pam Foster (CAUT), Diana Martin (MiningWatch) and ICLMG supporter Gavin Perryman, with expertise in non-profit development, to make ICLMG revenues more sustainable on the long-term;
- Met with several ICLMG members to provide updates and discuss strategy;
- Worked to identify and recruit new coalition members;
- Worked with the co-chairs and Diana Martin to update staff contracts.

Comments: The fundraising subcommittee has met twice and will be coming forward with some new proposals.

8. Foreign interference and the expansion of anti-terror & national security powers, a presentation by Tim McSorley

The wide-ranging bill was introduced on May 6 and it's quite impactful for our work. It comes in four parts. It modifies the CSIS act; adds a section on measures to counter foreign interference which are modifying the Security of Information Act and the Criminal Code; there's measures relating to the protection of information, one of the more technical areas that changes the Canada Evidence Act; and there's the creation of a new Foreign Influence Transparency and Accountability Act. That last part has gotten the most attention because it creates the new foreign influence registry.

We have some overall concerns with the bill, but some context here recalls discussions previously at assemblies and at the steering committee about the extent to which we should be taking on issues around foreign interference. But as it's moved forward, and especially as the government held their consultation this winter on changes to the CSIS Act and the Criminal Code and other areas, we saw that with everything that's in this bill, it goes far beyond addressing foreign interference. These changes will impact how evidence is handled in courts and what evidence individuals will be able to access in terms of disclosure in national security hearings. It addresses what kinds of surveillance and warrant powers CSIS has access to (it already has access, but now it's making changes to what's considered access).

Something that I don't think we quite understood at first is the intersection of the Security of Information Act, which isn't often known. It's used to be the Official Secrets Act. That speaks not just of foreign entities, but also terrorist entities. They're making significant changes to what's included in the Security of Information Act, changing its name. That could have much broader implications for freedom of expression, especially if you're working in association with international organizations or foreign partners, or even work done in Canada that criticizes the Canadian government's foreign policy.

That could lead to being accused of being in line with a foreign government or undermining the Canadian state. It also undermines and undercuts the review of the National Security Act. For example, one of the first things in the legislation is changes to the CSIS dataset collection regime. That came in with C-59, and any review of that should have been part of a review of national security laws. But instead, they've lumped it in with a review of foreign interference measures. During the winter consultations, not many people who work on these particular issues were involved in those consultations or submitted briefs, because it wasn't clear to them that CSIS data sets would be the subject of a foreign interference consultation. So this was introduced in a way that limited participation.

In terms of civil society groups that we work with, only ICLMG and the Canadian Muslim Lawyers Association had the capacity to submit briefs, because most groups that we spoke to didn't know that this was part of it. There were roundtables held and we participated in one of them, but in those fora, you're learning about the provisions as you go, so it's hard on the fly to give specific, concrete feedback. There was an online consultation where you could submit a longer written document; it wasn't a scientific survey, and unsurprisingly, it came back with 85%, 75% support for every single measure that CSIS is asking for.

I imagine if we got the breakdown of who was going on to the site to actually vote, a lot of them wouldn't be groups that have actually been critical of CSIS work.

Part one is the Canadian Security Intelligence Act. It modifies the data set regime, which allows CSIS since 2019 to collect information that isn't directly related to their investigations to protect the security of Canada. Before that, CSIS was much more restricted in what they could collect, and were expected to destroy any information they collected that wasn't directly related to their mandate. But they were found by the courts in 2016 to have been retaining that information that they were collecting alongside the more targeted information under the guise that this would help predict threats and provide a better understanding of national security issues in Canada.

The courts told them they had to shut it down and get rid of it. Although they stopped, within three years, they've adopted new legislation to legalize that work. But since then, CSIS has found that it's too restrictive (a complaint we had warned about). In this bill, they're asking to modify the regime. In terms of the changes to the data set regime, the way it was interpreted was that they would be able to collect their target information and they would have a separate stream of collecting data sets. But what's actually being realized (and this was in a

report from the National Security Intelligence Review Agency just about a month ago) was that CSIS interpreted things differently. When they're ostensibly collecting threat-related information, if they're collecting excess information that they don't think is related to the threat, they're just throwing it into data sets, which isn't how it was proposed and how CSIS originally talked about it, even internally.

Over time, they've just combined the whole thing into a machine for collecting information, which they justify by saying this is more flexible because it cuts down on delays, allows them to act on the information more quickly, and it doesn't become outdated. Essentially, it's rewarding them for again deciding how they would like the law to work and the government modifying it to work better for them. In addition, it allows them to collect data sets from outside Canada, as well as disclose data sets to third parties. Until now, there were strict rules around what CSIS can disclose. But this would allow them to share data sets and databases of information with any entity: local, domestic and foreign. There are also different levels of authorization. If it's a publicly available data set, they argue it's just information they can collect because it's out there. We still challenge whether they should be allowed to just do that, but they are doing it and they're saying that they can disclose that information without any form of authorization or oversight. This is very troubling and problematic for foreign data sets.

Currently for Foreign Intelligence activities, CSIS can only collect information "within Canada." C-70 would allow CSIS to collect "from within Canada information or intelligence that is located outside Canada if the assistance is directed at a person or thing in Canada or at an individual who was in Canada and is temporarily outside Canada."

They need a ministerial authorization to do that collection. Now they're saying, "we want to be able to share those data sets with ministerial authorization as well." For Canadian data sets, they need judicial authorization to hold on to them, and they would need judicial authorization to disclose them. There are still levels of authorization, but originally, they were never supposed to be able to share these data sets. We have questions about who they want to share these data sets with, and what kind of reporting and accountability there will be around sharing that information. A big question is whether or not data sets as bulk information should be something that they can just share completely, or rather (while it is still problematic), sharing targeted pieces of information.

Question: Would sharing with third parties cover, for instance, the meetings that CSIS had with mining companies and sharing information they had on opponents?

Answer: In theory it would. There's another section they're adding that would actually be more suited to sharing information with mining companies and others. But my understanding is that at least for the publicly available information and datasets, they would be able to share it with private entities as well with corporations. Their argument is that it's public already so it doesn't matter if we share it, since the private entities can find it somewhere else. My understanding is that there is no further restriction on who it can be shared with.

Another area that's changing in the CSIS Act is that right now, there are three broad mandates. One is addressing threats to security of Canada, and to do that, they can operate within Canada and outside of Canada. They also provide foreign intelligence assistance to Foreign Affairs and National Defence, but they've been limited in that work because the CSIS Act said that they can only do that work from within Canada. The courts have interpreted that as meaning that the information that they collect has to be within Canada, too.

CSIS has been arguing and asking for warrants to be able to collect information when, for example, they're investigating somebody in Canada in terms of foreign intelligence, but that person's email account is held on foreign servers and they want to access that email account. They couldn't get a warrant to do so because the wording of the law was that they have to operate within Canada. So this change would allow CSIS to operate

from within Canada and collect intelligence that is located outside of Canada if the assistance is regarding something directed at a person or thing in Canada, or an individual who was in Canada is temporarily outside of Canada.

If they wanted to access my email and my email account was held on a server in the United States, this would now allow them to obtain a warrant to access my email account. If they were investigating you for foreign intelligence purposes, they argue that's a technical solution to a problem where it used to be that if an individual was in Canada, all their information was in Canada. When the CSIS Act was adopted in 1984, that made sense. While today it's changed, there was a reason why they had that restriction in the first place. Just because it seems technologically necessary to have that change now doesn't mean that it undoes the reasons for having that restriction. That restriction is because CSIS isn't meant to be a foreign intelligence agency. Our question is how targeted will these new surveillance powers be? Will they go on fishing expeditions on foreign servers once they have a warrant to go look at somebody's email or somebody's account, and will they argue that to find their account, they have to go through 20 other accounts? And if so, will they keep everything they find because that's what they do? Even though they say that the judicial authorizations for this will be targeted, we know that they constantly push the envelope.

The main area that touches more directly on foreign interference in the changes of the CSIS Act is their power to disclose information. If the information is personal or private information dealing with individuals, they currently need the Minister of Public Safety's authorization to share that with ministers or people in the federal government. Now they're changing it to be any person or entity. Thus, the minister could authorize access to be able to share information if it's in the public interest on any person or entity, which is a broad expansion of their powers. The example given to me was that if there is a specific threat of foreign interference from an individual, they want to be able to share that with community partners in order to address that foreign interference threat. That in itself raises questions as we know that CSIS shares information that is inaccurate and biased. They target communities. It also raises questions of what kind of entities will be receiving that information. And it won't simply be limited to foreign interference. They could use it for any part of their mandate. That alone raises significant concerns, even though there's ministerial authorization required. The other area of disclosure that would be added is that they would be able to share information that doesn't contain personal details with any person or entity for the purpose of building resiliency against threats to the security of Canada. So, it's not restricted to foreign interference. It's only restricted to threats to the security of Canada. It would include personal information. They would now be able to share information without any form of oversight so long as it's not private information. Even though one of the major concerns is sharing information about individuals, we know from the past about CSIS engaging in racial profiling and targeting specific communities. We raised this in the meeting with CSIS last week with the representative on Islamophobia's office, and they said their goal would be to create public facing documents, that there will be a process around it, to try to reassure us.

But of course, none of that's in the law. At a minimum in other sections of Canadian laws, when agencies engage in information sharing for national security purposes, there's strict rules around who you can disclose to and why they can request that disclosure: there's keeping and sharing those records with the National Security Intelligence Review Agency; the ability to verify the accuracy of that information; the requirement to destroy that information once it's been used or it's no longer needed. But we don't see any of that here. It could be used to share information with universities to talk about general threats in relation to sensitive research. But it's not restricted to that. This could easily be used to further support CSIS meeting with mining and natural resource companies that have targeted Indigenous communities and branded them as extremists for being land defenders, with no reporting or accountability.

Question: Would this aspect of CSIS work not be subject to NSIRA overview?

Answer: NSIRA would be able to look at it, but there's no provisions for them to do record keeping. They could ask, but CSIS may be able to say, “well, here's what we have,” but they may not share everything with them. For the ministerial authorization, there's a specific requirement where they need to share with NSIRA every time they make a disclosure under the ministerial authorization. But there's no requirement for the broader information sharing information disclosure. So, at a minimum, at least with a ministerial authorization, NSIRA knows that it's happening and there's a record of it. But, for the more general purpose of building resiliency, which we don't have a definition of, my understanding from reading the bill is that it doesn't apply to that part of information sharing. It only applies to the ministerial authorization.

Under the bill they’re also looking at granting CSIS new powers of preservation and production orders. CSIS right now has a more complicated warrant application process than law enforcement agencies. Preservation production orders would allow them, if somebody has a document they want to look at, to preserve that document so that they don't destroy it. It will become illegal for them to destroy that document while they get a production order. The production order is different from a search warrant, in that it's only to request the person to produce a specific thing that they're asking for, rather than CSIS going in and searching an area for a specific thing. But in speaking with some lawyers, it seems these specific powers aren't as concerning because it would actually reduce the need for CSIS to go in and search given it is a more targeted request.

Nonetheless, anytime CSIS is given more police-like powers it's a concern. Right now, CSIS has a one size fits all warrant. They argue that they need more targeted kinds of warrant powers. But the concern again is anything that would allow them to go into a place to search in secret and to take any particular thing, read any document, make copies of things, surreptitiously and secretly. It's still with judicial authorization, but what it removes is what they call investigative necessity. Usually for their warrants, they have to prove that they've exhausted all other methods before they can obtain a warrant to do something secretly or something that would breach the Charter.

But now they don't need to say that they've exhausted everything else. They're saying, “we think this would be easiest for us, and so we want you to authorize this.” The judge could still say “no, I'm not going to authorize this,” but the history shows courts have a very mixed record about what they are willing to authorize. This is more worrisome than the production orders.

The last thing that it does do, and it's fairly non-controversial, is mandate a five-year review of the CSIS Act. From their perspective, it would allow them to update and modernize the CSIS Act on a more regular basis. From our point of view, it could provide an opportunity to criticize CSIS and ask for their powers to be reduced, but it doesn't often work that way. Hopefully in these reviews information will come out around how CSIS is using these powers. But then again, if we look at the record of Parliament actually sticking to these review schedules, at least in terms of national security legislation, they hardly ever meet them, and there's no penalty if they don't do it. So, it's to be seen if this will actually have any impact at all, if they would actually carry out a five-year review, or if it would just be something on the books for the next 20 years that’s never used.

The argument that they're using in large part to justify a lot of these changes is that the CSIS Act hasn't been modernized in 40 years. But we know that's not true. So, it's something that we've tried to push back on in both our submissions and in the consultations that we've been holding, that there's been lots of opportunities to update the CSIS act. With Bill C-51 and C59, they updated the Act.

Part 2 of the Act is measures to counter foreign interference

They are changing the Security of Information Act to now be the Foreign Interference and Security of Information Act. The wording of one of the sections of the act is “Foreign-influenced or Terrorist-influenced”

acts that undermine the Canadian state and security of Canada. It's rare to see the counterterrorism aspects used. They're expanding it to now be the foreign influence or terrorist influence, *intimidation, threats or violence.* It adds intimidation to various offences under the act, but there's no definition of intimidation and it's unclear where the line is between a threat and intimidation. If threat is only specifically a threat of violence, intimidation could be interpreted as threats of other things that fall short of an actual threat of violence. But we haven't been able to get a clear idea yet of what intimidation will entail, because that could obviously broaden what is considered a foreign influence or terrorist influence. The broader it gets, the bigger it gets, and thus the more possibility that it's misused (and in fact, the university demonstrators are being accused of intimidation).

Up until now, the threat has had to be tied to an act that would undermine the security of Canada, but that's being removed, and now it's simply engaging in an act influenced by a terrorist or foreign entity that would be considered an offence.

Question: What about the red triangle associated with Hamas, and whether that is necessarily linked with the group or is influenced by that.

Answer: It has to be at the direction of, for the benefit of, or in association with. There's a question of what "in association with" means. Does Hamas have to know that you're working in association with them? Are you doing something to benefit them? It does have to be in line with a terrorist entity, but it doesn't have to be a listed entity. Take the Muslim Brotherhood for example. There's no consensus in the Canadian government about whether or not they should consider the Muslim Brotherhood a terrorist entity. It's not listed. But we know that, for example, CBSA officers deny people entry into Canada on the grounds of there having been involved with either the Muslim Brotherhood or political parties that are aligned with the Muslim Brotherhood, like the Freedom and Justice Party. So, it's incredibly broad. What they consider a terrorist entity based on what they do doesn't have a set list; thus it could be interpreted broadly. There's the wording here that every person who commits an indictable offence under this act or any other act at the direction of, for the benefit of or in association with a foreign entity (and that includes a terrorist entity) is guilty of an indictable offence and is liable to imprisonment for life.

This one is a little bit more restricted than the previous one because when they only say foreign entity, they define a foreign entity as being a few different things. One is a foreign entity working in conjunction with a terrorist entity. So, for example, if they say Hamas is working in conjunction with the Iranian government, that would trigger this. Although this is slightly more restrictive, it's very easy for them to get around because there's often arguments that most terrorists or terrorist entities have some link to some government either through funding or association. This is a brand-new offence and a very broad one. It also means that you can be engaging in an offence that would normally have a lesser sentence (like arson) which is an indictable offence. But if they believe that was done in conjunction with a foreign entity, then you would be facing life in prison for a crime that maybe otherwise would face two years less a day or five years. This automatically opens up a possibility of life in prison if they are able to prove that it's at the direction, benefit of or association with (which isn't clearly defined in the legislation).

There's a new offence of engaging in surreptitious or deceptive conduct. If you're working for the benefit or in association with a foreign entity, if you engage in surreptitious or defensive conduct or admit that you are, if it's for a purpose that's prejudicial to the safety or interests of the state, where the person is reckless as to whether their conduct or omission is likely to harm Canadian interests, that's also an offence. Say you're working secretly with someone and with an entity, and your purpose is prejudicial to the safety or interests of the state (which again is very broad, it's not limited -- the wording of security of Canada is actually defined in the CSIS Act but the safety and interest of the state is not defined specifically). It could also be that you're reckless. If they can prove that you weren't diligent in assuring that what you were doing isn't going to be prejudicial to the interests of the

state, and that you're doing it secretly (a surreptitious act could just be not disclosing it), you could be facing an offence that would also be punishable by life in prison.

Question: If I work for an NGO and we receive some funding from a foreign organization and they decide that I've omitted to tell CSIS something, then I can be imprisoned simply because of it?

Answer: It has to be prejudicial to Canada in their determination.

Question Is there any other case of a non-criminal offence that is liable to life imprisonment?

Answer: With the Criminal Code changes to create a new hate offence, it doesn't need to be tied to a criminal offence. It simply means if you commit an offence with hate motivation then you can be facing life in prison. There's a lot of similarities between what's being created here and what's being proposed in the online harms bill.

Comment: One of the things which is striking is how a lot of the conditions are not factual, they're impressions, so if you think that the person *could have* done something that *could be* in the interest of, it seems to be contrary to what has been our Criminal Code.

Continuing the presentation
They're also creating an offence of influencing a series of political or governmental processes. It's punishable by life imprisonment if it's surreptitious or deceptive conduct with the intent to influence a political or governmental process, educational governance, the performance of a duty in relation to such a process or such governance or the exercise of a democratic right in Canada. It's very broad. Educational governance is a completely new term that we're still trying to understand.

For example, if a student encampment is viewed as interfering somehow with the governance of an educational institution or influencing it in a surreptitious way, could that be considered an offence under this Act? Beyond the educational governance, it defines political or government process as: any proceeding of a legislative body; the development of a legislative proposal; the development or amendment of any policy or program; the making of a decision by a public office holder or government body, including the awarding of a contract; the holding of an election or referendum; and the nomination of a candidate or the development of an electoral platform by a political party. So, anything that's surreptitious or deceptive in conjunction with a foreign entity, that could influence (and not even necessarily negatively) any of these bodies would be considered an offence liable to life in prison. It applies to federal, provincial and municipal governments and Indigenous governance bodies.

They hold up as being the safety valve on all this that the charges need to be approved by the attorney general. It can't just be a local Crown prosecutor who decides it. But it still doesn't provide that much comfort in terms of how these could be used, the chilling effect that it could have. It's definitely not beyond the scope of an attorney general acting in a political manner in deciding which charges to lay or not.

Question: I suppose this would not apply to an editorial for the *National Post* on the eve of an election when the majority shareholders are Americans.

Answer: They're Americans, but it's not the American government that's the shareholders. So, they would be okay.

Comment: But it would apply to all of us who are engaged in international solidarity for the government of Venezuela or if you're in support of an entity that the Canadian government has complex relationships with.

Question: When it says foreign entity, is there any sort of past definition?

Answer: A foreign entity is a foreign government, a group of foreign governments, an individual working on behalf of a foreign government or a group of foreign governments and, a foreign government and a terrorist and a terrorist entity working in conjunction with either a foreign government or a group of foreign governments is considered a foreign entity.

Question: What about a state-owned entity?

Answer: That's a foreign economic entity. That doesn't actually apply to this section. But it does apply to the registry. But they're pretty clear that this is only foreign entities and doesn't apply to the foreign economic entities. Jim Turk and I met with the Criminal Lawyers Association who are starting to analyze the bill. They'll probably catch a lot more and know for sure whether or not foreign economic entities would be captured by this section as well. But it doesn't seem so at first glance.

Question: Does this include advocating for Israel?

Answer: It could be if it's done in conjunction with the Israeli government, depending on what process it's under. So, it could capture working surreptitiously or deceptively with the Israeli government, but it's a question of whether the attorney general lays charges in that situation, or are they more likely to lay charges if they believe somebody is working surreptitiously with the Iranian government or the Indian government or somebody else that we're at odds with?

There are new changes to the Criminal Code for the sabotage offences and there's one actual improvement. For the general sabotage offence against military installations, they've actually added an exception that excludes advocacy, protest or dissent, so long as it does not intend to endanger the safety, security or defence of Canada or foreign military lawfully present in Canada. But it also creates a whole new sabotage offence for interfering with essential infrastructure with the same safeguard in place around protests and work stoppage and labour action as well. The list of essential infrastructure is very broad, including “a facility or system, whether public or private, that provides or distributes services that are essential to the health, safety, security or economic well-being of persons in Canada, including the following: (a) transportation infrastructure; (b) information and communication technology infrastructure; (c) water and wastewater management infrastructure; (d) energy and utilities infrastructure; (e) health services infrastructure; (f) food supply and food services infrastructure; (g) government operations infrastructure; (h) financial infrastructure; and (i) any other infrastructure prescribed by regulations.

If you engage in an activity that essentially threatens the security of Canada to the health or security of Canadians or any sector of the Canadian public, you could be charged with a sabotage offence. They admit that this has nothing to do with foreign interference, but they wanted to update the Sabotage Act.

Comment: The list of infrastructure looks similar to something in one of the other national security bills (C51).

Answer: Also similar to the Security of Canada. Information Disclosure has a similar list. They're allowed to disclose information related to those threats. One of the things that's come up is that they talk about critical infrastructure in other pieces of legislation where it is defined and there's jurisprudence, but “essential infrastructure” is completely new. People have asked why all of a sudden they’re inventing this term of

“essential infrastructure” when we already have an idea of what critical infrastructure means. They say they want to go broader because often critical infrastructure hasn't included, for example, health services or food supply.

The Transparency and Accountability Act would create a new foreign influence transparency commissioner who would be appointed by the Governor General through a very similar process as the appointment of other commissioners, like the Privacy Commissioner. They would be independent, in charge of running the foreign influence transparency registry. There are three components that would trigger registration. One is that you would have to be working in conjunction with a foreign principal. This isn't if it's done surreptitiously or secretly, or any money is exchanged. It's simply that you're working for the benefit of or in association with foreign principals: foreign power (a foreign state government), a foreign entity, a foreign economic entity (a private corporation that is substantially owned by a foreign government). There are questions about what substantially means (ownership versus control over). The difference between foreign power and foreign state is a foreign power could be a group that seeks to obtain government in a foreign state. It could be a rebel group, it might be a political party, but clarification is needed here. It could also be the de facto government of an area or a region. The influence activity must be undertaken at the direction of, or in association with a foreign principal. That includes any communication with a public office holder, any communication or information to the public, and any disbursement of money or items of value. In the third piece of the process, you have to be doing so to influence a government process. They define that as the development of any policy, program or legislative proposal, proceeding of a legislative body, decision making by a public office holder, nomination of a political candidate, or the holding of an election or a referendum. If all three of those things come together, then you would have to register.

Right now, the very narrow exemption is essentially for foreign diplomats, but they're saying it provides for regulations to broaden who would be considered exempt. One example that's come up is regarding a state owned or public broadcaster or a public academic institution. Are you working in association with them to communicate information to the public about decision-making by a public office holder (for example, working to vote against Bill C-70). If so, you may need to register on this foreign influence registry, even though what you're doing isn't actually influenced by them, but it's in association with them. There's vagueness around the concept of association which raises significant questions around what the cut off is. Benefit is maybe a bit more clear, but even then, what does it mean to actually benefit someone? If you don't register, if you fail to fulfill your responsibilities under the law or you provide any false information, you could be convicted on indictment and fined up to $5 million or five years in prison or both, or on summary conviction, a fine up to $200,000 or two years less a day in prison or both. So there's significant penalties for a fairly broad requirement to register.

Question: We know that the Israeli government has an action plan to engage in covert operations in the US to crack down on antisemitism. That involves pressuring donors, doxxing, etc. We assume that's taking place here as well. Does that type of operation qualify?

Answer: It could be a mix under the Security of Information Act (viewed as intimidation) and could possibly be covered here because it's surreptitious. We’d have to see how they judge the impact. For the registry, they would be excluded because its diplomats engaging in that activity. But it’s unclear if they're doing it in secret and not talking about it publicly whether or not it could trigger one or the other kind of offences.

Comment: It seems we cannot talk about this without looking at the power shifts in the world between different countries. There are countries that are demonized. We saw with the war in Ukraine how people coming for some cultural presentation, a pianist or a sports person, could not be admitted because suddenly the whole population of this country became a threat to Canadian security. It seems to me that we're moving towards a

new Cold War, a new period of McCarthyism. When you look at all the details in this, it seems to me to be laying the groundwork for precisely that. We mustn't forget to place this in the big picture, because we could get bogged down arguing on one item or the other. The United States is a foreign power, so could we apply this to them? But we don't think of the United States when we read this; in our minds, we know it's China, Russia. How do we deal with this without contributing to a climate of xenophobia in the interests of a certain number of Western countries?

Answer: They want to engage in second reading before the house rises. If they institute closure on the debate, they could even have it at committee before the House rises. The Conservatives have said they want to help the Liberals run this through. With respect to the Commission on Foreign Interference, ICLMG received standing for the policy phase of the commission, and we are looking to participate in round tables or provide feedback to the commission on what they should be keeping in mind in terms of their policy proposals.

9. The new Online Harms Act: Breaking down Bill C-63, a presentation by Domonique Peschard

Bill 63 was introduced three months ago. The long title ("An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*")* reflects the deplorable tendency of the government to tack on all sorts of items in its bills which don't have a direct relation with the main purpose of the bill. They are, in many respects, scandalous. There are five sections to this bill.

The main part of the bill is the Online Harms Act. What is harmful content in this act? It's defined as:

- Intimate content communicated without consent
- Content that sexually victimizes a child or revictimizes a survivor
- Content that induces a child to harm themselves
- Content used to bully a child
- Content that foments hatred
- Content that incites violence
- Content that incites violent extremism or terrorism

We challenge having such a broad range of content under one bill. For each of these forms of content, there's a definition. Below are the main concerns of the ICLMG.

Regarding fomenting hatred: *"*content that, given the context in which it is communicated, is likely to foment detestation or vilification of an individual or group of individuals on the basis of such a prohibited ground within the meaning of the Canadian Human Rights Act." It's essentially a definition of hatred which is compatible with the Criminal Code. There is an added element: "For the purposes of the definition, content does not express detestation or vilification solely because it expresses disdain or dislike, or it discredits, humiliates, hurts or offends." This is in alignment with the way the Supreme Court has defined the limits of hateful content.

Regarding content that incites violence:

"Content that actively encourages a person to commit — or that actively threatens the commission of — an act of physical violence against a person, or an act that causes property damage, and that, given the context in which it is communicated, could cause a person to commit an act that could cause: (a) serious bodily harm to a person; (b) a person's life to be endangered; or (c) serious interference with or serious disruption of an essential service, facility or system."

Item C is also present in the Anti-Terrorism Act (ATA), except in the ATA, there's the added specification after C that this must be other than as a result of advocacy, protest, dissent, or stoppage of work that is not intended to result in the conduct of or harm referred to in any of the clauses A or B. This protection, if you could call it that, from the ATA is not present in the definition within the context of this new act.

Re: Content that incites violent extremism and terrorism:
"Content that incites violent extremism or terrorism means content that — for a political, religious or ideological purpose, and given the context in which it is communicated, could cause a person to commit an act that could cause

- (a) serious bodily harm to a person.
- (b) a person's life to be endangered; or
- (c) a serious risk to the health or safety of the public or any section of the public

In order to enforce Online Harms Act, the bill enacts three bodies: a Digital Safety Commission of Canada (DSCC), a Digital Safety Ombudsperson of Canada and the Digital Safety Office of Canada.

The Digital Safety Commission of Canada is the most important of these bodies. It has, a lot of powers and it will determine in many ways how the Act will be implemented. The composition of the Commission is 3 to 5 full-time members appointed by the Governor in Council. The mandate of the Commission is to: ensure the administration and enforcement of this Act; ensure that operators are transparent and accountable (a positive); investigate complaints relating to content that sexually victimizes a child or revictimizes a survivor, and intimate content communicated without consent; and develop standards and regulations with respect to online safety. A lot in this bill is left to regulations. And the Commission has a lot of powers to regulate how this Act will be implemented. The Commission may issue guidelines, codes of conduct and other such documents for the purpose of this Act. It has lots of powers to regulate online harms. The Commission must take into account freedom of expression, equality of rights, privacy rights, the needs and perspectives of the Indigenous people of Canada and any other factor that the Commission considers relevant.

The phrase "must take into account" is important given we are talking here about Charter rights, freedom of expression, equality rights and privacy rights. It doesn't say the Commission must respect Charter rights; it says they must be taken into account. The requirement is not standard and in my opinion, it's not very high. The Commission can order the provider of a regulated service to make available to a researcher the electronic data related to the purpose of this Act. To make accessible to somebody who wants to research how harmful acts are treated by a regulated service opens the door to, for example, university researchers doing research on how these powers are implemented.

In terms of administration and enforcement, the Commission has lots of power. In ensuring an operator's compliance with this Act or investigating a complaint the Commission may summon and enforce the appearance of persons before the Commission and compel them to give oral or written evidence on oath, and to produce any documents or other things in the same manner, to the same extent as a court of record. It can also receive and accept any evidence or information, whether or not it would be admissible in a court of law. The Commission is not bound by any legal or technical rules of evidence. It must deal with all matters as the circumstances and considerations of fairness and natural justice permit. The Commission may designate inspectors and an inspector may, for the purpose related to verifying compliance with this Act, enter any place in which they have reasonable grounds to believe that there is anything relevant to that purpose; and examine any document, information or any other thing that is found in the place, or take it for examination and copy it.

They don't need a warrant to do that. They only need a warrant if the information is in a private dwelling. But if they want to see the information of a service provider, they have the power to do so.

There's lots of accountability on the part of the service providers to the Commission. They have to report to the Commission how many online harms complaints they've received, how they've treated them, and they even have to report on things they've taken off online platforms which are not related to the Act as such, which are not even online harms as defined by this Act.

The Digital Safety Ombudsperson of Canada is appointed by the Governor in Council, and: holds the office on a full time basis for a renewable term of not more than five years; has the mandate to provide support to users of regulated services; advocates for the public interest with respect to systemic issues related to online safety; gathers information with respect to these issues; and highlights issues related to online safety. It's someone the public can address if it has questions, and it also has a mandate to improve the situation with respect to online safety, and make proposals.

The Digital Safety Office of Canada's role is to support the Commission and the Ombudsperson in the performance of their mandates. There's a duty to report on the part of the Commission within three months after the end of each fiscal year to submit a report of its activities to the Minister and the same for the Ombudsperson. The Minister may request from the Commission or the Ombudsperson a report on any matter within their respective mandates. The Minister must cause each report to be laid before each House of Parliament. The positive aspects of this bill are the amount of accountability and transparency.

What is regulated by the bill?
The duties imposed on the operator do not apply in respect of any private messaging feature of a regulated service that does not enable a user to communicate content to a potentially unlimited number of users not determined by the user. Private messaging services are not connected to this bill.
A service is not a social media service if it does not enable a user to communicate content to a potentially unlimited number of users not determined by the user.
A regulated service is a social media service that: has a number of users that is equal to or greater than the significant number of users provided for by regulation (remains to be determined), or is designated by the Governor in Council if it is satisfied that there is a significant risk that harmful content is accessible on the service.
The Governor in Council may make regulations establishing types of social media services, the number of users for each type of social media service and the manner of determining the number of users of a social media service.

What are the duties of the operators of the regulated services?
One positive aspect: Nothing in this Act requires an operator to proactively search content on a regulated service that it operates in order to identify harmful content. The operator of a regulated service must implement any measures that are provided for by regulations; make user guidelines publicly available on the service, which must include a standard of conduct that applies to users, and a description of the measures that the operator implements with respect to harmful content. Further duties of operators of regulated services mean they must implement measures that are adequate to mitigate the risks that users of the service will be exposed to harmful content. To determine whether the measures are adequate, the Commission must take into account the following factors: the effectiveness of the measures in mitigating the risk; the size of the service, including the number of users; the technical and financial capacity of the operator; whether the measures are designated or implemented in a manner that is discriminatory on the basis of a prohibited realm within the meaning of the Canadian Human Rights Act; and any factor provided by regulations.

The operator is not required to implement measures that unreasonably or disproportionately limit users' expressions under regulated service. At first reading it may sound positive, but when you reread it, it means that in fact, the operator can implement measures that limit users' expression on the regulated service. It's just that they're not required to go overboard and eliminate users' expression. When you take into account that the Commission, in establishing regulations, must only "take into account" Charter rights then it would appear that the criterion for removing content is not the same as free speech as guaranteed by the Charter and the Criminal Code.

In the Criminal Code there's the awful but lawful speech, which means that in order to be unlawful, you have to meet the fairly narrow standards as determined by the Supreme Court. But here with this Act, you can ban awful but lawful speech. How far will they go in banning awful but lawful speech? That is quite open because it's all going to be determined by the regulations and by the standards of the Commission. So that is a cause for concern.

The operator of a regulated service must make available to users tools to block other users from finding or communicating with them on the service. That's a positive. For example, a woman who's harassed by her ex can ask the service provider to block the ex from communicating with her. The operator of a regulated service must implement tools and processes to enable a user to easily flag to the operator harmful content, notify a user who flagged the content of any measures taken by the operator with respect to the content, or the fact that no measures were taken (i.e. the content was not removed); and notify a user who communicated content that was flagged of the fact that the content was flagged as well as of any measures taken by the operator with respect to the content or of the fact that no measures were taken.

That leaves a lot of power to the operator to remove content. The operator of a regulated service must not notify a user of any report that the operator has made to a law enforcement agency in relation to the content. In previous proposals that the government put forward all the content reported to the operator had to be transmitted to law enforcement; that is not present here, but an operator can report content to law enforcement, and if it does, they must not notify the user that they have flagged his content to law enforcement. The operator must label as harmful content that which is the subject of multiple instances of automated communication (bots are considered harmful content); and must submit a digital safety plan to the Commission. If the operator of a regulated service makes inaccessible content that incites violence or violent extremism or terrorism, the operator must preserve that content and all the computer data related to it for the period of one year (in other words, eventually to make it accessible to law enforcement).

Review of the Act is to take place no later than the fifth anniversary of the day on which the section comes into force and every five years after that. The Minister must cause a review of this Act and its operation to be undertaken, and a report on the review to be laid before each House of Parliament within one year after the review is completed.

Re Criminal Code changes

A new hate crime has been added to the Criminal Code. "Everyone who commits an offence under this Act or any other Act of Parliament if the Commission of the offence is motivated by hatred based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation or gender identity or expression, is guilty of an indictable offence and liable to imprisonment for life. In other words, if you can tag on the hate motive to the offence committed under any Act of Parliament, an act which would normally be a minor offense with a one -or two-year sentence or even a fine could lead to imprisonment for life. This has been soundly denounced and may not pass the Charter test.

Modifications to the Criminal Code increase the sentences for existing offences and include: advocating genocide, which was an offence liable to imprisonment for a term of not more than five years but now it would be life; public incitement of hatred, which was liable to a term of not exceeding two years, but would now be five years (same with the promotion of hatred and the promotion of anti-Semitism, which would go from not exceeding two years to possibly up to five years).

There's a new motive to impose sureties to keep the peace. They include the fear of hate propaganda offence or hate crime. A person may, with the Attorney General's consent and information before a provincial court judge, if the provincial court judge before whom the parties appear is satisfied by the evidence adduced that the informant has reasonable grounds for the fear, the judge may order that the defendant enter into a recognizance to keep the peace, and the conditions can be quite harsh. In fact, they're similar to what is being imposed on people on security certificates: to wear an electronic monitoring device, return and remain at their place of residence at specified times, abstain from the consumption of drugs or alcohol or any other intoxicating substance; provide for the purpose of analysis a sample of bodily substance prescribed by regulation; abstain from communicating, directly or indirectly, with any person identified in a recognizance, or refrain from going to any place specified in the recognizance.

There is also a modification in the Canadian Human Rights Act. The Act is amended by adding it is discriminatory practice to communicate or cause to be communicated hate speech by means of the internet or any other means of telecommunication in a context in which the hate speech is likely to foment detestation or vilification of an individual or group of individuals on the basis of a prohibited ground of discrimination. If the complaint is substantiated, the person found to be engaging or to have engaged in the discriminatory practice may be ordered to pay compensation of not more than $20,000 to any victim identified in the communication or ordered to pay a penalty of not more than $50,000 to the Receiver General. This reintroduces something which was in the Canadian Human Rights Act and was invalidated by the Supreme Court because the definition of hate in the Human Rights Act was too broad. But the hate speech as now defined is more in line with what the Supreme Court has defined as hate speech. But it's been widely criticized because it would potentially swamp the Human Rights Commission with a whole lot of complaints. The most important thing from our point of view is that it's very easy to lay a complaint at the Human Rights Commission against someone. That means that it would be a chill factor, because if you're fired, if you're found guilty, then you could be potentially fined up to $70,000.

Question: Inspectors can do search and seizure without warrant anywhere but a private residence. Does an office like where we are meeting require a warrant? I'm picturing a circumstance where, say, Kate sends a message out on a regulated service, like their Facebook page calling on their members to go out and strike or protest somewhere in a way that the government could deem blocks an essential service in some way. Could the inspector then come along and seize all the computers and drag them off?

Answer: My understanding is no, because the Act and the regulations are with respect to service providers of a regulated service. The inspectors act in the name of the Commission to see if the Act is respected and the persons who are targeted by the object of this Act are the service providers. I didn't think that it would be the users of the services that could be targeted by the inspectors.

A lot of these service providers aren't even in the country, so that's one of the questions about how the Canadian version of this will be enforced.

Tim McSorley summarizes main concerns from ICLMG perspective:

1. Of four parts to the bill, only two address online harms regulations.

2. “Content that incites violent extremism or terrorism” is overly broad, vague and redundant.
3. Platforms would be required to preserve data relating to content alleged to incite violence or incite violent extremism or terrorism for one year.
4. While not explicitly requiring platforms to proactively monitor content, does not disallow it.
5. Vagueness in definition of regulated service could impact messaging apps.
6. Could allow for malicious accusations of posting “terrorist content,” with little recourse.
7. The proposed Data Safety Commission is granted incredibly broad powers with minimal oversight.
8. New hate offences raise *Charter* concerns and could aggravate terrorism investigations and sentencing.

Combined, these could have serious impacts on fundamental rights, target dissent and disproportionately impact marginalized or racialized communities

Regarding content alleged to incite violence or incite violent extremism or terrorism:
This can be overly broad, vague and can lead to political discretion; “terrorism” and “extremism” are subjective terms and continue to be used to target marginalized and racialized communities; and inclusion of a “motivation” for incitement to violence will influence interpretation of what is considered “terrorist” or “extremist”. For example, somebody posts on social media that people should join encampments, and the fact that “from the river to the sea” has been viewed as being an incitement and support for terrorism, which it clearly isn't, could be interpreted even though there's no call for an act of violence. If it was to take to the streets and do everything we can to defend women's rights and or defend gender diverse people's rights versus defending Palestinian rights, a service provider could interpret whether or not one incites violence and one is more acceptable.

There are still problems with the idea of incitement to violence because it's simply redundant. If they want to monitor content that incites violence, just monitor content that incites violence. There's no need to include a motivating factor. That would reduce the potential for bias around what is considered violent or a call to terrorism. In our meeting with Dept. of Justice, they acknowledged that issue, but said that because terrorism is in the Criminal Code, they have to include it. There's lots of things in the Criminal Code that aren't included as online harms, so why this has to be there is a question.

In terms of incitement to violence, they lack any protections for freedom of expression, association, etc. For example, the interference with essential service or serious risk to health and safety of the public. Those are the seeds from both the terrorism and the incitement to violence provisions. They're almost identical. We could look at something that builds on what's in the Anti-Terrorism Act, but that goes a little bit further because there's been concerns that this could capture journalistic work and academic work, especially because it's online. There are concerns about what would be considered computer data related to a post. Is it just the wording of the post, or could it also include IP addresses, usernames, account information, email addresses, phone numbers associated with that account? That ties into what we were talking about before with CSIS getting new production orders. It is supposed to exclude private messaging services, but the way it's defined is that it has to be a private messaging service that does not enable a user to communicate content to a potentially unlimited number of users not determined by the user, but for those who use WhatsApp or Telegram, you can create public channels. There's WhatsApp communities where you can create a link, and anybody can join. It's essentially public, but it's on WhatsApp, which is a private messaging service.

I've asked Dept. of Justice to get back to us about whether or not this could be included because it has the additional issue of WhatsApp being end-to-end encrypted even in these communities. If they're mandating that Meta would have to monitor WhatsApp or WhatsApp communities, then they would have to be monitoring encrypted content, and that would mean creating backdoors or undermining encryption. Alternatively, since it's a public group, even though the messages are encrypted, they could join the group, but then they would need

somebody to join every single group on the platform to be able to monitor it. So there's some concerns around what that definition of private messaging system captures, and whether or not it could actually still be used to target encrypted messaging services

Malicious accusations: individuals are allowed to make a submission with concerns about whether or not a platform is respecting harmful content regulations, but there's no way to challenge those submissions. So, it's not a complaint per se, but it's a mission. The concern would be if there is a campaign to the Commission accusing platforms of not doing enough to take down content about encampments because that's allegedly inciting terrorism, that could be done. And there's no clear way in the legislation to actually challenge the impact of those submissions. In some ways it's good because complaints are more specific about the victimization of children and non-consensual sharing of intimate images. But there's still this question about how the submission system could work and what its impact could be.

There's been petitioning to remove the parts on the Criminal Code and the Human Rights Commission from the rest of the bill. ICLMG joined on that open letter and there's a network of groups facilitated by the center for Free Expression.

Because the government wants to prioritize the foreign interference bill, we're more likely to see this get to committee in the fall. It's still not clear if it'll go to justice or heritage committee. Budget 2024 did provide funding for the Digital Safety Commission, so it appears they are hoping for a quick rollout for this.

They Conservatives were against previous the previous proposal. They are adamantly against the changes to the Canadian Human Rights Act. There's definitely been conservatives on the industry committee with concerns around surveillance and privacy protection. Their main critic on industry has been fairly open to meeting with us and discussing issues around artificial intelligence We proposed amendments to C 27 to remove provisions for broad exceptions to the need for consent to collect information under national security. There are exceptions in the bill to allow private entities to collect information without consent, if it's on national security grounds, and we proposed amendments to either strike it or to restrict it further. His office has said they're open to moving those amendments which is a surprise since Conservatives aren't usually open to restricting national security provisions.

The Heritage Committee, at least on the liberal side, is better than justice.

CLOSING

Overwhelmed by number of issues raised. It feels almost as bad when we started 24 years ago with the ATA, except now it feels like there is a more malicious framing. Back then it was a crisis reaction and they are staggering forward. This seems too coherent and invasive. In many ways the public is less aware of it now than they were at our first meeting in 2002 two weeks after the ATA. In going through this legislation, you can see how it almost was perfectly constructed for the current Israel Palestine conflict. I would hate to be an academic right now. People must be looking over their shoulder. The atomization of the academy is criminal.

Assembly adjourned