Submission for the 2023 Universal Periodic Review of Canada by the International Civil Liberties Monitoring Group

ANNEX I

This annex contains issues that were included in previous UPR submissions but have yet to be fixed, additional details on issues that are mentioned in this UPR submission, and developments that are not yet final or enshrined in law but that we must keep an eye on.

A. The O'Connor/Arar Commission

1. Maher Arar is a Canadian citizen who was a victim of extraordinary rendition. On September 26, 2002, while passing through JFK Airport in New York, Mr. Arar was arrested, detained by U.S. officials for twelve days and then removed against his will to Syria where he was imprisoned and tortured for nearly a year. He was released without any charge and returned to Canada on October 5th, 2003. On February 8th, 2004, in response to public pressure, the Canadian government appointed Justice Dennis O'Connor to conduct a public inquiry to investigate and report on the actions of Canadian officials in relation to Mr. Arar's experience and to make recommendations concerning an independent review mechanism for national security activities.

2. Justice O'Connor carried out his inquiry from February 8th, 2004 and tabled his first report in September 2006. He found that the Canadian police (RCMP), without any justification, had labelled Mr. Arar as an "Islamist extremist linked to Al Qaida", and then shared this inaccurate information with U.S. law enforcement agencies. Judge O'Connor concluded that it was likely that in arresting Mr. Arar in New York and sending him to Syria, the U.S. authorities relied on the false information provided to them by the RCMP.

3. On December 12th, 2006, Judge O'Connor released his second report, making strong recommendations to establish a comprehensive review and oversight mechanism for security and intelligence operations in Canada. While there were several review bodies already existing in Canada, they were narrowly focused, diverse in their mandates and powers, ineffective against joint force operations and unable to protect Mr. Arar from the abuse which he endured. Judge O'Connor's recommendations would provide greater assurance that security and intelligence activities respected the rule of law, due process and human rights standards. We were happy that the *National Security Act, 2017* – adopted in 2019 – created the National Security and Intelligence Review Agency (NSIRA), an overarching review mechanism like the one suggested by Justice O'Connor. To date, NSIRA has produced strong reports and has met its mandate. However, there are still some areas of concern, including that the Agency is unable to issue binding orders; complainants are limited in what they can share publicly even about their own submissions to the Agency; and information can be heard in secret, apart from the complainant. NSIRA has also reported issues with security agencies withholding access to information or delaying the provision of information.

B. The Iacobucci Commission

4. During his inquiry, Judge O'Connor came across three other cases similar to that of Maher Arar. Three Arab-Canadians (A. Almalki, A. Abou-Elmaati and M. Nureddin) were all arrested in Syria, detained and tortured in the same prison as Mr. Arar and were subject to the same questioning and abuse. They were finally released without charge and returned to Canada. Since Judge O'Connor did not have a mandate to investigate these three cases, he recommended a new, separate inquiry to carry out this task. As a result, on December 11th, 2006, the Canadian government appointed former Supreme Court Justice Frank Iacobucci as a Commissioner to determine whether any Canadian officials were directly or indirectly responsible for the abuse suffered by these three Canadians. The Commission found that the actions of Canadian government officials respecting these three men were deficient and indirectly led to their detention and mistreatment. In March 2017, the Canadian government finally settled the lawsuit launched by the three men, officially apologized and compensated the torture survivors.

C. The *Anti-terrorism Act* of 2001 (C-36)

5. The *Anti-terrorism Act* (ATA) was adopted by the Canadian Parliament in late 2001. It contained provisions dealing with preventative detention, arbitrary arrest, investigative hearings, listing of alleged terrorist groups, delisting of charitable organizations, suspension of the right to remain silent and the principle of innocence until proven guilty. Many of these provisions are in contravention of the ICCPR, in particular art. 9, 14, 17 and 18. While art. 4 of the ICCPR allows for derogation of these articles in times of emergency ("…to the extent strictly required by the exigencies of the situation…"), the ICLMG argues that the measures go beyond what is strictly required and the Canadian government should be questioned about them. These provisions in the ATA are also in contravention of sections 7, 8, 9, 10 and 11 of the *Canadian Charter of Rights and Freedoms* and are not legitimized by section 1 of said Charter.

6. Two provisions of the ATA – preventative detention and investigative hearings – became inoperative in 2006 due to a five-year sunset clause. After a failed attempt to reintroduce the measures in 2007, the government was finally successful in 2013 with the adoption of Bill S-7. Investigative hearings were finally repealed in 2019 with the adoption of Bill C-59, the *National Security Act, 2017*. Preventative detention is however still law, and not only contravenes the *Canadian Charter of Rights and Freedoms* and the ICCPR but also opens the door to cruel and inhuman treatment and other treaty violations.

D. The *Protection of Canada from Terrorists Act* (C-44)

7. The *Protection of Canada from Terrorists Act*, approved by Parliament in April 2015 provided for greater powers and resources for the Canadian Security Intelligence Service (CSIS), permitted it to operate internationally, and expanded its power to share information as well as a blanket protection of its informants' identity in court. This law should be read in conjunction with the *Anti-terrorism Act 2015* which followed it and expands the role of CSIS still further.

E. The *Anti-terrorism Act, 2015* (C-51)

8. The *Anti-terrorism Act, 2015* (ATA 2015) was adopted in June 2015. The legislation provided for a massive increase in CSIS threat disruption powers similar to those granted to police — this despite CSIS being created as a way to separate intelligence and policing activities, after a federal inquiry (the McDonald Commission) found that the the combination of the two under the Royal Canadian Mounted Police (RCMP) had led to human rights abuses. In particular, the ATA 2015 increased the ability of CSIS to engage in secret counter-terrorism actions in Canada, as well as in foreign countries.

9. It also introduced far-reaching and ambiguous changes to the *Anti-terrorism Act* of 2001 that potentially criminalized lawful activity. ICLMG argues that these provisions are contrary to articles 14, 17, 18, 19 of the ICCPR, and go beyond what is permitted under art. 4. Serious concerns have been raised about the impact of these measures on dissent in Canada, in particular dissent by indigenous and environmental activists who could be labelled as terrorists under the act.

10. With respect to security certificates, the bill made a bad situation worse by allowing the minister to request the court to withhold information from the special advocates who were meant to assist the detainees in secret trials. This appears to be in complete violation of the Supreme Court decision in the Adil Charkaoui case.

11. Further, the bill expands the list of those who may be put on the “no-fly list“ in contravention of articles 9, 12, 14, and 17 of the ICCPR. The ATA 2015 codifies a system for establishing a Canadian no-fly list without providing a clear mechanism for how a person on the list becomes aware of their status, and severely limits their ability to challenge the listing. The law allows for a judicial hearing that may occur outside of public view and allows for the use of secret evidence. It also boosts the wider sharing of intelligence information, which is contrary to recommendations in the O’Connor report (more details in section L below), and which puts at risk, and could seriously harm many innocent individuals [art. 2, 9, 14, and 17 ICCPR].

12. ICLMG supports measures to combat terrorism, but such measures already exist in our criminal law. While we challenge the constitutional legality of provisions in the *Anti-terrorism Act, 2015*, we also question their effectiveness. They will certainly open the door to the criminalization of now lawful activities and the suppression of dissent, but according to many experts they do very little to combat terrorism and protect the public.

F. The “No-Fly List”

13. Passenger Protect, Canada’s “no-fly list” program, was introduced by the government in June 2007 under the authority of an obscure provision in the *Public Safety Act* (2004) granting discretionary powers to the Minister of Transport. The program allows the government to place the names of persons on a list of specified individuals prevented from boarding flights, without any judicial process or authorization and without notice to the listed person. The individual learns of the listing upon arriving at the airport but is not given the reasons for the listing. The information providing the basis for the listing is furnished by the police and intelligence authorities. The individual in question can apply to have his/her name removed

from the list but has no access to the information forming the basis of the listing. It is unknown how many individuals are on the list, which is kept secret.

14. Likewise, it is unknown how many individuals have been barred from boarding a flight since the program's inception. However, reports have shown that more than 100 individuals – including dozens of children – have been the subject of false positives because of similarities in name, age or other features, which have caused them to be intercepted and delayed at airports each time they travel. Based on reports of impacted individuals, many listings appear to have been influenced by racial and religious profiling.

15. The 2019 adoption of the *National Security Act* implemented changes to establish a redress system for "false positive" flyers, where they are able to obtain a unique identifier known as a Canada Travel Number (CTN). However, the system remains new and has not been adequately reviewed in order to ascertain its impact or effectiveness. Further, while it addresses the issue of individuals with similar names as those on the no-fly list, it does not remedy the rights violations of the no-fly list itself.

16. These issues are exacerbated by an agreement between the Canadian and U.S. governments reported in our 2009 UPR submission, which subjected travelers in and out of Canada, including Canadians, to the U.S. Secure Flight List. All flights in or out of Canada which pass through U.S. airspace, even if the planes do not touch U.S. soil, must share their passenger manifests with the US Department of Homeland Security to be screened against the US Secure Flight List. This was further cemented in a 2011 amendment to Canada's privacy laws explicitly allowing airlines to share this information with US authorities. Based on this screening, passengers, including Canadian citizens, may be denied boarding. Because an approximate 85% of flights out of Canada pass over US airspace, the impact is to strictly limit the ability of listed individuals from leaving or returning to Canada. In recent years, this has been exacerbated by an apparent expansion of flights subject to these rules to those which do not over-fly U.S. airspace but would need to land in U.S. airspace should there be an emergency. Notably, foreign nationals are not able to challenge their listing on the U.S. Secure Flight List. Finally, while the bill to enact the 2011 amendments to Canada's Privacy Act contained a provision for a study of the impacts of these changes within 5 years, no such review ever took place.

17. The ICLMG argues that this "No-Fly Program" contravenes the ICCPR, and in particular, art. 2, 9, 12, 14 , 17, 18 and 19. These contraventions go beyond what is strictly required for an emergency under Art. 4. There has been a serious loss of freedom without any trial, due process or transparency.

G. The *National security Act, 2017* (C-59) – CSIS and immunity for offences

18. In September 2022, it was revealed that Mohammed al-Rashed, the human trafficker who helped Shamima Begum, a 15-year-old British girl, and two other British girls aged 15 and 16, enter into Daesh (ISIS) controlled territory in Syria in 2015, was a CSIS asset recruited to continue his illegal activities in exchange for citizenship. While Prime Minister Trudeau pledged to "look into" this issue further, he also defended the "creativity of intelligence services." One of the central issues was that CSIS had been working with sources who

engaged in illegal activity, and CSIS happened to withhold that important bit of information from the courts, including its work with al-Rashed.

19. At the time in 2015, CSIS did not have clear legal authority to recruit and provide resources to someone engaged in supporting terrorism. That changed, though, with the passage of Bill C-59 in 2019, which brought in rules that allow for CSIS agents and their sources to engage in certain designated unlawful activities. We opposed that change at the time, because it raised deep concerns around what unlawful activities CSIS could be supporting, and do not believe that the safeguards the government put in place go far enough to make up for the potential harm these powers can cause. Regardless of it now being made legal, CSIS still lied to the courts at the time to cover up working with a human smuggler who helped secure passage for dozens of people, including minors, into Daesh territory. Some will argue that CSIS will need to work with the "bad guys" at times in order to collect information, and that doing so in secret is the only way to protect human sources. This can at times be true, but does that mean that anything goes and that no limits or boundaries should be placed? If, when Bill C-59 was being studied, Members of Parliament had been told that the new law could allow CSIS to promise citizenship in exchange for information to a human smuggler trafficking minors, they may have reacted differently.

H. The *National security Act, 2017* (C-59) – CSIS & threat reduction powers

20. In February 2023, the National Security and Intelligence Review Agency (NSIRA) released a report on the Canadian Security Intelligence Service's threat reduction activities which showed, once again, that the spy agency cannot be trusted to follow the law or the Charter of Rights and Freedoms when they are granted secret powers to disrupt the lives of Canadians.

21. It was found that CSIS believes it can ask third parties, like private companies, to take action against individuals based on a secret risk assessment without taking responsibility for the possible impacts. CSIS also disagrees with NSIRA's recommendation that it take the actions of these third parties into account when deciding to seek out a warrant. This shows that the service continues to skirt the law and should no longer be trusted with these powers.

22. We had been told over and over that we should not be concerned with CSIS' threat reduction powers because they have not reached the point of being so invasive that they require a warrant (something the law allows CSIS to determine by itself). It is now clear that CSIS is farming out threat reduction measures to third parties, and using that as a reason to avoid considering whether they need a warrant in the first place. We also know that CSIS is employing threat reduction measures outside of Canada that may violate Charter Rights, but this was beyond the scope of this NSIRA report.

23. Also of concern was the fact that the NSIRA was unable to properly assess the outcome of threat reduction measures carried out by third parties, because CSIS' "reporting system was inadequate or that these reports were improperly filed or non-existent." Finally, the government continues to censor the number of threat reduction measures requested by CSIS and those carried out. This information poses no threat to national security and should not be redacted from NSIRA reports.

24. The ICLMG has opposed CSIS, an intelligence agency, being granted threat reduction powers since they were first introduced in the *Anti-terrorism Act, 2015*. The reforms implemented by the federal government in 2019 (through the *National Security Act, 2017*) did not solve the severe threat to fundamental rights that come about when an agency that operates in nearly complete secrecy can carry out real world, tangible actions against individuals. This was true when the McDonald Commission found in 1981 that there must be a division between intelligence services and law enforcement services, and it remains true today. The ICLMG has thus called the federal government to intervene by suspending CSIS' use of threat reduction measures and referring this issue to the Federal Court. We also reiterate our call that CSIS' threat reduction powers be abolished.

I. The *National security Act, 2017* (C-59) – CSIS & mass surveillance

25. Historically, CSIS has engaged more in what is called HUMINT – human intelligence: going out and collecting information in person on targeted individuals. Over the years, though, it has become much more engaged, like the Communications Security Establishment (CSE), in SIGINT: signals intelligence. Unlike the CSE, they are allowed to collect data inside Canada and about Canadians. However, CSIS is supposed to limit the information that they keep to what is directly related to a particular target or investigation – extraneous information should be destroyed. In 2016, though, a federal court judge found that CSIS, through its Operational Data Analysis Centre (ODAC) program, was illegally spying on Canadians for over a decade. Instead of restricting these activities, the *National Security Act, 2017* has basically enshrining them into law. It has created the concept of "datasets," or categories of information CSIS is allowed to collect – with the Minister of Public Safety's authorization, and the Intelligence Commissioner's approval. On top of all that, the *National Security Act, 2017* allows the collection of data "relevant to the performance of CSIS", which is too broad, it allows the collection of datasets that do not directly relate to activities that are a threat to the security of Canada, and it allows datasets that are publicly available to be "retained, queried and exploited".

J. The *National security Act, 2017* (C-59) – The Communications Security Establishment

26. The Communications Security Establishment (CSE), originally created in 1946 by order-in-council, was given a new legislative mandate and powers in the *Anti-terrorism Act (*ATA) of 2001. It allows the minister of Defence to authorize the CSE to intercept private communications coming into and out of Canada in relation to any activity or class of activities specified in the authorization, for the very broad purpose of obtaining foreign intelligence. While the CSE used to be restricted to spying outside of Canada, the legislation now allows it to spy on domestic communications as long as it involves someone outside Canada. There is no requirement for judicial authorization. The CSE needs only to seek a discretionary authorization from the Defence minister who is given an open-ended range of grounds in making his decision. The language of the legislation mirrors that of the National Security Agency (NSA) in the USA which has allowed spying without warrants on emails, faxes, and phone calls. The CSE provisions in the ATA have opened the door to massive domestic and international spying on ordi-

nary citizens. The ICLMG argues that the powers and operations of the CSE constitute a major violation of articles 2 and 17 of the ICCPR.

27. Recently released heavily redacted documents about the CSE paint a picture of a powerful spy agency in dire need of oversight. Despite rules against targeting Canadians, the CSE regularly collected Canadians' communications, shared Canadians' information with third parties, chose to protect those intelligence sharing relationships over the privacy of Canadians, and prioritized its continued operation over all else.

28. More precisely, the documents revealed how:

- The CSE redefines common words to create its own vocabulary. These non-standard definitions provide a misleading impression of CSE's actions to the public, and potentially to the ministers tasked with authorizing CSE's surveillance powers.
- The CSE had expansive metadata surveillance programs in place, and those programs were expanding: This likely means that the CSE has records of Canadians' use of websites or apps based outside of Canada, including Google, Facebook, Instagram, YouTube, Tiktok, Twitter, and more, along with their calls, emails, or instant messages to people living outside Canada. Even the metadata of domestic telecommunications can be subject to collection, as a large percentage of Canada-to-Canada internet traffic crosses the Canadian border during its travels.
- CSE's cybersecurity mandate gives it the authority to access Canadians' personal information from within other government agencies.
- The CSE developed a system to share bulk metadata collected by the CSE with Five Eyes partners.
- The CSE violated the law for five years by failing to minimize Canadian information shared with Five Eyes partners.
- The CSE asks Five Eyes countries to report monthly on measures meant to protect the privacy of Canadians whose information is shared with them. However, the CSE states that it would not penalize second party countries for failing to comply with those safeguards, because doing so would "have a significant negative effect on [the CSE]."

K. *The National Security Act, 2017 - Avoiding Complicity in Mistreatment by Foreign Entities Act*

29. In 2011, the Public Safety Minister sent ministerial directives to the Canadian Security Intelligence Service (CSIS), giving them the authority to use and share information that was likely extracted through torture in "exceptional circumstances". One year later, he sent similar memos to the RCMP and Canadian Border Services Agency (CBSA). It is worth noting that if it wasn't for a request of access to information, we would not have known about the directives, commonly known as the "torture memos". The directives apply to the use of this information for investigative purposes and to information-sharing with foreign government agencies, armies and international organizations. The instructions were criticized by human

rights advocates and opposition Members of Parliament as a violation of Canada's obligations under the *Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment.*

30. In 2017, without prior notice or consultation, the Canadian government unveiled new directives: *Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities.* Although the new directives clearly mention a strong rejection of torture, they still allow for the sharing, requesting and use of information that could lead or could have been obtained through torture, among other problems of scope, transparency, retention of information and oversight.

31. These directives are even more troublesome in light of the Canada/U.S. *Joint Statement of Privacy Principles* under the North American Security Perimeter. The "principles" released in 2013 permit the sharing of personal information gathered at the border with third countries – in some cases, without informing the other government until after the fact.

32. The ICLMG among other groups have denounced the above directives leading the government to modify it in the *Avoiding Complicity in Mistreatment by Foreign Entities Act,* part of the *National Security Act, 2017*. While an improvement on previous ministerial directions, these new regulations still allow, under certain circumstances, for Canadian agencies to use information obtained through mistreatment or torture; a completely unacceptable stance. There is also nothing in the Act that would prevent this or any future government from weakening ministerial directions, as we have seen in the past. The protection of rights must be enshrined, and not left to the whims of the government of the day or to be guarded by public pressure.

33. ICLMG submits that not only are such policies in violation of the CAT Art. 2.2 but they also promote a market for information obtained from torture. In 2006, Justice Dennis O'Connor, reporting for the federal Arar Commission, recommended policies "aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuing accountability." The act falls short on this absolute principle.

L. Security Certificates

34. Security Certificates (or Certificates of Inadmissibility) are provided for in the *Canadian Immigration and Refugee Protection Act* (IRPA). The Act allows the Minister of Immigration and the Minister of Public Safety to issue such a Certificate leading to the detention and deportation of a permanent resident or a foreign national deemed to be inadmissible on security or certain criminality grounds. The definition of security inadmissibility is extremely broad, including people who are not alleged to represent any security danger (for example, who are merely members of an organization that is believed to have committed terrorist acts). The information used to issue such a Certificate is provided by the police or the intelligence services. The Certificate is subject to review by a judge to determine if it is reasonable (a very low level of proof) and the review is based on intelligence, not on evidence as generally required in a trial. The judge may hear evidence in secret (which is often the case) that is not disclosed to the person concerned or their lawyer, and use that evidence in deciding whether the Certificate is reasonable. Security Certificates cannot be used against Canadian citizens.

35. On February 23rd, 2007, the Supreme Court of Canada ruled that this non-disclosure of evidence contravened the Canadian *Charter of Rights and Freedoms* and decreed that a fair hearing leading to detention must include the right to know the case put against one, and the right to answer that case (*Charkaoui vs Canada*). At the time of the ruling, five Muslim men had been in detention or under house arrest with control measures, without charge or a fair trial for a combined twenty-six years.

36. In February 2008, the Canadian Parliament passed a law to offset the 2007 Supreme Court ruling and to resurrect the Security Certificate process. The key difference between the new law and the one ruled unconstitutional is the provision of Special Advocates to protect the interests of the persons named in the Certificates at the review process. However, these Special Advocates do not have the right to discuss the so-called evidence with the persons subject to the Certificate. In these circumstances, the ICLMG argues that these Security Certificates still contravene both the *Canadian Charter of Rights and Freedoms* as well as the ICCPR (Art. 2, 9, 13 and 14). The person affected is still held in detention without trial, does not have the right to know the case against him, nor the right to answer that case. The security certificate regime has been amended by the *Anti-terrorism Act of 2015* to reduce the access of Special Advocates to the evidence, and the contraventions of the ICCPR have become more serious.

37. Additionally serious is information contained in a letter sent in 2008 by the Director of the Canadian Security and Intelligence Service (CSIS) to the Minister of Public Safety. The letter warned that if certain opposition amendments were made to the *Immigration and Refugee Protection Act*, it could become impossible to use Security Certificates to arrest suspected terrorists since it would prohibit the use of information from regimes known to use torture, thus indicating that such cases might not stand up without information obtained under duress. This information vindicated the suspicions of the five men who had been detained in Canada for long periods under Security Certificates, i.e., Messers. Charkaoui, Harkat, Almrei, Jaballah and Mahjoub. In 2009, the courts quashed the security certificates against Messers. Charkaoui and Almrei and, in 2016, found the certificate against Mr. Jaballah unreasonable. Because Mr. Mahjoub faces a risk of torture if returned to Egypt, he has remained in Canada, essentially in a state of limbo. He was released from detention in 2009 under strict conditions, eased substantially since then, but upheld in July 2017. In 2020, he filed a lawsuit against the federal government for information he says he needs to mount a full argument against deportation to his native Egypt and possible torture. Although the conditions of his detention have been significantly relaxed as well, deportation procedures have started in 2015 against Mr. Harkat, an Algerian refugee. He lives in constant fear of being deported as he risks potential detention and torture if sent back to Algeria.

M. Extradition and due process – The Hassan Diab Case

38. The Canadian citizen Hassan Diab was extradited to France on incredibly flimsy evidence that even the extradition judge in Canada expressed concern over. Under Canada's extradition law, there is first a hearing before a judge and then a reference to the Minister of Justice who makes the final decision. The hearing does not provide the recognized protections for a fair trial – there is a lack of due process, no procedure to test unreliable evidence – including

secret evidence and evidence obtained through torture (violating art. 15 of the Convention against Torture) – nor is there protection against unjust extradition requests that are politically motivated. The burden to prove the evidence is "manifestably unreliable" is on the person sought, however they are not allowed to present exculpatory evidence. Further, neither the requesting state nor the Canadian government are obligated to reveal exculpatory evidence in their possession, in violation of domestic and international standards for a fair trial.

N. The Canadian Security and Intelligence Service and duty of candour

39. Over the years, the CSIS has been found multiple times to have engaged in unlawful activities, and then misled the courts about it. In July 2016, a Federal Court decision was made public in which it was found that CSIS had also misled the courts regarding illegal actions carried out as part of their intelligence gathering activities. In August 2020, another federal court decision revealed yet another case of CSIS engaging in potentially illegal activities to gather intelligence in support of a surveillance warrant. The decision also revealed that in applying for the warrant, CSIS not only withheld exculpatory information regarding the warrant's target, and violated its duty of candour – to make full and frank representations to the courts when applying for a warrant in an *ex parte* (secret) hearing. A 2020 review found that CSIS officers saw the warrant process not as a means to protect fundamental rights or the integrity of the justice system, but a "necessary evil." In 2022, the National Security and Intelligence Review Agency (NSIRA) released a report on the issue, making multiple recommendations and finding that, "quick reforms, followed by neglect," policies that are "vague, dated, overlapping and contradictory" and a "a system of diluted accountability," has meant that the "warrant process has repeatedly failed to meet these candour obligations" causing them to "struggle... to... meet their legal obligations" to the court.

40. However, there have been no repercussions for these breaches and despite promises to implement policy changes, it is unclear whether they have been appropriately implemented or what impact they have had; as far as we understand, there has yet to be changes to the internal culture at CSIS that has undermined the warrant process.

O. Facial Recognition Technology & Artificial intelligence

41. Facial recognition surveillance is invasive and inaccurate. This unregulated technology poses a threat to the fundamental rights of people across Canada. Federal intelligence agencies refuse to disclose whether they use facial recognition technology. The RCMP has admitted (after first lying about it) to using facial recognition for 18 years without regulation, let alone a public debate regarding whether it should have been allowed in the first place.

42. In 2021, the Office of the Privacy Commissioner of Canada (OPC) found that the RCMP's use of facial recognition technology – specifically the Clearview AI system – broke the law. The OPC report concluded that the RCMP is responsible for ensuring that the technology it uses does not violate the laws governing the privacy rights of people in Canada. Disturbingly, the RCMP contests that decision, believing that it has no responsibility to verify that third party contractors it works with are not breaking the law.

43. In 2022, a parliamentary committee published a report on facial recognition technology (FRT) and artificial intelligence (AI) that demonstrated the urgent need for the federal

government to regulate the use of facial recognition technology in Canada. The committee recommended a moratorium on the use of this technology until appropriate restrictions and rules are put in place. It also recommended that the government must establish no-go zones, particularly for the use of facial recognition for mass surveillance purposes.

44. Finally, the federal government has recently introduced legislation aimed at regulating artificial intelligence: the *Artificial Intelligence and Data Act* (AIDA), part of Bill C-27, the *Digital Charter Implementation Act 2022,* a bill to reform some of Canada's privacy laws. Although such legislation is necessary as the application of AI systems has a highly significant and potentially negative impact in sensitive areas, most notably healthcare, employment, immigration, border security, and education, AIDA offers an inadequate response and would cause more harm than good for multiple reasons: the absence of public consultations has made it hard for civil society groups, researchers and historically marginalized communities to significantly contribute to the legislation; many important pieces of the Act are left to regulation, and will be decided on only after it is passed. This will result in less scrutiny and transparency; the proposed oversight is arbitrary and the enforcement mechanism is fragile; the Act fails to apply to government institutions, including national security agencies, including the RCMP; and the Act does not address the significant human rights implications of algorithmic systems. We have asked that the parties vote against it unless these changes are made.

45. Research has shown that facial recognition surveillance undermines our freedoms of association, assembly, expression and movement, as well as our right to privacy and protection against unreasonable search and seizure. Therefore, Canada must ban the use of facial recognition surveillance by federal law enforcement and intelligence agencies; initiate a meaningful, public consultation on all aspects of facial recognition technology in Canada; and establish clear and open policies and laws regulating the use of facial recognition in Canada, including reforms to our privacy laws.

P. Encryption

46. In July 2017, a ministerial meeting of the security officials of Australia, Canada, New Zealand, the United Kingdom and the United States was held in Ottawa, where possibilities for facilitating increased state access to encrypted data were discussed. The meeting occurred under the auspices of the 'Five Eyes' – a surveillance partnership between intelligence agencies within the five countries, including Canada's Communications Security Establishment (CSE). It generated a joint Communique, which presented encryption as a serious barrier to public safety efforts and an impediment to state agencies wishing to access the content of some communications for investigative reasons. In 2019, former Public Safety Minister Ralph Goodale started calling for companies to inject communications insecurities into their applications. He even cast the security experts and privacy advocates who defend strong encryption as supportive of pedophiles. In September 2021, Canada and the rest of the G7 met in London, where the group reasserted its commitment to undermine encryption.

47. Interfering with the availability of strong encryption will impact our right to security, our right to silence, as well the right to be secure against unreasonable search and seizure. It will also impact our freedom of expression, thought, peaceful assembly and association, as well

as equality rights. ICLMG and others called on the Five Eye governments to respect the right to use and develop strong and uncompromised encryption, as it protects our most sensitive data, our increasingly critical online interactions, even the integrity of our elections. We argue that actions and legislation that would undermine encryption violate Art. 2 and 17 of the *International Covenant on Civil and Political Rights*.

Q. International assistance and anti-terrorism laws

48. On March 9, 2023, the federal government introduced long-awaited amendments to the *Criminal Code* to allow Canadian organizations to carry out their vital international assistance work in Afghanistan and other regions under de facto control of an entity deemed by the government to be a terrorist group. The proposed Bill C-41 would create a new exemption regime allowing Canadian organizations to apply to operate in areas under de facto control of an entity deemed by the government to be a terrorist group where the organization's activities risk providing financial support to the controlling entity. Positively, this new regime would address not only the prohibition of international assistance in Afghanistan, but also other regions facing conflict or politically complex situations where the payment of fees and taxes to a governing entity could place Canadians at risk of criminal prosecution. Importantly, the exemption covers a broad array of activities, including humanitarian aid, education, human rights defense and more. This will allow Canadian organizations to provide not just crisis relief, but to engage with local communities on crucial, ongoing projects to support their well-being and livelihoods. However, the new exemption regime raises important concerns, particularly in regards to a possibly onerous process to apply for an exemption; the creation of new information-sharing protocols between government agencies; and broad criteria that can justify the denial of an application based on undefined "links" to terrorism. Further, organizations whose applications are denied may not be privy to the reasons for or to the information used in the denial of their application.

49. As Médecins sans frontières has stated, despite finally acknowledging that Canadian laws can inadvertently criminalize impartial humanitarian workers, these amendments create new bureaucratic hurdles for organizations to overcome and contradict the fundamental principles of independence and impartiality of humanitarian assistance under international humanitarian law. Upholding these principles is essential to delivering assistance quickly and safeguarding humanitarian workers and organizations who are increasingly targeted by violence during armed conflicts. Canada should instead enact a full humanitarian exemption, as recommended by the Canadian Parliament's Special Committee on Afghanistan and enacted by other states, to ensure that humanitarian assistance to people affected by conflict is not held back by any laws intended to criminalize terrorism-related offences.

50. The ICLMG is also concerned that an exemption regime does not address the central problem at the heart of this issue: that Canada's overly-broad counter-terrorism laws allowed for this situation to occur in the first place. The ICLMG, among others, has long raised concerns that the inherent vagueness and political nature of "terrorism" will continue to have unintended consequences, including on Canada's international human rights and humanitarian obligations, evidenced by the current restrictions on the provision of aid, which many legal experts have described as a misinterpretation of the law in contradiction with international standards regarding the provision of international assistance. While an

exemption regime may provide a route forward, it avoids how counter-terrorism laws create areas and entities that are considered ‘no-go,’ and continue to primarily, and unjustly, impact majority-Muslim countries and regions. We renew our call for the government to fundamentally revisit its approach on counter-terrorism laws and their enforcement.

R. Omar Khadr

51. Omar Khadr is a Canadian citizen who at the age of 15 was detained by the United States at Guantanamo Bay for ten years, during which he pleaded guilty to war crimes. He later appealed his conviction, claiming that he falsely pleaded guilty so that he could return to Canada where he remained in custody for three additional years. In 2010, the Supreme Court of Canada ruled that the Canadian government's interrogation of Khadr at Guantanamo Bay "offend[ed] the most basic Canadian standards [of] the treatment of detained youth suspects." In 2012, Khadr returned to Canada to serve the remainder of his sentence in Canadian custody. Khadr was released on bail in May 2015 after the Alberta Court of Appeal refused to block his release as had been requested by the Canadian government. In 2017, the Canadian government announced a $10.5 million settlement with Khadr and a public apology to compensate for damages arising from its previous handling of the case.

52. Despite this, the government and political officials have continued to share misleading and prejudicial information about the violation of Khadr’s rights. For example, the government’s statement of regret regarding Khadr referred to his torture, ill-treatment and illegal detention as an “ordeal abroad” and expressed regret about “any role Canadian officials may have played” in “any resulting harm” (emphasis added). Another statement attributed the settlement as a measure to prevent costs of litigation. These statements are not true apologies and fail to meet the Convention against Torture requirements of redress.

53. The Canadian government continues to neglect its obligations to investigate and bring to justice those complicit in the torture and illegal sentencing of Omar Khadr, to truly and fully apologize, and to ensure such an incident does not happen again.

S. Abousfian Abdelrazik

54. Mr. Abdelrazik was arrested while visiting Sudan in 2003, at the request of Canadian intelligence agents. Allegedly tortured while in detention, he was never charged and was released from prison in 2005. He was finally cleared of all links to terrorism by the RCMP and CSIS in 2007 and returned to Canada in 2009, but he remained on the U.N. 1267 blacklist until 2011. Internal documents released under freedom of access requests indicate how hostile the foreign affairs bureaucracy was to helping return a Canadian. While the Federal Court found that the Canadian government violated Abdelrazik's rights in refusing to return him home (and ordered the government to comply with a repatriation order), there was no consequence for the foreign affairs bureaucracy.

55. In his legal action against the Canadian government (Abdelrazik vs. Canada, 2009, FC 580), the court found that CSIS was complicit in his initial detention in Sudan and that torture was a viable cause of action. The Canadian government moved to strike the claim on the grounds that there is no enforceable right to protection from torture but the court disagreed. Although the federal governement wanted to reach a settlement in Mr. Abdelrazik’s suit, it

backed out of mediation on the day before it was scheduled to begin, in April 2018. Again, on the eve of the opening of the long-anticipated 8-week trial for Abousfian Abdelrazik's civil case in September 2018, the federal government asked the case be adjourned so that, under Section 38 of the Canada Evidence Act, documents which the government itself had already released be reviewed for national security concerns. Notably Federal Court Justice St. Louis agreed to grant the adjournment "reluctantly" and ordered the government to immediately pay the costs of Mr. Abdelrazik's legal team in preparing for trial, costs that she concluded have been "thrown away as a result of the adjournment". To this day, the case is still adjourned and Mr Abdelrazik continues to be denied justice.

56. We believe these last-minute indefinite delays are cynical and shameful, and were likely pursued for partisan concerns, as the recent settlements and compensations for Canada's complicity in detention and torture abroad were met with outrage from a portion of the Canadian population and media. This action skirts Canada's fundamental obligation under international law to provide an effective remedy when its officials are complicit in serious human rights violations. We repeat our demand that the Canadian government halt these contemptuous delay tactics and move instead to promptly ensure Mr. Abdelrazik receives appropriate and fair redress.

T. Mohamedou Ould Slahi

57. Former Guantanamo Bay detainee Mohamedou Ould Slahi, a Mauritanian who lived in Montreal for two months, launched a $35-million lawsuit in April 2022 alleging that faulty intelligence provided by Canadian authorities contributed to his detention at the U.S. offshore military prison, where he said he suffered fierce beatings, sleep deprivation and sexual assault. A statement of claim from Slahi, whose story became a best-selling memoir and Hollywood film, states that surveillance by Canada's spy agency and police force was fed to his American interrogators. Eventually their "torture broke him down" and prompted a false confession about a plan to blow up the CN Tower, which he had never heard of, the court filings state. The federal government acknowledges in a new court filing that the Canadian Security Intelligence Service and the RCMP interviewed a Mauritanian man at a Guantanamo Bay prison in 2003.

58. Slahi, a Mauritanian citizen with permanent resident status in Canada, lived in Montreal in late 1999 and early 2000 upon moving from Germany. He left Canada after the RCMP started questioning him about supposed ties to Ahmed Ressam, the so-called millennium bomber who planned to attack the Los Angeles airport. Slahi denies ever meeting Ressam. Slahi's amended statement of claim, filed in January of this year, says surveillance during his brief period in Montreal pushed him to return to West Africa, setting off a lengthy pattern of arrests, interrogations and imprisonment. The statement says he was arrested on arrival in Senegal and interrogated by American officials about the same allegations Canadian authorities had pursued. Slahi contends that Canadian authorities induced him to leave the country so he could be arrested and interrogated in countries where the rule of law and international human rights are not respected.

59. He also alleges Canadian authorities contributed to his detention and torture by sharing "false and exaggerated intelligence" about him without appropriate safeguards. "For example, his interrogators pressed him about a phone call in Montreal in which Slahi invited someone

for tea and asked him to bring sugar," the claim says. "His interrogators insisted the request for 'sugar' was code for 'explosives.' This made no sense to Slahi and was entirely untrue." Slahi argues Canadian authorities had knowledge of his torture and mistreatment leading up to the confession. "In the alternative, they should have known, or showed reckless disregard or wilful blindness to his torture and mistreatment," the statement says. The statement of defence says Canadian authorities did not aggressively monitor Slahi or induce him to leave Canada. However, it acknowledges a Canadian official called Slahi's family at one point to say he should not return to Canada. The government also says while Canada shared information with other governments or foreign agencies, it was not false, faulty or exaggerated. We know this to be false from two commissions of inquiry – O'Connor and Iacobucci – into the cases of Maher Arar, and Abdullah Almalki, Ahmad El Maati and Muayyed Nureddin that have found that Canada has been complicit in their arrest, detention and torture because of erroneous information shared with foreign authorities.

U. Afghan Detainees

60. There are very serious concerns that the Government of Canada knew — or had been warned — that prisoners handed over to Afghan authorities by Canada were tortured or faced the likelihood of abuse. If the government had been aware, and did nothing to stop it, then it could be considered a war crime. Federal Liberals who argued for a public inquiry, while in opposition, into the treatment of prisoners during the Afghan war, have said they will not conduct such an investigation now that they are in power. This decision was penned by Defence Minister Harjit Sajjan, who served three tours in Afghanistan as a member of the Canadian Forces, putting him in a conflict of interest. The Ethics Commissioner found no conflict of interest but based her conclusion only on Sajjan's account of his involvement in Afghanistan, which was different than what he told a military historian. Canada has potentially violated the *Convention against Torture* and the *Geneva Convention — Treatment of Prisoners of War.* This issue is grave enough, and murky enough, that we believe a public inquiry is necessary. There hasn't been any government action on this file since our last UPR submission.

V. Armed drone purchase

61. Canada announced in the fall of 2022 that it would open bidding to weapons manufacturers for up to $5 billion worth of armed military drones. Armed drones threaten people's lives around the world. Rather than making the world safer, they are used in extrajudicial executions, surveillance of targeted populations and other violations of human rights.

62. Armed drones don't stop terrorism. In 2015, American Air Force whistleblowers wrote that Obama-era drone strikes "fueled the feelings of hatred that ignited terrorism and groups like ISIS, while also serving as a fundamental recruitment tool. Armed drones are tools of imperialism, used to implement assassination campaigns across the Middle East and North Africa by the United States, killing and permanently wounding thousands of civilians. Canada has also shown worrying signs of using armed drones on civilians and non-civilians alike. For example, the Canadian government has used the term "Fighting Age Males" in its industry call-out. Historically, this term implies that any male over 16 in an area designated as a strike zone is considered an enemy combatant "unless explicit intelligence posthumously proving them innocent." In practice, this has made it virtually impossible to determine how many

civilians have been killed simply because they were holding a cellphone or gathering in the wrong place at the wrong time.

63. The official industry call-out specifically cites that armed drone capabilities could be used to conduct surveillance, within Canadian borders, of “radical elements” who intend to “hang a banner concerning global warming” – in complete violation of the rights to privacy, and freedom of speech and assembly. Canada has also expressed interest in the surveillance of Indigenous peoples living in the Arctic.

64. Finally, at least one of the companies on the short-list is the research, development and manufacturing arm of the Israeli military, Israel Aerospace Industries. The Israeli military, using IAI products developed explicitly for its use, routinely commits war crimes against the people of Palestine and exports war machines that have been ‘tested’ on Palestinians.

W. Prejudiced Canada Revenue Agency audits

65. In June 2021, the ICLMG released a report detailing how a secretive division within the Canada Revenue Agency (CRA) is targeting Muslim charities in Canada for audits, and even revocation, amounting to an approach that is both prejudiced and lacks substantiation. It revealed that, after 9/11, the CRA, its Charities Directorate and the secretive Review and Analysis Division (RAD) were enlisted to monitor the work of Muslim charities in Canada under the unsupported premise that they pose the greatest terror financing risk. The Canadian government’s National Risk Assessment (NRA) for terrorism financing in the charitable sector focuses almost exclusively on Muslim charities, and entirely on charities based in racialized communities, with little to no public substantiation of the risk. This risk assessment is used to justify surveillance, monitoring and audits of leading Muslim charities on questionable grounds. RAD operates largely in secret, in tandem with national security agencies, with little to no accountability and no independent review. As a result, between 2008 and 2015, 75% of all charities who had their charitable status revoked by RAD following these secretive audits were Muslim charities, harming the sector and impacting the larger Muslim community in Canada. The number of audits and revocations before and after that period are unknown because they have never been made public.

66. The government had tasked the Office of the Taxpayers’ Ombudsperson (OTO) with reviewing this situation but the OTO revealed recently that it was refused access to many documents necessary for its review. As a result, the government then tasked – as we initially recommended – the National Security and Intelligence Review Agency with examining the issue as it has the necessary security clearance to gain access to the documents. We have urged for a moratorium to be placed on new audits by the RAD while this – second – review is ongoing, to no avail.

X. Counter-radicalization

67. The government has dedicated millions of dollars to a Office for Counter-Radicalization. They have publicly committed to addressing all forms of violent extremism. However, experts state that the causes of “radicalization” and “extremism” are still little understood. And in other countries, such offices have mostly ended up targeting Muslim and Arab communities. We do need to address violence in society, but shouldn’t the focus be on all forms of violence and its

causes – such as poverty, lack of social services, underfunded education systems, racism, homophobia, sexism — rather than on one path to violence which has lead to the disproportionate profiling and targeting of minorities as well as "radical" dissent, activists and even thoughts. Such irresponsible initiatives undermine art. 2, 17, 18, 19, 21 and 22 of the *ICCPR.*

Y. Protecting Canadians from Online Crime Act (C-13)

68. With the *Protecting Canadians from Online Crime Act*, the federal government aimed to "modernize" the lawful access provisions of the Criminal Code that allow the state to get access to electronic communications in appropriate circumstances. This had little to do with cyberbullying, the bill's supposed target. The lawful access provisions were recycled from past failed attempts at lawful access reform, the main parameters of which were set in the post-Sept. 11 world. They provide a tool kit that has long been sought by the state in relation to investigating terror cases although the case for the necessity of this tool kit is weak.

69. C-13 created new types of production orders that permit police to access "transmission data" as well as "tracking data" on a standard of reasonable suspicion. It also creates new warrants that allow authorities to collect transmission data through a transmission data recorder and tracking data through a tracking device, again on a standard of reasonable suspicion. The authorities need to suspect that 1. an offence has been or will be committed, and 2. the transmission data "will assist" the investigation. These standards of suspicion fall below the usual requirements for a search warrant: reasonable grounds to believe that an offence has been committed and that the search will produce evidence of it. This law violates Art. 17, 19 and 21 of the ICCPR.

Z. The Preclearance Act, 2016 (C-23)

70. The Preclearance Act was adopted in December 2017. ICLMG and other groups have warned that the law grants too much power to US officers operating in Canada, with absolutely no mechanism for accountability unless their actions cause death, bodily harm or damage to property. The *Preclearance Act, 2016*, allows US officers to strip search a traveler, even if a Canadian agent declines to do so; allows US officers to carry firearms; and removes the ability of travelers to withdraw from preclearance areas without further interrogation and without triggering grounds for suspicion. ICLMG is also concerned with Canadian MPs' assertions that they are unable to strengthen protections when traveling to the US because of an agreement signed between the countries' governments. Human rights, and the democratic, legislative process, should trump agreements signed without public parliamentary debate and scrutiny.