CLOUDFLARE

December 4, 2019

The Honorable Richard Blumenthal
U.S. Senate
706 Hart Senate Office Building
Washington, DC 20510

The Honorable Joshua Hawley
U.S. Senate
212 Russell Senate Office Building
Washington, DC 20510

The Honorable John Cornyn
U.S. Senate
517 Hart Senate Office Building
Washington, DC 20510

The Honorable Lindsey Graham
U.S. Senate
290 Russell Senate Office Building
Washington, DC 20510

The Honorable Mazie Hirono
U.S. Senate
713 Hart Senate Office Building
Washington, DC 20510

Dear Senators Blumenthal, Cornyn, Graham, Hawley, and Hirono,

We write in response to your letter dated November 18, 2019 which expresses your significant concerns about the proliferation of Child Sexual Abuse Material (CSAM) on online platforms and sets forth a number of related requests for information. Cloudflare shares your concern about the proliferation of CSAM on online platforms, so we appreciate the opportunity to provide the information in this letter to assist your efforts, and we pledge our continued support for your efforts on this issue.

As you note in your letter, the Internet has "fostered unprecedented opportunities for social and economic growth," but that promise is threatened by various forms of abuse that occur, perpetuate, and grow online. Since our founding, Cloudflare has been focused on identifying and responding to some of the most insidious hackers and cybercriminals online and have worked to make broadly available cybersecurity tools that can be used to counter such threats. Even though we are not a platform and generally do not host content, we have worked hard to understand our role in the Internet ecosystem and have built tools and relationships to allow us to play a productive role in the response to concerns about CSAM and other harmful content.

As we think about the question of how to preserve the promise of the Internet while addressing these abuses, we have engaged proactively to help lawmakers and civil society understand how the core of the Internet operates as they work to develop proactive responses to challenges like CSAM, disinformation, privacy, etc. in the places

they can be most effective.

Background on Cloudflare

Cloudflare is an American Internet infrastructure company that provides security, performance, and reliability services to more than 20 million Internet web properties (e.g. domains, websites, application programming interfaces, mobile applications). Internet properties powered by Cloudflare have their Internet traffic routed through Cloudflare's intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks.

Founded in 2010, Cloudflare has a mission to "help build a better Internet." Inherently this means we aim to serve everyone on the Internet, from individual developers, to small businesses, to the largest enterprises. In the past, delivering Internet security, performance, and reliability not only required an organization to buy rooms full of expensive network appliances but also to hire IT teams to manage them. While there were some companies that could afford this, the cost was prohibitive for many. Instead of serving only those that could have paid the most, Cloudflare intentionally made the decision to start by focusing on organizations and individual developers that had previously been underserved. We made our products not only affordable, but easy to use.

Importantly for consideration of the present issue and in response to your questions, Cloudflare is an Internet infrastructure company that does not operate a platform and our core services do not include hosting. This means that content is not uploaded to our network by users of our core services. Similarly, Cloudflare does not operate a social network where individuals can post or communicate with each other, and we don't provide any sort of service resembling direct messaging. Instead, Cloudflare sits several layers below those sorts of interactions occurring at the application layer of the Internet stack, and even outside the services that host content, to provide network infrastructure to ensure the secure and effective transmission of Internet communications in the face of rapidly-increasing cyber threats. By our estimate, Cloudflare's network blocks more than 72 billion cyber attacks each day.

Headquartered in San Francisco, CA, Cloudflare currently has approximately 1200 full-time employees.

Response to Abuse Complaints

Cloudflare provides its services through a network of data centers located in more than 90 countries, functioning as what is called a "reverse proxy." This reverse proxy sits between the websites that use our services and the public Internet in order to protect the websites from malicious attacks. In effect, these servers work as a gatekeeper reviewing

incoming requests to identify and block suspicious malicious actors or incoming requests that reflect the pattern of a cyberattack, like a distributed denial of service (DDoS) attack.

As a result of this configuration, Internet users attempting to identify where certain domains resolve, or where they are hosted, using widely-available tools (e.g., the ICANN WHOIS lookup) will often find information about the Cloudflare edge server. When people have questions or complaints about websites that are operated by others or whose content is hosted elsewhere, they will often reach out to Cloudflare as a result of information obtained through these search tools. Cloudflare has set up a process to address effectively the thousands of abuse complaints we receive each week regarding websites using Cloudflare's services.

The centerpiece of Cloudflare's abuse process is an automated system accessible through www.cloudflare.com/abuse, where third-parties can submit complaints about websites based about concerns on any basis, including common reports regarding things like cyber threats (e.g., phishing or malware) or illegal or concerning content (e.g., copyright, violent threats, CSAM). In response to such complaints, Cloudflare will forward the complaint to the website operator and hosting provider, and in addition, will respond to the complaining party with information identifying and providing contact information for the website hosting provider.

Cloudflare's abuse processes are based on the idea that the goal of those looking to address problematic content is in having the website operator take action or having the hosting provider remove the content. Cloudflare's abuse process attempts to facilitate those processes. Removing Cloudflare's core services from a website will not modify or remove the content available on the origin server, it will merely remove cybersecurity protections and other performance tools that will continue to allow access the content, albeit in a marginally slower way and in a way that is more vulnerable to cyber attack.

Specifically with regard to abuse complaints reporting CSAM, Cloudflare has created an abuse process based upon the policy judgments in the 2008 PROTECT Our Children Act (the "Act") and its recent amendments. Such a legal regime is vitally important as the infrastructure of a company like Cloudflare may touch millions of websites and their users, and we need to understand how we can contribute constructively to this effort even if we are not able to remove the content on our own. Understanding the role of different types of infrastructure in the larger framework is therefore important. We appreciate your focus in this area.

Cloudflare's abuse process for addressing CSAM is designed to comply with the Act's goals of ensuring the National Center for Missing and Exploited Children (NCMEC) and law enforcement have the information they need to investigate reports of CSAM while

minimizing human intervention and "legitimate" review of CSAM outside those organizations.

Following an allegation or report of CSAM, Cloudflare immediately forwards the report to NCMEC and, unless the complaint chooses otherwise, to the website operator and hosting provider. Cloudflare will also provide NCMEC with the name of the hosting provider, the abuse point of contact for that hosting provider, and the origin IP address identifying where the website at issue is hosted. We provide this information so that NCMEC can quickly identify and contact the hosting provider. Over the last three years, we have provided 1,111 reports to NCMEC in 2019 (to date), 1,417 in 2018, and 627 in 2017.

Through our ongoing work with them, we understand that NCMEC and law enforcement typically work to confirm the legitimacy of the report by reviewing the content and, if appropriate, work directly with the website operator and hosting provider to investigate the report and take appropriate action. Cloudflare's termination of service to a domain at this point will not remove that content from the web and has the potential to disrupt the investigation being done by NCMEC and law enforcement. Although we generally do not receive updates from NCMEC about their work on our reports, there are occasions when NCMEC will come back to us with requests for additional information or to report that they have confirmed the legitimacy of the complaint but have not been able to work effectively with the hosting provider; in those cases, Cloudflare will take action to remove the website from our network and to disable caching for the website. In cases where it is determined that a website is solely and intentionally engaged in the distribution of CSAM, Cloudflare will terminate service to that domain. In addition to working with NCMEC as contemplated under the Act, Cloudflare works cooperatively with a number of law enforcement and advocacy groups on this topic.

Cloudflare has set up a "trusted reporter" program where we will provide hosting provider information as well as the origin IP address in an expedited manner to nearly 60 organizations that are tracking investigations of CSAM violations around the world, including the IWF, INHOPE, the Australian eSafety Commission, and Meldpunt. We routinely respond to requests from these organizations for hosting information, providing responses over the last five years, for example, to more than 13,000 IWF requests, more than 5,000 requests from Meldpunt, and more than 86,000 requests from the Canadian Centre for Child Protection's automated crawler. Cloudflare also receives and responds to law enforcement requests for information as part of investigations related to CSAM or exploitation of a minor. In addition, Cloudflare is regularly in touch with Interpol, and frequently receives an updated copy of the Internet Worst of List (IWOL). Following notification from Interpol, Cloudflare takes immediate action to terminate service to a domain identified on the IWOL.

Based upon these determinations and interactions, we have terminated service to 5,428 domains over the past 8 years.

Cloudflare's Outlook

Based on the role of Cloudflare's core services, which do not host these websites and are unable to remove or modify content hosted elsewhere, our current role of facilitating information to support the effective operation of the system set out in the Act makes sense. Nonetheless, we believe it is important to contribute to ongoing efforts to review this problem and the ways that various service providers on the Internet can contribute to improved solutions.

We have worked in 2019 to improve our channels of communication with NCMEC, and with international organizations that are focused on combating the abuse of children. We have been focused on ways in which we can more directly support their efforts. In response to their requests, we are in the process of developing an automated tool that will allow trusted reporters like NCMEC to directly access information about the underlying hosting providers of websites that use Cloudflare's services. We expect this tool will be available and rolled out in early 2020.

In addition, we will be implementing revised policies to address new Cloudflare products like Cloudflare Stream and Cloudflare Workers that will serve as the origin host of some content. Although we do not have any information to suggest that these products, which have limited utilization to date, have been used to store CSAM material, we plan to implement proactive searching and scanning of content that we host before those products expand to a broader audience. We are currently working with NCMEC and IWF to develop the tools, including potentially PhotoDNA, that we would need to implement such scanning as those products grow in use.

Finally, we do not believe that improving the privacy and security of our users has to come at the expense of efforts to combat CSAM. Indeed, as a cybersecurity company, we believe it is critical that companies think proactively about ways to address CSAM online as technology evolves, and online environments become more secure. Having law-abiding companies avoid new privacy-enhancing standards or technology will not prevent use of that technology to spread CSAM, but it will prevent the development of creative technical ways of combating its spread in a more secure environment.

The new technical standard of DNS-over-HTTPs (DoH) provides a good example of this challenge. DoH is a relatively new standard approved by the Internet Engineering Task Force (IETF), that limits unnecessary access to web-browsing data and helps prevent

bad actors from misdirecting Internet traffic, by encrypting Domain Name Service (DNS) requests. Some entities that want continued access to unencrypted DNS data have argued that DoH will prevent them from blocking CSAM, even though there are a variety of technical solutions that would allow such blocking while still limiting access to private data through DoH. Rather than arguing about a standard that has already been approved and deployed, our view is that the goal should be to work to expand understanding of and access to the technical solutions to block CSAM that work with DoH, such deployments of DoH at the network level, filtered DNS resolvers, and browser plug-ins.

****

We hope our responses to your questions have been helpful, and we would be happy to come in to speak with you and your staff to answer any questions or provide you additional information.

Sincerely,

Doug Kramer
General Counsel