

**WRITTEN TESTIMONY OF DR. DANIEL J. ROGERS**  
**BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES**  
**SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT,**  
**AND MONETARY POLICY ON**  
**“DOLLARS AGAINST DEMOCRACY: DOMESTIC TERRORIST FINANCING IN**  
**THE AFTERMATH OF INSURRECTION”**  
**ON THURSDAY, FEBRUARY 25, 2021**

Chairman Himes, Ranking Member Hill and members of the committee, good morning, and thank you for the opportunity to appear before you to discuss the funding mechanisms of domestic violent extremist groups. I am a Co-Founder and the Chief Technology Officer of the Global Disinformation Index, a transparent, independent, neutral nonprofit focused on catalyzing change in the technology industry to disrupt the incentives that exist to create and disseminate disinformation online. We partner with advertising and technology companies, governments, and advocacy groups to provide data to demonetize disinformation and hate. Our primary focus is on disrupting the monetization of disinformation through online advertising, but we also consider other ways in which disinformation is monetized, including payments, merchandising, and infrastructure such as web hosting or domain name registration.

Last Fall, my colleague Ben Decker and our team at the Global Disinformation Index collaborated with the Institute for Strategic Dialogue, a think tank based in the U.K., to conduct a study entitled “Bankrolling Bigotry” that examined the funding mechanisms of American hate groups. You may ask why a disinformation-focused nonprofit examined hate groups in America,

and what is the relevance to the events of January 6, 2021. We view disinformation through the lens of what we call adversarial narrative conflict. Whenever someone peddles an adversarial narrative that intentionally pits people against each other, or against trusted institutions, is intentionally misleading, and carries with it a risk of harm, that is the core of disinformation in our view. And no narrative is more adversarial than hate and bigotry. Furthermore, many of the groups implicated in the events of January 6<sup>th</sup> are the same groups we examined last year in our study. This is why I sit before you today: to discuss what we learned about how technology and payments companies inadvertently facilitate the fundraising that enables groups like those that participated in the insurrection on January 6<sup>th</sup> to operate.

Hate is on the rise. In 2018, the FBI announced that hate crimes had reached their highest volume in nearly two decades. In 2019, the Southern Poverty Law Center, representatives from whom sit alongside me today, calculated that the number of avowed white supremacist groups had doubled between 2017 and 2019. The COVID-19 pandemic, coupled with the death of George Floyd and the most divisive election cycle in recent history, has inspired many of these groups to mobilize both online and offline to threaten safety and security writ large.

It is no longer a surprise that these groups leverage the internet as a primary means of disseminating their toxic ideologies, soliciting funds, and selling merchandise. One only needs to search Amazon or Etsy for the term “Qanon” to uncover shirts, hats, mugs, books, and other paraphernalia that both monetize and further popularize the domestic violent extremist threat. Images from that fateful day last month are rife with sweatshirts that say “Camp Auschwitz” or “6 Million Was Not Enough” that until very recently were for sale on websites like TeeSpring

and CafePress. As we speak, at least 24 individuals indicted by the U.S. Department of Justice for their role in the January 6<sup>th</sup> insurrection, including eight members of the Proud Boys, have used the crowdfunding site GiveSendGo to raise nearly a quarter million dollars in donations.<sup>1</sup> And it's not just about the money. Yes, the merchandise sold through these platforms supplies funds to those who would peddle or exploit this ideology, but this merchandise also acts like a team jersey for the hate groups, bolstering the narrative itself and helping the groups recruit new members and foment further hatred toward their targets.

We set out to study the online funding mechanisms for these groups in a data-driven, systematic way. For the purposes of our study, we adopted the definition of hate group from the Southern Poverty Law Center (SPLC). The SPLC-defined hate groups include anti-immigrant, anti-LGTBQ, anti-Muslim, white nationalist, white supremacist, and militia groups, all of whom had some sort of online presence. All in all, we analyzed the digital footprints of 73 US-based groups across 60 websites and 225 social media assets and their use of 54 different online fundraising mechanisms, including 47 different payment platforms and 5 different cryptocurrencies, ultimately finding 191 instances of hate groups using online fundraising services to support their activities. The funding mechanisms used by these groups included both primary platforms that facilitate financial interactions between organizations and individuals directly on the platforms – Amazon, for example – and intermediary platforms such as Stripe or Shopify that build donation buttons or merchandise stores directly into a group's own website. We also included crowdfunding sites like GoFundMe, payments facilitators like PayPal, monetized content streaming services like YouTube Super Chats, and cryptocurrencies such as

---

<sup>1</sup> Brittain, Amy and Willman, David. “‘A place to fund hope’: How Proud Boys and other fringe groups found refuge on a Christian fundraising website,” Washington Post. 18 January 2021.

bitcoin in our analysis. All of these payment mechanisms were linked with either websites affiliated with each group or with associated social media accounts on Facebook, Telegram, YouTube, Instagram, LinkedIn, Pinterest, Gab, BitChute and Minds. The sheer number of technology providers I just mentioned is the first clue to the scale and scope of the problem – this is not the problem of any one individual company or platform, but rather a systemic problem of hate and bigotry exploiting an entire industry, and even government policy, to raise funds, peddle extremist ideologies, and ultimately, as Jan 6th demonstrated, commit acts of violence, even insurrection.

A number of interesting conclusions stood out to us in performing this work. For starters, over half – 62%, to be exact – of the platforms we identified already have explicit policies against hate and extremism on their platforms. The tools to intervene already exist, and this data point suggests either a lack of resources or a lack of will to adequately enforce existing terms of service against these groups. That is not to say there is zero enforcement. We found that the most extreme groups associated with the highest risk of violence – white nationalist and white supremacist groups – were the most likely to eschew more mainstream platforms in favor of pseudonymous cryptocurrencies, while militia groups tend to prioritize funds through the sale of merchandise rather than via direct donations. This suggests that the platforms have moderated at least the most violent groups toward more cumbersome, less centralized methods of exchanging funds. But given the sheer number of groups still making use of more mainstream monetization platforms, the industry has a long way to go.

But there are other hurdles to platform moderation whose origins are much closer to home in Washington, DC. A large fraction of the groups we studied – 44% to be specific – have been recognized as tax-exempt under sections 501(c)(3) or 501(c)(4) of the Internal Revenue Code.. A full 100% of anti-Muslim groups as identified by the SPLC have approved tax exempt status in the US, along with 75% of anti-Immigrant groups and 70% of anti-LGTBQ groups. Over one third of militia groups we identified in this study, including the Oath Keepers, multiple members of which were recently indicted by the Justice Department on conspiracy charges related to the January 6<sup>th</sup> insurrection,<sup>2</sup> have charity status. And this status gives these groups automatic access to a whole spectrum of charity fundraising tools, from Facebook Donations to Amazon Smile, to the point where the overall most common fundraising platform we identified across all of the data was actually Charity Navigator’s “Giving Basket” function. These platforms are reticent, to say the least, to make unilateral decisions about which IRS-approved charities to host and which ones to moderate.

This problem is not new. Marcus Owens, who ran the Exempt Organizations Division at IRS from 1990 until 2000, testified to the House Committee on Ways and Means in 2019 about the problem of the tax code subsidizing hate. He pointed to a specific example involving avowed white supremacist Richard Spencer, who founded his National Policy Institute “think tank” using an EIN of a dormant organization, The Institute for Free Enterprise Development, which hadn’t filed a Form 990 with the IRS since 1997. When Spencer resurrected the EIN and subsequently filed a Form 990 in 2005, it was for an organization with a new name and new officers and

---

<sup>2</sup> Savage, Charlie, Goldman, Adam, and MacFarquhar, Neil, ““This Kettle Is Set to Boil”: New Evidence Points to Riot Conspiracy.” The New York Times. 19 January 2021.

directors.<sup>3</sup> This sounds like fraud, but in fact it comports with existing law and allows legitimate organizations to adapt to changing circumstances, but also allows groups like Spencer's to evade even the most basic scrutiny of their activities by the IRS. It is a problem that goes back decades and stems from a combination of the lack of resources at the IRS to properly enforce compliance by exempt organizations as well as a long standing effort by some to exploit the charity rules for political, and now extremist, purposes.

The events of January 6<sup>th</sup> have brought this issue into stark relief. In the days leading up to the insurrection, the Oath Keepers' founder, Stewart Rhodes, appeared on a podcast hosted by notorious anti-vaccine conspiracy theorist Mike Adams and solicited charitable donations to the Oath Keepers Educational Foundation.<sup>4</sup> One can speculate that funds that listeners contributed, which they were notably able to deduct from their federal taxes, went to transporting and lodging members of the group slated to participate in the ensuing riots.

Fortunately, according to the experts we've consulted, this is one area that Congress and IRS can address unencumbered: In fact, IRS could quickly and unilaterally remove the Oath Keepers section 501(c)(3) status using the jeopardy assessment process to bypass the normal internal IRS administrative appeal process thus preventing further charitable fundraising<sup>5</sup>, given that nine members of their leadership have now been indicted.

---

<sup>3</sup> How the Tax Code Subsidizes Hate: Hearing Before the House Committee on Ways and Means, Subcommittee on Oversight. 116<sup>th</sup> Congress. 8 (2019) (testimony of Marcus S. Owens)

<sup>4</sup> <https://www.brighteon.com/fa01234a-d2ca-4b22-ab39-10d1d466bcab> at minute 42 of the video.

<sup>5</sup> Section 6861 of the Internal Revenue Code and Section 4.4.17 of the Internal Revenue Manual

But to date the IRS has not done so, according to our experts, largely because they lack the resources and training to properly enforce the regulations governing exempt organizations. The enforcement gap is the result of larger misaligned priorities within the design of the IRS as a whole. The IRS is, at its core, a revenue collecting agency, yet the Exempt Organizations Division, which is in charge of regulating the very organizations we're discussing today, by design generates no significant revenue. Thus, it is last in line for resources, making it an easy target for exploitation. One fix would be to remove that function from the IRS and create a new, separate, and well-resourced governmental organization outside of the IRS with the mission of regulating tax-exempt organizations, much like the independent Charity Commission does in the United Kingdom.

In the meantime, private industry must step up and do more. They have taken some action, but they can go further. Since the publication of our report in October 2020, we've documented at least seventeen private-sector actions taken by platforms against the groups we enumerated. For example, after our publication, four of the six payment mechanisms routing funds to the Oath Keepers were blocked. Subsequently, Amazon has even removed the Oath Keepers from Amazon Smile. But seventeen actions out of the nearly 200 instances we observed speak to the breadth of the problem and the rampant way it has been allowed to persist. As I mentioned, over half of these platforms already have policies in place that would prohibit such activity but fail to enforce them. And those policies are not harmonized with each other – what is prohibited on one platform could be perfectly allowable on another. In fact, while most platforms have removed the Oath Keepers, payment facilitator RallyPay still to this day services the group's fundraising needs and has shown no sign of responding to public pressure to stop.<sup>6</sup>

---

<sup>6</sup> <https://twitter.com/socialistdogmom/status/1362096551120748549>

More must be done. Industry-wide standards must be set, and enforcement across both the public and private sectors must be stepped up if we are to stem the growth of Domestic Violent Extremism. Chairman Himes, Ranking Member Hill and members of the committee, thank you again for your time this morning, I welcome your questions, and I look forward to discussing these issues in more detail with you all.