

MEMORANDUM

To: CRCL, Brian Sterling and Jennifer Brand

From: HSOAC RAND

Date: August 08, 2022

Subject: Monitoring Online Activity to Combat Violence and Protecting First Amendment Rights

On July 21, 2022, at the request of CRCL, RAND hosted a brainstorming session with experts on social media, extremism, and constitutional law. This session had two primary aims: 1) first, to identify potential research questions related to monitoring online activity to combat violence while protecting civil liberties and 2) second, to identify organizations, subject matter experts, and other stakeholders that should be invited to a future conference or workshop on this topic. This memorandum summarizes the results of the brainstorming session.

Research Questions

Brainstorming session participants identified a number of potential research questions related to monitoring online activity to combat violence while protecting civil liberties. These questions are listed below.

General

1. How useful is monitoring online activity as a law enforcement mechanism for preventing offline violence?
 - a. How predictive is social media activity of the likelihood of violence?
 - b. What types of social media activity suggest an increased likelihood of violence?
2. What is the current ecosystem of governmental and non-governmental entities that monitor online activity, and how does DHS fit into this ecosystem?

Existing Authorities and Policies

3. What are the existing constitutional, statutory, regulatory, and policy restrictions on investigating violent speech online?
 - a. Are there legal or ethical limitations on the types of online information that can be investigated, such as metadata, anonymized information, posts in public fora, and posts in private fora?
 - b. What are the legal and ethical considerations involved in governmental purchases of information from the public marketplace, such as GPS data, social media feeds, and social media analytics platforms?
 - c. What can the government do with the information it collects?

- d. What can state and local governments (e.g., fusion centers, law enforcement agencies) do that the federal government cannot do in this space? Can the federal government provide support to SLTT partners to conduct this work?
- e. What can private citizens and non-profit organizations do that the federal government cannot do in this space? Can the federal government provide support (e.g., grants) to non-governmental partners to monitor online activity?
- 4. Does the federal government need new authorities, guidance, or capabilities to effectively monitor and investigate online activity?
- 5. How should the federal government coordinate its approach to online violence?

Credibility and Public Support

- 1. How can the federal government build public support for monitoring online activity to combat violence?
 - a. What steps should be taken to reduce the gap between what is legally permissible and what is acceptable to the public?
 - b. Are there ways to modify internal processes or establish guardrails to increase public support?
- 2. How can the federal government measure public support for approaches to countering online violence and violent speech?
- 3. How can the federal government build public support by promoting equity in its approach to monitoring online speech?
 - a. How can the federal government ensure that its approach does not have a disproportionate impact on marginalized communities?
 - b. Should the federal government deemphasize the distinction between posting pro-jihadi material versus pro-REMVE material as a predicate for investigation?

Collaboration

- 1. To what extent should the federal government collaborate with social media companies and SLTT authorities to combat violence through monitoring online activity?
 - a. Should the federal government establish a forum to enable social media companies to voluntarily report concerning information to federal and SLTT authorities? What might such a forum look like?
 - b. Should the federal government establish working groups or collaborations between researchers and federal and SLTT authorities to monitor online activity to combat violence?
- 2. How can the existing fusion center model be modified to improve collaboration and coordination?
- 3. To what extent should the federal government rely on tech companies and other large vendors to provide tools monitor online activity?

Key Stakeholders

In addition to the research questions noted in the previous section, brainstorming session participants identified organizations—including non-profit, for-profit, and academic organizations—and individuals that should be invited to a future conference or workshop on this topic. Table 1 provides a list of these key stakeholders.

Table 1. Key Stakeholders

Government Entities	Non-Profit Organizations	For-Profit Organizations	Academic Centers	Individuals
• DOJ OLC • U.S. Attorney's offices • FBI OGC	• Anti-Defamation League (ADL) • Southern Poverty Law Center • Institute for Strategic Dialogue • Atlantic Council Digital Forensic Research Lab • Stanford Internet Policy Center • Color of Change • American Bar Association	• Google Moonshot • Miburo Solutions • Twitter • Meta	• Center on National Security, Fordham Law School • Reiss Center on Law and Security, NYU Law • Brennan Center for Justice, NYU Law • Institute for Constitutional Advocacy and Protection, Georgetown Law	• David Schanzer • Kate Klonick • Renee DiResta • Daphne Keller • David Kaye • Rashad Robinson • Evan Sellinger • Eva Galperin • Jillian York • Nina Jankowicz • Evelyn Douek • Danah Boyd