United States Senate

WASHINGTON, DC 20510

November 18, 2019

Matthew Prince
Chief Executive Officer
101 Townsend Street
San Francisco, California 94107

Dear Mr. Prince,

We write with concern that technology companies have failed to take meaningful steps to stop the creation and sharing of child sexual abuse material (CSAM) on their online platforms. While the internet has fostered unprecedented opportunities for social and economic growth, it has also nurtured the flourishing of horrendous crimes, including crimes against children. We are writing to request information on what your company is actively doing to identify, prevent, and report child sexual abuse material and other forms of child exploitation.

Recent *New York Times* investigative reports have vividly described the rapid increase of CSAM images and video on prominent online platforms; a threat that has not received a consistent and forceful response from the tech industry.[1] Over the past four years, reports of suspected child sexual exploitation to the National Center for Missing & Exploited Children's (NCMEC) CyberTipline have exploded, from 1.1 million in 2014 to 18.4 million reports covering 45 million photos and videos in 2018. The increase of online sextortion and other changes in the nature of exploitation have driven up the amount of CSAM videos, posing greater risk to victims and causing more technical challenges to the detection of abusive content. Considering the breadth of internet platforms and services, even these jarring numbers likely represent only a limited amount of the child exploitation crimes online.

Initiatives to end child exploitation, such as the CyberTipline, have benefited substantially from the expertise, participation, and technical resources provided by many in the tech industry. We welcome the efforts of those companies that have gone beyond what is legally required and exercised leadership among their peers. However, it is clear to us that others in the tech industry have not consistently acted on their responsibility to prevent child exploitation. Congress recognized the need for the tech industry to step up when it passed the PROTECT Our Children Act in 2008, which required that online platforms report child abuse to NCMEC and preserve evidence for authorities, and Congress updated these provisions in 2018. Despite this

[1] Keller, Michael H., and Gabriel J.X. Dance. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" New York Times, September 28, 2019. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

Keller, Michael H., and Gabriel J.X. Dance. "Child Abusers Run Rampant as Tech Companies Look the Other Way" New York Times, November 9, 2019. https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html.

requirement, *New York Times* cited concerning examples of how law enforcement has encountered delays of weeks or months in responses to requests for information, sometimes leading to suspects being notified of investigations or data being no longer available. In other cases, platforms failed to take down clearly abusive content. We have heard similar concerns from children's protection advocates and law enforcement that platforms' detection and enforcement efforts have not kept pace with technological development and changes in the nature of child exploitation. For example, malicious individuals have grown adept at circumventing the blocking tools used by platforms, such as bypassing hashing and fingerprinting techniques by altering images and videos.[2] Yesterday's solutions are not sufficient to stop technologically enabled crimes.

Technology companies have a vital and irreplaceable role in stemming this flood of child exploitation and abuse. Online platforms cannot be a haven for child exploitation due to neglect and siloed efforts, and companies should be willing to collaborate with peers and NGOs to keep up with the threat. While we applaud the development of new technologies to improve detection of CSAM, these efforts should not lead to companies acting as islands because they produce incompatible fingerprints or are fettered by proprietary dependencies. Preventing child exploitation, including stopping the sharing of CSAM, requires a sustained and serious commitment across teams and the life cycle of products that uses the state-of-the-art, promotes collaboration, and is responsive to the needs of law enforcement.

Given the sensitivity and seriousness of the matter, we request a written response to the following questions by December 4, 2019:

1. Do you automatically identify CSAM that is created and uploaded to your platform(s)? If so, does this include assessing uploaded videos and video streaming for CSAM? Please describe how you identify CSAM and what measures have been taken to ensure this system reflects the state-of-the-art and is accurate. If you use known detection products or services, such as PhotoDNA, please indicate so.

2. Does this detection process use the NCMEC database of hashes of known CSAM to match against content created and uploaded to your platform(s)? If not, why not?

3. How many reports of CSAM have you provided to the NCMEC CyberTipline on an annual basis for the past three years?

4. How many pieces of CSAM did you remove from your platform(s) in 2018? Of those, how many pieces of CSAM were removed or blocked based on automated detection? How many pieces of CSAM that were identified had not previously existed in known CSAM databases used by your company?

5. What measures have you taken to ensure that steps to improve the privacy and security of users do not undermine efforts to prevent the sharing of CSAM or stifle law enforcement

---

[2] Lapowsky, Issie. "Why Tech Didn't Stop the New Zealand Attack From Going Viral" Wired, March 15, 2019. https://www.wired.com/story/new-zealand-shooting-video-social-media/

investigations into child exploitation?

6. What are the main obstacles in identifying all CSAM posted to your platform(s) automatically? Please describe any circumstances in which you do not or cannot apply detection technologies against content transmitted on your platform(s), such as within certain products or features.

7. Do you provide notice to individuals involved in the transmission of CSAM when you report or submit evidence of such activities to NCMEC or law enforcement?

8. Do you share with the cross-industry database of CSAM hashes and fingerprints? How many unique indicators of child exploitation did your company share within this arrangement in 2018? If you do not provide to this database, why not?

9. Do you take hashes from the cross-industry database of CSAM hashes and fingerprints? How many such CSAM hashes and fingerprints did you take in 2018?

10. Are the hashes and other indicators of CSAM produced by your detection technology compatible with other systems used in the tech industry? What steps have you taken to standardize fingerprints and ensure that your fingerprints of CSAM can be used as actionable input for other companies' detection efforts?

11. What other barriers do you face in receiving or sharing information, hashes, and other indicators of CSAM with other companies?

12. Have you implemented any technologies or techniques to automatically flag CSAM that is new or has not been previously identified, such as the use of machine learning and image processing to recognize underage individuals in exploitative situations?

13. What steps have you taken to ensure that CSAM detection efforts are incorporated in each appropriate product and service associated with your platform(s)? How many dedicated engineering full time employees work on CSAM detection and elimination?

14. What steps have you taken to ensure that reports to NCMEC on a consistent basis include all information necessary to respond to threats to children, such as the inclusion of contextual information connected to the CSAM and appropriate metadata related to the timing and source of the material?

15. What steps have you taken to ensure that you respond in a timely manner to questions from law enforcement regarding CSAM reports? What auditing procedures have you put in place to ensure that you maintain records regarding CSAM after reporting illegal content to law enforcement authorities?

16. If your platform(s) include a search engine, please describe the technologies and measures you use to block CSAM from appearing in search results.

17. What, if any, proactive steps are you taking to detect online grooming of children?

Thank you for your attention to these important issues. We look forward to your response.

Sincerely,

Richard Blumenthal
United States Senate

Josh Hawley
United States Senate

John Cornyn
United States Senate

Lindsey O. Graham
United States Senate

Mazie K. Hirono
United States Senate