Council of Agencies Serving South Asians (CASSA)
5200 Finch Ave. East, Suite 301A, Toronto, ON M1S 4Z5
Phone: (416) 932-1359
Email: cassa@cassa.on.ca Website: www.cassa.on.ca

TO THE UN HUMAN RIGHTS COUNCIL
UNIVERSAL PERIODIC REVIEW OF HUMAN RIGHTS IN CANADA

SUBMISSION

By

COUNCIL OF AGENCIES SERVING SOUTH ASIANS (CASSA)

4th Review Cycle – April 2023

Council of Agencies Serving South Asians (CASSA)
5200 Finch Ave. East, Suite 301A, Toronto, ON M1S 4Z5
Phone: (416) 932-1359
Email: cassa@cassa.on.ca Website: www.cassa.on.ca

Introduction

The Council of Agencies Serving South Asians (CASSA) is pleased to submit to the fourth Universal Periodic Review ("UPR") of its state party, Canada. This submission consists of a collection of concerns that CASSA holds with regard to Canada's shortcomings in combatting hate crimes, hate speech, and online hate in Canada. CASSA is a social justice umbrella organization of over 120 agencies and groups serving South Asian communities in Canada. CASSA's mandate is to facilitate the economic, social, political and cultural empowerment of South Asians by serving as a resource for information, research, mobilization, service delivery coordination and leadership on social justice issues affecting our communities.

Preventing and Combatting Hate Crimes in Canada

1) Form an inter-provincial and-territorial committee to create a national anti-hate strategy and oversee its implementation. Support provincial and territorial ministries in establishing inter-ministerial committees to combat hate crimes.
    a) Organize the committee via the Ministry of Public Safety and Emergency Preparedness, involving appropriate provincial and territorial government stakeholders.
    b) In provincial and territorial committees, support the involvement of ministries including: Ministries of the Attorney General, Community Safety and Correctional Services, and Education and Training, Colleges and Universities, and provincial Human Rights Commissions.
    c) Ensure the development of implementation, monitoring and evaluation mechanisms for the national hate crime strategy.
    d) Create a joint community-based Hate Crimes Governance Committee to include community members, representatives from the private sector and government officials with knowledge and experience in hate crime issues. The committee would be responsible for monitoring the implementation of the strategy, coordinating joint community and government initiatives, and act as a resource for the inter-provincial and -territorial committee.

2) Reinstate a provision comparable to the previous Section 13 of the Human Rights Act in order to provide a needed tool to hold individuals promoting hatred of identified groups accountable, especially for online postings on websites and social media.
    a) Increase funding to the Canadian Human Rights Commission and the Canadian Human Rights Tribunal in order to provide resources sufficient to deal with hate crime complaints made using Section 13 in a timely manner.

3) Require Attorneys General to publish an annual report in order to report details of hate crime cases that requested Attorney General consent on Section 318 and 319 of the Criminal Code in order to increase transparency with the public.
    a) Create and enforce defined criteria for cases requiring Attorney General consent.
    b) Require Attorney General reporting on:
        i) All cases that requested approval

ii) When it provided consent and did not provide consent
iii) Why it provided consent or why it did not provide consent

4) Collect, monitor and share national hate crime data.
   a) Utilize Statistics Canada's General Social Survey to collect more robust data on hate crimes.
      i) Repeat the Victimization portion of the General Social Survey on an annual basis.
      ii) Expand questions in the Victimization portion of the General Social Survey.
   b) Through Statistics Canada's Canadian Centre for Justice Statistics program, provincial Attorneys General, appropriate provincial Ministries, and police boards, develop standard forms and procedures for collecting and keeping statistics on police-reported hate incidents.
      i) Through an intersectional gender-based analysis (GBA+), design these forms to capture, at a minimum, all incidents that complainants have identified as hate crimes or hate incidents and all incidents for which there is evidence that suggests that they may qualify as hate crimes or hate incidents, including:
         (1) What investigation was undertaken
         (2) What charges, if any, were laid
         (3) Why charges were not laid
         (4) What other charges might reasonably have been laid in the circumstances but were not
         (5) Whether any charges laid proceed to trial and if they did it, why they did not
         (6) What the disposition of the charges was
         (7) Whether, if the accused was convicted, the Crown raised hate or prejudice as an aggravating factor in sentencing
         (8) Whether, in such instances, the court took hate or prejudice explicitly into account as an aggravating factor in sentencing, and what the sentence, if any, was
      ii) Enact regulations requiring that such statistics be kept and made available as indicated above.

5) Provide sufficient funding to create community-based civilian groups, composed of community members, including communities with negative experiences with the police, in order to act as a neutral reporting and advocacy body between police boards and communities. Victims would feel safer reporting to this body as opposed to working directly with the criminal justice system.
   a) Funding should be for community-based agencies to provide anti-oppressive victim support services and trusted third-party reporting platforms to their communities
   b) Funding should be long-term and stable so that community-based agencies can deliver sustainable programming

Council of Agencies Serving South Asians (CASSA)
5200 Finch Ave. East, Suite 301A, Toronto, ON M1S 4Z5
Phone: (416) 932-1359
Email: cassa@cassa.on.ca Website: www.cassa.on.ca

Combatting Online Hate through a National Online Hate Legislation

Online hate legislation is critical in order to support online enterprises in taking action on hate speech posted on their platforms. We recommend developing online hate legislation that includes the following:

1. Adopt a Basic Minimum Standards Approach built on the *Whatcott* Standard

We advise that a basic minimum standards risk-based approach to regulation be adopted. This approach needs to be anchored in a duty for all online platforms to adhere to the Supreme Court of Canada's articulation of the *Whatcott* standard under the *Criminal Code*. Applied in this context of online harms, the *Whatcott* standard should be used to identify online content which, when objectively assessed, would persuade a reasonable person that the content incites violence towards an identifiable group. This will be the most appropriate and efficacious approach to balance the need to protect freedom of expression while mitigating violent impacts of hate online.

2. Require Online Enterprises to Demonstrate Capacity for Risk Assessment

Rather than relying on a nebulous "duty to act responsibly", the *Whatcott* standard should be used to require that all online enterprises, irrespective of size – from Meta, Google or Twitter to Reddit, 4Chan, or many others—to first demonstrate that they can identify and assess the risks of incitement to violence posed to the public by their service.

3. Set Rigorous Transparency Requirements on Online Service Providers

All online service providers with users in Canada would report on their identification and mitigation tools to demonstrate transparency and enhance accountability. On this latter step, we agree with experts on the need for rigorous, significant and sophisticated transparency requirements.

Additional Requirements, Principles, Minimum Standards and Sanctions

1. A New Tort vs. An Effective Regulatory Framework

In our view, confronting online hate that incites violence does not require a new tort involving a vague "duty to act" responsibly. Introducing such a duty risks being overbroad and unintentionally targeting Muslim, BIPOC and other marginalized, vulnerable, immigrant and securitized communities who have the democratic right to legitimately and critically comment on matters of domestic, national, and international concern without the threat of their online content being removed.

Rather, what is required is an effective regulatory framework based on a set of comprehensive, basic minimum standards, to which online service providers would be required to adhere as a condition of

operating. A "duty to act responsibly", while commendable in the abstract will, in practice, result in creating much uncertainty. Conversely, the *Whatcott* standard is one that is already clearly defined in Canadian law and lends greater certainty to an area requiring the same.

2. Foundational Principles as a Condition of Operating

2.1 All online service providers will adhere to the foundational principle that they will not host, cache, or disseminate, content that incites violence towards any identifiable group, including groups identified on the basis of race, national or ethnic origin, colour, religion, immigration status, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, or disability. This foundational principle will inform the basic minimum standards.

2.2 Online service providers will proactively strive to maintain online environments, including video, animated or graphic video and games, chat groups, and any related online content, that are free from content which incites violence against any identifiable group, by developing robust protections and continually enhancing their ability to detect and remove content that incites violence.

3. Basic Minimum Standards as a Condition of Operating

3.1 All online service providers will publish the terms of reference upon which their business model operates, specifying the steps they will take to incorporate, operationalize, and assess their compliance with these foundational principles. This will serve to inject transparency and accountability into how online services operate.

3.2 All online service providers will invest in sufficient staff and technology, including the use of algorithms, artificial intelligence, or other electronic tools, to flag content enhancing rapid detection and removal of online content that incites violence and violates the foundational principles. They will also inform users of the algorithms they use to direct users to specific site or services.

3.3. These basic minimum standards would apply to all online service providers and the broadest spectrum of services operating online ranging from the large tech companies, such as Meta (Facebook, Instagram), to the smaller service providers, including all service providers who host, cache, or disseminate third-party content.

3.4 All online service providers must demonstrate that their trust and compliance departments are robust, efficacious, and coherent with the foundational principles in section 2 above.

3.5 All online service providers will designate a legal representative that must be physically located in Canada and can be held legally liable for violations of the Act.

3.6 All online service providers will maintain bank accounts or physical assets in Canada, with a valuation of no less than 1% of their annual global revenue, with such accounts being subject to garnishment or assets being subject to seizure in the event the service provider is fined for failure to comply with the Act.

3.7 There must be clearly identified benchmarks that all online service providers must meet in order to operate online. For example, how would entities such as 4chan and Reddit demonstrate that they are meeting their obligation to adhere to basic minimum standards? What steps will be taken to enforce compliance by online service providers with the basic minimum standards?

3.8 It is essential that online content which incites violence against Muslims or another identifiable group be removed from the site upon being discovered or reported or, in any event, within 24 hours of being flagged, so as to reduce harm to the victims as soon as practicably possible.

3.9 Racialized communities, given their heightened vulnerability, require proactive measures to prevent online harms from arising. Therefore, service providers must transparently assess the types of risks their service may generate and proactively mitigate those risks through enhanced protections.

Other basic-minimum-standards could include requirements such as:

3.10 Regulating the obligations of digital services that act as intermediaries;

3.11 Providing better protection to users and to fundamental rights online, establishing a powerful transparency and accountability framework for online platforms;

3.12 Establishing effective safeguards for users, including the possibility to challenge platforms' content moderation decisions based on a new obligatory information to users when their content gets removed or restricted;

3.13 Wide-ranging transparency measures for online platforms, including better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users;

3.14 Obligations for very large online platforms and search engines (with a client/user base of 10% of the population or greater) to prevent abuse of their systems by taking risk-based action, including oversight through independent audits of their risk management measures. Platforms must mitigate against risks such as cyber violence or inciting violence against identifiable groups online. These measures must be carefully balanced against restrictions of freedom of expression, and should be subject to independent audits;

3.15 Application of the Act without discrimination, including to those online intermediaries established outside of Canada that offer their services in Canada. When not established in Canada, they will have to appoint a legal representative, as many companies already do as part of their obligations under other legal instruments;

3.16 Very large online platforms and very large online search engines will have to assess and mitigate societal risks stemming from the design and use of their service;

3.17 All platforms, except the smallest, will be required to set up complaint and redress mechanisms and out-of-court dispute settlement mechanisms, cooperate with trusted flaggers, take measures against abusive notices, deal with complaints, vet the credentials of third-party suppliers, and provide user-facing transparency of online advertising;

3.18 Very large online platforms and very large online search engines, may be subject to further specific rules due to the particular risks they pose in the dissemination of illegal content, including content that incites violence and consequent societal harms;

3.19 Very large online platforms will have to meet risk management obligations, external risk auditing and public accountability, provide transparency of their recommender systems and user choice for access to information, as well as share data with authorities and researchers;

3.20 Enforcement mechanisms are not limited to fines: the appropriate authority, Digital Services Commissioner (DSC) for example and the Commission, would have the power to require immediate actions where necessary to address very serious harms, and platforms may offer commitments on how they will remedy them;

3.21 For rogue platforms that refuse to comply with important obligations and thereby endanger people's life and safety, it will be possible to seek a court order for a temporary suspension of their service, after involving all relevant parties;

3.22 When it comes to supervision of very large online platforms and online search engines, it will be the DSC who will be the sole authority to supervise and enforce the specific obligations under the Act that apply only to these providers. In addition, the DSC will be responsible for supervision and enforcement for any other systemic issue concerning very large online platforms and very large online search engines;

3.23 In order to ensure effective compliance with the Act, it is important that the Commission has at its disposal necessary resources, in terms of staffing, expertise, and financial means, for the performance of its tasks under this Act. To this end, the Commission will charge supervisory fees on online service providers, the level of which will be established on an annual basis and scaled in relation to the volume of annual gross revenue of each service provider. The overall amount of annual supervisory fees charged will be established on the basis of the overall amount of the costs incurred by the Commission to exercise its supervisory tasks under this Regulation, as reasonably estimated beforehand.

4. Sanctions

4.1 There must be a clear, meaningful, and significant sanctions regime that will compel all online service providers to operate in a manner that encourages compliance with the foundational principles and basic minimum standards as codified in the Act and reduces online harms.

4.2 It is crucial that all online service providers understand that the hosting, caching, or dissemination of content that violates the foundational principles, thereby inciting violence towards (Muslims or another) any identifiable group, will be harshly sanctioned.

4.3 All online service providers will designate a legal representative that must be physically located in Canada and can be held legally liable for violations of the Act.

4.4 All online service providers will maintain bank accounts or physical assets in Canada, with a valuation of no less that 1% of their annual global revenue, with such accounts being subject to garnishment or such assets being subject to seizure in the event the service provider is fined for failure to comply with the Act.

4.5 Sanctions will be imposed for failing to comply with the basic minimum standards. Sanctions, including escalating monetary fines, up to 10% of the service provider's gross annual revenues, for example, as well as potentially de-platforming or blocking service providers who:

(i) Repeatedly violate the foundational principles after having been advised to correct their behaviour, or

(ii) Fail or neglect to remove online content that violates the foundational principles, within 24 hours after having being advised to do so.

4.6 Online service providers who repeatedly violate the Act could, in addition to escalating fines, also face temporary de-platforming or blocking.

4.7 As an alternative, or in addition, to fines, de-platforming or blocking service providers, create an offence provision whereby the owner of the online service provider would be personally subject to direct criminal sanction: charged, arrested, and prosecuted for the hosting, caching, or dissemination of online content that incites violence. Or, if the owner of the online service provider is outside of Canada, charged, subject to an extradition request, and then prosecuted to the full extent of the law. Appropriate amendments to the *Criminal Code*, providing for substantial fines and/or imprisonment in the event of conviction, dependent upon whether the offence is summary conviction or indictable, would be required to dovetail this sanction.