



שורת הדין (ע"ר)

בית הקרן, רח' התע"ש 10 רמת גן, 52512
Beit Hakeren, 10 Hata'as Street, Ramat Gan 52512, Israel
info@israellawcenter.org • www.israellawcenter.org
Israel • Tel: 972-3-7514175 • Fax: 972-3-7514174
USA • Tel: 646-661-2811

וי אלול תשע"ז
August 28, 2017

Mr. Matthew Prince, CEO
Cloudflare, Inc.
101 Townsend Street
San Francisco, CA 94107
Fax: 650-230-7173
Email: matthew@cloudflare.com

**Re: Knowingly Providing Material Support or Resources to Terrorists
is a Violation of Federal Criminal Law**

Dear Mr. Prince,

I am an Israeli attorney and the president of the Shurat HaDin Law Center based in Tel Aviv. Our organization is dedicated to combatting the scourge of international terrorism through the court system in jurisdictions worldwide. We represent hundreds of families who have had loved ones killed and injured in grievous terrorist attacks. Specifically, we represent many victims of Palestinian terrorism, including those who have been injured in attacks perpetrated by the Hamas terrorist organization and the Palestine Islamic Jihad. Recently, our Law Center assisted in a federal court case brought by American families against the Palestinian Authority and the PLO, which resulted in a unanimous \$655 million jury verdict against these entities in a Manhattan court.

As such, Shurat HaDin writes to notify your company, Cloudflare, that its knowing provision of material support or resources to Hamas and other designated terrorist organizations is a violation of U.S. federal criminal law, and to demand that Cloudflare immediately terminate any and all accounts and services provided to these terrorist groups. The provision of such support could render your company both criminally and civilly liable under America's Anti-Terrorism law.

1. The issue of providing services to Hamas is not merely a matter of offensive speech

As an initial matter, it is important to distinguish between our demand regarding the terrorist group Hamas, and Cloudflare's recent decision to terminate the account of a customer roundly condemned for disseminating anti-semitic and racist hate-speech.

On Wednesday, August 16, 2017, as CEO of Cloudflare, you announced that Cloudflare had terminated the account of a neo-Nazi and white supremacist website known as *The Daily Stormer*, and had “taken measures to ensure that they cannot sign up for Cloudflare’s services ever again.”¹ According to *Gizmodo*’s Kate Conger, you explained this decision in an internal email to your staff as follows:

This was my decision. Our terms of service reserve the right for us to terminate users of our network at our sole discretion. My rationale for making this decision was simple: the people behind the Daily Stormer are [expletive deleted] and I’d had enough.

Let me be clear: this was an arbitrary decision. It was different than what I’d talked with our senior team about yesterday. I woke up this morning in a bad mood and decided to kick them off the Internet...It was a decision I could make because I’m the CEO of a major Internet infrastructure company.

Having made that decision we now need to talk about why it is so dangerous. I’ll be posting something on our blog later today. Literally, I woke up in a bad mood and decided someone shouldn’t be allowed on the Internet. No one should have that power.

...It’s important that what we did today not set a precedent. The right answer is for us to be consistently content neutral. But we need to have a conversation about who and how the content online is controlled.²

In her article, Ms. Conger elaborated on your call for a wider discussion about control of online content, quoting you as stating:

We need to have a discussion around this, with clear rules and clear frameworks. My whims and those of Jeff [Bezos] and Larry [Page] and Satya [Nadella] and Mark [Zuckerberg], that shouldn’t be what determines what should be online ... I think the people who run The Daily Stormer are abhorrent. But again I don’t think

¹ Matthew Prince, “Why We Terminated Daily Stormer,” *Cloudflare blog* (Aug. 16, 2017), <https://blog.cloudflare.com/why-we-terminated-daily-stormer/>.

² Kate Conger, “Cloudflare CEO on Terminating Service to Neo-Nazi Site: ‘The Daily Stormer Are A[-----],’” *Gizmodo* (Aug. 16, 2017), <http://gizmodo.com/cloudflare-ceo-on-terminating-service-to-neo-nazi-site-1797915295>.

my political decisions should determine who should and shouldn't be on the internet.³

As your statements above demonstrate, decisions about whether to provide services to customers who disseminate highly offensive but otherwise lawful content on the internet raise difficult questions for companies such as Cloudflare, including for example: 1) whether the decision to deny services is unfair because it is arbitrary, politically motivated, or otherwise improperly discriminatory; 2) whether the decision violates traditional principles of freedom of speech; and 3) in the case of major companies or where alternative providers are limited or unavailable, whether the decision represents an abuse of market power.

However, we are not writing to weigh in on these issues, because none of these issues pertain to providing services to Hamas or other designated terrorist entities. The reason is simple: legally, there is no decision for a U.S. company to make. Federal law prohibits the provision of any services to or for the benefit of Hamas or other designated terrorists.

2. Federal prohibitions against providing support to Hamas and other terrorists

A. Executive Order No. 12947

The United States has banned transactions with the terrorist organization Hamas, including providing or receiving any property or services, since 1995. Prompted by the escalation of horrific Palestinian terror attacks following the 1993 Oslo Accords, including many suicide bombing attacks carried out by Hamas, President Bill Clinton issued Executive Order No. 12947 (“EO 12974”) pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 *et seq.* (“IEEPA”), on January 23, 1995. EO 12947 legally blocked all property and interests in property of specially designated terrorists (“SDT”), including specifically Hamas,⁴ and prohibited “any transaction or dealing by United States persons ... in property or interests in property of an [SDT].” Title 31 C.F.R. § 595.204 specifies that this prohibition “includ[es] but [is] not limited to: (a) The ... provision of funds, goods, or services by, to, or for the benefit of a specially designated terrorist; and (b) The receipt of any ... funds, goods, or services from a specially designated terrorist.” Under the IEEPA, violation of EO 12947 is a federal criminal offense. *See* 50 U.S.C. § 1705.

³ *Id.*

⁴ The name “Hamas” is an acronym for the group’s full name in Arabic, *Harakat al-Muqawama al-Islamiyya* (the “Islamic Resistance Movement”).

As a U.S. company, Cloudflare is prohibited by EO 12947 and related federal regulations and statutes from providing services to Hamas or other SDTs, whether the services are provided for free or whether Cloudflare receives any payment for such services.

B. Executive Order No. 13224

In addition, following the 9/11 terror attacks, President George Bush issued Executive Order No. 13224 (“EO 13224”) pursuant to the IEEPA on September 23, 2001. EO 13224 legally blocked all property and interests in property of specially designated global terrorists (“SDGT”), and prohibited the provision of funds, goods, or services for the benefit of SDGTs. The U.S. Government designated Hamas and its constituent paramilitary organization, the *Izz al-Din al-Qassam Brigades* (the “*al-Qassam Brigades*”), as SDGTs pursuant to EO 13224 on October 31, 2001. *See* 67 Fed. Reg. 12633-12635 (2002). Many Hamas leaders and Hamas-controlled or affiliated entities are also designated SDGTs, so that transactions with, and provision of services to, those individuals and entities are also prohibited by EO 13224. Violation of EO 13224 is also a federal criminal offense. *See* 50 U.S.C. § 1705.

Thus, also under EO 13224 and related federal regulations and statutes, it is illegal for Cloudflare to engage in any transactions with Hamas or other SDGTs, including providing services or receiving payment for such services.

C. Federal “material support” statutes

Title 18 U.S.C. § 2339A imposes criminal penalties upon anyone who “provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out” terrorist activity. That statute broadly defines “material support or resources” to mean “any property, tangible or intangible, or service,” and specifically includes, among other things, “expert advice or assistance ... communications equipment, facilities, [and] personnel.” § 2339A(b)(1). The term “expert advice or assistance” is further defined as “advice or assistance derived from scientific, technical or other specialized knowledge.” § 2339A(b)(2).

Title 18 U.S.C. § 2339B makes it a crime to knowingly provide “material support or resources” to a designated foreign terrorist organization (“FTO”), without regard to how such support or resources will be used. To violate § 2339B, the defendant need only have knowledge that the beneficiary is a designated FTO, or that the beneficiary either has engaged or engages in terrorist activity or terrorism. § 2339B(a)(1). Hamas and its constituent paramilitary organization, the *Izz al-Din al-Qassam Brigades* (the “*al-Qassam Brigades*”), have been designated FTOs pursuant to Section 219 the Immigration and Nationality Act, 8 U.S.C. § 1189, since October 1997. *See* 62 Fed. Reg. 52650 (1997).

It is clear that the products and services that Cloudflare provides to its customers constitute “material support or resources” under the statutory definition applicable to § 2339A and § 2339B. Cloudflare’s website describes its products and services as enhancing a website’s performance, security, and reliability, while also providing insights, analytical tools, and technical support. Cloudflare also gives customers access to and use of its computer servers, and applications. All of these products and services are “derived from scientific, technical, or other specialized knowledge” and would constitute *expert advice or assistance*. Cloudflare’s physical infrastructure clearly serves as *communications equipment and facilities*, and Cloudflare provides *intangible property* to its customers in the form of a license to use Cloudflare’s products and services. Cloudflare also provides its customers with *personnel* who monitor, troubleshoot, and maintain the customers’ presence online, and who provide live technical support.

In its landmark decision in *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010), the U.S. Supreme Court upheld § 2339B in the face of claims that the statute was too vague under the Due Process Clause of the Fifth Amendment, and that it violated the petitioners’ rights to freedom of speech and association under the First Amendment of the Constitution. In the ruling, the Supreme Court specifically credited State Department testimony that: “[t]he experience and analysis of the U.S. government agencies charged with combatting terrorism strongly support[t]’ Congress’s finding that all contributions to foreign terrorist organizations further their terrorism.” *Id.* at 33 (quoting McKune affidavit).⁵ The Court explained the necessity of § 2339B as follows:

[P]laintiffs simply disagree with the considered judgment of Congress and the Executive that providing material support to a designated foreign terrorist organization—even seemingly benign support—bolsters the terrorist activities of that organization. That judgment, however, is entitled to significant weight, and we have persuasive evidence before us to sustain it. Given the sensitive interests in national security and foreign affairs at stake, the political branches have adequately substantiated their determination that, to serve the Government’s interest in preventing terrorism, it was necessary to prohibit providing material support in the form of training, expert advice, personnel, and services to foreign terrorist groups, even if the supporters meant to promote only the groups’ nonviolent ends.

Id. at 36.

⁵ The affidavit added: “Given the purposes, organizational structure, and clandestine nature of foreign terrorist organizations, it is highly likely that any material support to these organizations will ultimately inure to the benefit of their criminal, terrorist functions – regardless of whether such support was ostensibly intended to support non-violent, non-terrorist activities.” *Id.*

Returning to your official Cloudflare blog post of August 16, 2017, we note that you wrote:

Due Process requires that decisions be public and not arbitrary. It's why we've always said that our policy is to follow the guidance of the law in the jurisdictions in which we operate. Law enforcement, legislators, and courts have the political legitimacy and predictability to make decisions on what content should be restricted. Companies should not.⁶

As shown above, all three federal branches—Congress, the Executive, and the Judiciary at its highest level—have all decided that the provision of material support or resources to Hamas and other designated foreign terrorist organizations must be banned, and that this ban does not violate Due Process or the Constitutional right to freedom of speech. We call upon Cloudflare to “follow the guidance of the law” as you claim is your policy, and terminate all accounts and services to Hamas, its *al-Qassam Brigades*, and other designated terrorists as required by federal law.

3. Exposure to civil liability for providing support to Hamas and other terrorists

A. Liability under the Antiterrorism Act (“ATA”)

Pursuant to 18 U.S.C. § 2333, U.S. nationals injured by reason of an act of international terrorism are entitled to sue for their injuries and recover treble damages and costs, including attorney’s fees. Courts have recognized that Congress enacted § 2333 as a means of civil enforcement intended to punish and deter those who commit acts of international terrorism. Moreover, courts have held that providing material support or resources to terrorists in violation of § 2339A or § 2339B constitutes an act of international terrorism for which a defendant may be held liable under § 2333.

Last year, with the intent to expand the ability of civil plaintiffs to bring ATA claims under § 2333 against those who “knowingly or recklessly” provide material support or resources to terrorists, Congress enacted the Justice Against Sponsors of Terrorism Act (“JASTA”), Pub. L. No. 114-222 (2016). Among other things, JASTA established new federal causes of action for aiding and abetting and conspiracy liability under the ATA. *See* 18 U.S.C. § 2333(d).

Hamas and other designated terrorist organizations and their affiliates use their websites to promote their terrorist ideologies, recruit followers, raise funds, incite terrorist acts, disseminate their anti-Semitic views, glorify terrorists, and their deadly attacks, and much more. For example, a website of Hamas’s *al-Qassam Brigades* supported by Cloudflare maintains a gallery

⁶ “Why We Terminated Daily Stormer,” *supra* note 1.

of gruesome photographs of many suicide bombing attacks carried out by that group, as well as videos and biographies of the murderous attackers to inspire future terror attacks. We represent many innocent victims of these heinous attacks.

While some internet platforms have claimed immunity from civil liability in certain circumstances based upon the federal Communications Decency Act (“CDA”), Cloudflare does not purport to act as an internet “publisher” or platform provider. Rather, Cloudflare promotes its products and services primarily as enhancing performance, security, and reliability of websites (for example, through “reverse proxy” services, “firewalls,” encryption, and other such features). Therefore, it is not likely that Cloudflare would have a basis to assert CDA “immunity” as basis to avoid civil ATA liability.

B. Other civil enforcement penalties

In addition to criminal sanctions, a defendant who violates EO 12947 or EO 13224 or any of the regulations enacted pursuant to those orders can also be required to pay civil penalties for each violation or attempted violation. *See* 50 U.S.C. § 1705(b).

A recent enforcement action brought by the U.S. Treasury against Barracuda Networks, Inc. (“Barracuda”) is instructive.⁷ In November 2015, Barracuda agreed to pay civil penalties as part of a settlement with OFAC for alleged violations of sanctions against Iran, Syria and Sudan by distributing software, subscriptions, and updates to countries and Specially Designated Nationals (SDN) and Blocked Persons. In that case, OFAC contended that Barracuda had reason to know that it was violating the sanctions based on the information that could be derived from the IP addresses and sales invoices of the recipients, and that Barracuda failed to have an OFAC compliance program at the time of the transactions.

OFAC publishes comprehensive lists of individuals and entities, including SDNs, SDTs, SDGTs, and FTOs, against whom sanctions are imposed and with whom transactions are prohibited. Hamas, the *al-Qassam Brigades*, and many other individuals and entities affiliated with Hamas and other terrorist organizations are publicly listed by OFAC. There is simply no excuse for Cloudflare to provide any accounts or services to these individuals or groups in blatant violation of federal law.

⁷ *See* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151124_Barracuda.pdf. Although the civil enforcement action against Barracuda was based upon sanctions against Iran and other countries, the U.S. Treasury’s Office of Foreign Assets Control (“OFAC”) is also responsible for enforcing sanctions imposed upon SDTs and SDGTs. In addition to OFAC, the U.S. Department of Commerce’s Bureau of Industry and Security brought a separate civil enforcement against Barracuda, which resulted in a settlement payment by Barracuda of \$1.5 million.

4. Cloudflare's provision of support to Hamas and other designated terrorists

Cloudflare's provision of services to Hamas and other terrorists is well known. In 2012, Cloudflare posted a link to an article in the internet magazine *Wired*, which touted the fact that Cloudflare's clients include Hamas' *al-Qassam Brigades*.⁸ The article itself included a link to a blog report that described how Cloudflare's logo appeared upon initially opening the *al-Qassam Brigades*' website.⁹

In response to criticism of Cloudflare's reported provision of services to Hamas and other designated terrorists, *Reuters* quoted you as stating: "Both sides have an absolute right to tell their story.... We're not providing material support for anybody. We're not sending money, or helping people arm themselves.... We can't be sitting in a role where we decide what is good or what is bad based on our own personal biases.... That's a huge lipperry slope."¹⁰ The internet magazine *Mashable* likewise quoted you defending Cloudflare's provision of services in that instance as stating: "Our network can't be used to launch an attack, so it's not like we're supplying bullets to either side. But we are supplying the flak jackets to both sides..."¹¹

Of course, the argument that Cloudflare's provision of services to Hamas and other terrorists does not constitute "material support or resources" prohibited by federal law because it is not in the form of money, arms, offensive capabilities, or bullets, is completely refuted by the U.S. Supreme Court's decision in *Holder v. Humanitarian Law Project* discussed above. Indeed the Supreme Court understood that Congress intended to prohibit all forms of support to foreign terrorist organization, even support to charitable aims, because it frees resources for violence, and "[i]t also importantly helps lend legitimacy to foreign terrorist groups—legitimacy that makes it easier for those groups to persist, to recruit members, and to raise funds—all of which facilitate more terrorist attacks." 561 U.S. at 30.

Moreover, we agree that Cloudflare should not make its decisions about which customers it will serve based upon its "own personal biases," and our demand regarding Hamas does not require

⁸ See <https://www.cloudflare.com/press/2012/>; Robert McMillan and Spencer Ackerman, "Despite Ceasefire, Israel-Gaza War Continues Online," *Wired* (Nov. 28, 2012), <https://www.wired.com/2012/11/israel-gaza-ddos/>.

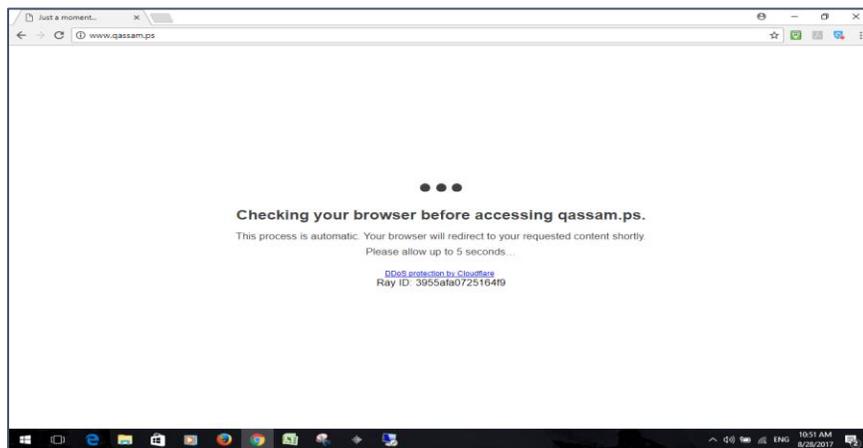
⁹ *Id.*; see <http://elderofziyon.blogspot.com/2012/11/how-hamas-website-avoids-denial-of.html>.

¹⁰ Gerry Shih, "Selling flak jackets in the cyberwars," *Reuters* (Dec. 13, 2012), <http://www.reuters.com/article/net-us-usa-cyberwar-cloudflare-idUSBRE8BC0OB20121213>.

¹¹ Alex Fitzpatrick, "Cyberattacks in Israel and Gaza Increased After Cease Fire Declared," *Mashable* (Dec. 5, 2012), <http://mashable.com/2012/12/05/cyberattacks-gaza-israel/#gAYU7CCI BOqP>.

you to do so. Instead, Cloudflare has a moral and legal obligation to comply with federal laws that prohibit engaging in any transactions or providing any services to designated terrorists.

Unfortunately, we have observed reports that Cloudflare continues to provide services to Hamas, the *al-Qassam Brigades*, the Palestinian Islamic Jihad's ("PIJ") *al-Quds Brigades*, the Popular Front for the Liberation of Palestine ("PFLP"), and the *al-Aqsa Martyrs Brigades*, all of whom are designated foreign terrorist organizations.¹² Indeed, our own review of the name server for websites of these entities via whois.net and similar information sites, as well as the appearance of Cloudflare's own "DDoS protection" notice upon opening these websites, confirms that Cloudflare continues to provide services to these entities. For example:



5. Conclusion

In light of the above, we demand that Cloudflare immediately terminate any and all accounts and services it provides to Hamas, the *al-Qassam Brigades*, and other designated terrorist entities and individuals. We urge Cloudflare to carefully review the comprehensive list of designated terrorists published by OFAC, and to ensure that Cloudflare complies with federal law in this regard.

We greatly admire your work and the company you have built and strongly advise you to steer clear of the provision of your services to designated terrorist organizations such as Hamas, the PIJ and the PLO. I am available to discuss this matter with you and/or your legal staff at your earliest convenience.

¹² See <http://elderofzion.blogspot.com/2017/05/how-can-cloudflare-continue-to-protect.html>.

We reserve the right to take immediate legal action and pursue all available remedies against Cloudflare without any further notice.

Yours Sincerely,



Nitsana Darshan-Leitner, Adv.

President

Shurat HaDin Law Center