ANDREW R. GARBARINO, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

September 22, 2025

Mr. Kyle Daigle
Chief Operating Officer
GitHub
88 Colin P. Kelly Junior St.
San Francisco, CA 94107

Dear Mr. Daigle:

The assassination of Mr. Charlie Kirk serves as a sobering reminder of the escalating threats facing our nation from violent extremists. These heinous and senseless acts of violence further expose the challenging and sometimes dangerous nature of online platforms that serve to foment extremism, leading to deadly real-world consequences. In furtherance of our ongoing investigation into domestic terrorism cases, the Committee is investigating how specific bad actors may use online platforms to facilitate radicalization, disseminate extremist content, and aid in individuals' planning efforts to conduct violent attacks within the United States. Accordingly, the Committee requests documents and information to facilitate its investigative and legislative objectives.

In recent years, violent extremists have increasingly relied on secure communication tools and anonymous cloud storage services to evade detection by law enforcement.[1] These platforms, while serving as essential tools for legitimate privacy and free expression, have also been exploited to further extremist agendas.

Domestic terrorism cases continue to demonstrate the role of these platforms in both ideological radicalization and operational planning.[2] Last week, U.S. Federal Bureau of Investigation (FBI) Director Kash Patel testified that the FBI is investigating members of a Discord chat in which Tyler Robinson, the suspect charged with the murder of Mr. Kirk, allegedly confessed to the killing hours before being taken into custody.[3] This pattern of digital coordination and extremist messaging was observed in other recent attacks: in January of this year, Shamsud-Din Bahar Jabbar killed 15 people in New Orleans by driving a truck into a

---

[1] Gabriel Weimann, et. al., *Generative Terror: The Risks of Generative AI Exploitation*, CTC SENTINEL, Vol. 17, Issue 1 (Jan. 2024).
[2] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, EMERGING TECHNOLOGIES AND POSSIBLE MALIGN USES BY TERRORISTS (2024).
[3] Max Rego, *FBI 'running down' more than 20 Discord users in Kirk shooting probe: Patel*, THE HILL (Sept. 16, 2025).

crowd, after publicly posting videos declaring support for ISIS and linking his attack to the group's broader ideological agenda.[4] Also in January, a 17-year-old student at Antioch High School in Tennessee, who had reportedly been actively engaged with extremist content online through several platforms, fired multiple shots and killed a classmate in the school cafeteria.[5] Similar extremist views were identified in videos posted online by the 23-year-old shooter who opened fire on Annunciation Catholic Church in Minneapolis in August, killing two children and injuring 18 other worshippers in a case that FBI Director Patel referred to as "an act of domestic terrorism motivated by a hate-filled ideology."[6] In July 2024, the then 20-year-old who attempted to assassinate President Donald Trump in Butler, Pennsylvania, reportedly used encrypted messaging accounts hosted on foreign platforms during the planning stages of his attack. [7]

Beyond evading detection, these platforms can serve as crucial tools for global coordination, propaganda dissemination, and financing.[8] Extremists often begin cultivating their narratives on smaller, less regulated platforms before expanding their reach to larger audiences.[9] These same platforms are also being used to solicit funds—blurring the lines between propaganda and material support—and reinforcing the urgent need for more robust oversight. [10]

This evolving threat underscores the importance of timely intervention and highlights the vital role digital platforms play in safeguarding national security. The Committee has convened hearings and roundtables with law enforcement, technology experts, and community organizations, all of which have underscored the critical importance of early detection and the shared responsibility of digital platforms in this effort. The Committee must hear directly from these platforms to better understand what is already being done, and what more can still be done, to prevent extremist violence in the United States from being orchestrated through these online channels.

To further strengthen this partnership and support the Committee's ongoing inquiry into domestic terrorism, please produce the following documents and information covering the period of September 1, 2024, through the present by October 6, 2025:

1. All documents and communications, including but not limited to policies, procedures, and internal communications, regarding or referring to mechanisms, including any specific algorithms, used to monitor, detect, and flag extremist content—including text, videos, and images—shared on your platform.

---

[4] Adiel Kaplan, et. al., *'A perfect storm': Extremism online and political polarization are increasing the risk of attacks, experts say*, CBS NEWS (Jan. 4, 2025).
[5] *Antioch, Tenn., Shooter Inspired by Broad Extremist Beliefs and Previous Mass Killers,* ANTI-DEFAMATION LEAGUE (Jan. 23, 2025).
[6] Selina Guevara, et. al., *Minneapolis church shooting search warrants reveal new details and evidence*, NBC NEWS (Aug. 29, 2025).
[7] Greg Wehner, *Trump shooter had multiple encrypted accounts overseas, including Germany: Rep. Waltz*, FOX NEWS (Aug. 21, 2024).
[8] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-24-106262, COUNTERING VIOLENT EXTREMISM: FBI AND DHS NEED STRATEGIES AND GOALS FOR SHARING THREAT INFORMATION WITH SOCIAL MEDIA AND GAMING COMPANIES (2024).
[9] *Id*.
[10] U.S. DEP'T OF THE TREASURY, 2024 NATIONAL TERRORIST FINANCING RISK ASSESSMENT (2024).

2. All documents and communications regarding or referring to procedures for escalating and sharing suspicious behavior, as well as credible threats, with federal, state, or local law enforcement agencies.

3. All documents and communications between your platform and the FBI regarding suspicious behavior and/or credible threats.

4. A description of actions taken and/or policies implemented to enhance visibility into potential threats, detection capabilities, accountability measures, and transparency protocols.

5. Any internal reviews, audits, or red-teaming exercises and their respective results conducted to identify vulnerabilities that domestic violent extremists might exploit on your platform.

We appreciate your ongoing commitment to working collaboratively with the Committee to address these critical issues and ensure our shared goal of a safer digital environment.

Per Rule X of the U.S. House of Representatives, the Committee is the principal committee of jurisdiction for overall homeland security policy and has special oversight functions of "all Government activities relating to homeland security, including the interaction of all departments and agencies within the Department of Homeland Security." If you have any questions regarding this request, please contact the Committee on Homeland Security Majority staff at (202) 226-8417. Thank you for your prompt attention to this matter.

Sincerely,

ANDREW R. GARBARINO
Chairman
Committee on Homeland Security

AUGUST PFLUGER
Chairman
Subcommittee on Counterterrorism and Intelligence

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security

The Honorable Seth Magaziner, Ranking Member
Subcommittee on Counterterrorism and Intelligence