

**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

**Anti-hate Community Leaders' Group Joint Statement**

Dear federal government partners,

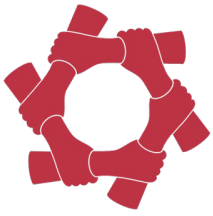
We are writing to you in order to present our recommendation to develop federal online hate legislation. We, the Anti-Hate Community Leaders' Group, represent over 40 diverse community leaders and organizations working to strengthen hate crime laws and policies across Canada. We urge you to take immediate action and bring a comprehensive legislation that balances people's life and dignity with the freedom of expression.

According to Statistics Canada, 364 cyber crimes were recorded by the police between 2010 and 2017. The most targeted populations included the Muslim population (17%), groups with diverse sexual orientation (15%), the Jewish population (14%), and the Black population (10%). Police reported hate crimes towards Indigenous communities rose by 152% in the pandemic.

However, there is a large discrepancy between the number of incidents of online hate witnessed by Canadians compared to those reported to police. In 2019, a poll by Léger Marketing for the Association for Canadian Studies found that 60% of Canadians have seen "hateful or racist speech on the internet." A large proportion of hate incidents today are taking place online, however, a lack of data collection, appropriate response and accountability from online platforms lead to perpetrators not facing accountability for posting content that incites violence. There is a significant need for online platforms to better identify, remove, respond to, and report content that incites violence in order to address rising online hate.

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. **An Effective Regulatory Framework:** 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.
2. **Foundational Principles as a Condition of Operating:** 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.
3. **Basic Minimum Standards built on the Whatcott Standard as a Condition of Operating:** All online service providers will specify the steps they will take to incorporate, operationalize, and assess their compliance with these foundational principles.
4. **Sanctions:** A clear, meaningful, and significant sanctions regime that will compel all online service providers to comply with the foundational principles and basic minimum standards. Violation of foundational principles will lead to harsh sanctions.



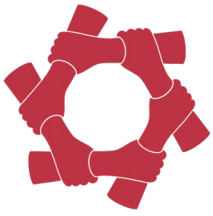
**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

Online hate legislation will develop a common standard for what constitutes online hate that incites violence against an identifiable group, ensure that online platforms are able to identify and respond to such online hate, and establish transparency and accountability where online platforms require enterprises to report on their compliance methods to government partners. We urge you to take immediate action and implement our legislative recommendations attached to this letter.

Signed,

The Anti-Hate Community Leaders' Group

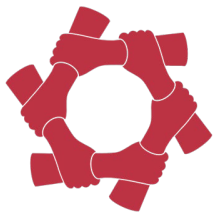
1. Access Alliance Multicultural Health and Community Services
2. Across Boundaries
3. Alliance for South Asian AIDS Prevention
4. Bangladeshi-Canadian Community Services (BCS)
5. Bangladesh Centre & Community Services (BCCS)
6. Canadian Anti-Hate Network
7. Canadian Arab Institute
8. Canadian Association of Jews and Muslims
9. Canadian Centre for Victims of Torture
10. Canadian Council of Muslim Women (CCMW)
11. Canadian Council of Muslim Women Montreal
12. Canadian Muslim Vote
13. Catholic Crosscultural Services
14. Coalition Against White Supremacy & Islamophobia (CAWSI)
15. Centre for Newcomers (Edmonton)
16. Centre of Race and Culture
17. Chinese and Southeast Asian Legal Clinic
18. Chinese Canadian National Council for Social Justice
19. Chinese Canadian National Council Toronto Chapter
20. City of Toronto - Confronting Anti-Black Racism Unit
21. Colour of Poverty - Colour of Change
22. Gibraltar Leadership Academy
23. Hispanic Development Council
24. Islamic Foundation of Toronto
25. JSpaceCanada
26. Midyanta Community Services
27. National Council of Canadian Muslims (NCCM)
28. Ontario Agency for Health Protection and Promotion
29. Ontario Council of Agencies Serving Immigrants (OCASI)
30. Progressive Intercultural Community Services (PICS) Society
31. Punjabi Community Health Services
32. Roots Community Services



**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

33. Salaam Canada
34. South Asian Legal Clinic of Ontario
35. South Asians Women's Rights Organization
36. Tamil Canadian Centre for Civic Action
37. Urban Alliance on Race Relations
38. United for All Coalition
39. United Way East Ontario
40. United Way of Greater Toronto
41. World Sikh Organization

The [Anti-hate Community Leaders Group](#) was convened in 2019 by the [Council of Agencies Serving South Asians \(CASSA\)](#) to take a proactive and preventative approach to address the increase hate-motivated violence and crimes that are unfortunately on the rise in Canada. The AHCL Group brought together more than 40 diverse organizations to tackle hate, with a specific mandate in the following six areas: online hate and social media, law enforcement and legislation, the education system, media engagement, political engagement, and interfaith/interracial dialogue. Aligned with these mandates, AHCL Group has undertaken multiple projects, including analysis of legal tools and legislation, developing tools to combat hate-motivated speech online, and working with municipal police services to improve their hate-crime reporting processes.



**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

**Recommendations to the Federal Government's to Address Online Hateful Content that Incites Violence**

**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**

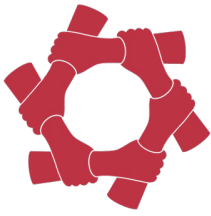
All online service providers with users in Canada would report on their identification and mitigation tools to demonstrate transparency and enhance accountability. On this latter step, we agree with experts on the need for rigorous, significant and sophisticated transparency requirements.

**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



## **ANTI-HATE COMMUNITY LEADERS' GROUP**

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.

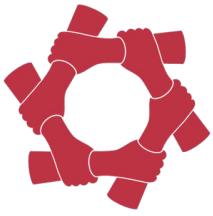
3.2 All online service providers will invest in sufficient staff and technology, including the use of algorithms, artificial intelligence, or other electronic tools, to flag content enhancing rapid detection and removal of online content that incites violence and violates the foundational principles.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



**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

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;

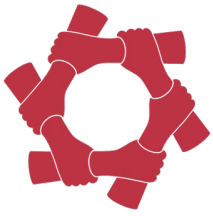
3.11 Providing better protection to users and to fundamental rights online, establishing a powerful transparency and accountability framework for online platforms;

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;



## **ANTI-HATE COMMUNITY LEADERS' GROUP**

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;

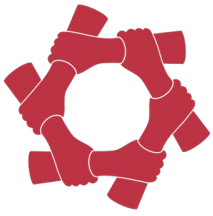
3.21 For rogue platforms that refuse to comply with important obligations and thereby endanger people's life and safety, it will be possible to seek a court order for a temporary suspension of their service, after involving all relevant parties;

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



**ANTI-HATE  
COMMUNITY  
LEADERS' GROUP**

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 than 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.

**We will not support a regulatory scheme that can be used to:**

1. Harm the safety of marginalized and securitized groups;
2. Undermine healthy citizen engagement and a flourishing active digital citizenship; or,
3. Render nugatory the essential and fundamental democratic freedoms of all Canadians.