UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, *Plaintiff*, v. ROMAN STORM, *Defendant.*	23-cr-430 (KPF) Hon. Katherine Polk Failla

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF ROMAN STORM'S MOTION FOR RECONSIDERATION

Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: mitch@eff.org

Dated: January 28, 2025

=

CORPORATE DISCLOSURE STATEMENT OF PROPOSED AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION

Proposed amicus curiae Electronic Frontier Foundation, by its attorneys and pursuant to Rule 7.1 of the Federal Rules of Civil Procedure, hereby states that it is a corporation organized under Section 501(c)(3) of the Internal Revenue Code. Electronic Frontier Foundation does not have a parent corporation, and no publicly held company has a 10 percent or greater ownership interest in it.

DATED: January 28, 2025

/s/ Mitchell L. Stoltz
Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
Email: mitch@eff.org

Counsel for Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization that has worked for nearly 35 years to protect innovation, free expression, and civil liberties in the digital world. EFF advocates for internet users and those who build the digital tools that advance users' privacy and free expression. That is why EFF has called for the careful application of criminal laws to new technologies and those who build them. For example, EFF has served as counsel or amicus in nearly every case addressing the interpretation of laws proscribing computer hacking, like the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and similar state laws. *See Van Buren v. United States*, 593 U.S. 374 (2021) (amicus); *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019); *Oracle USA, Inc. v. Rimini St., Inc*, 879 F.3d 948 (9th Cir. 2018); *United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024 (9th Cir. 2016); *Facebook, Inc. v. Power Ventures*, 844 F.3d 1058 (9th Cir. 2016) (amicus); *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015) (amicus); *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (appellate co-counsel); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (amicus); *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus); *Craigslist, Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (amicus); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus). EFF also participated as amicus in the challenge to the government's designation of Tornado Cash to the Specially Designated Nationals and Blocked Persons List. *Van Loon v. Dep't of Treasury*, 688 F.Supp.3d 454 (W.D. Tex. 2023). And as part of its Coders' Rights Project, EFF offers pro bono legal services to researchers engaged in cutting-edge exploration of technology whose work in the public interest may be unjustly chilled by criminal laws.

[1] Counsel for amicus curiae certify that no counsel for a party authored this brief in whole or in part, and no person other than amicus curiae made any monetary contribution to its preparation or submission.

INTRODUCTION

The Fifth Circuit's recent decision in *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024), rightly notes that the International Economic Emergency Powers Act (IEEPA) simply cannot reach the Tornado Cash software because the software itself, currently running as an immutable tool on the blockchain, is not properly characterized as property or as a service under the statute. We agree with Mr. Storm that the analysis in that case supports dismissal of his indictment.

At minimum, however, *Van Loon* underscores the due process and rule of lenity concerns in this case. The Fifth Circuit held that by attempting to extend the reach of IEEPA to the Tornado Cash immutable software, the government stretched the statutory language past the breaking point. Even if the court disagrees, the prosecution here has certainly created ambiguity and chilling uncertainty for a wide range of people who create and support privacy-protective tools, including those who contribute to building open-source tools and security researchers who study those technologies. These concerns are heightened by the Government's Opposition brief (Dkt. No. 120) ("Government Op."), which argues that even if *Van Loon* is correct about the Tornado Cash tool itself, criminal liability can still attach based on the development and use of ancillary tools that simply aid the same functionality.

As a public interest organization with a deep understanding of open-source software development, EFF knows that the community that develops and supports freely distributable privacy, anonymity and security-protective tools for a wide variety of users is watching this and similar cases closely.[2] Those developers are concerned that the government's aggressive

[2] *See* EFF amicus brief, *Van Loon v. Dep't of Treasury*, Case No. 1:23-cv-00312 (W.D. Tex. April 27, 2023) (Dkt. No. 70-1) https://www.eff.org/files/2023/05/10/070-1_eff_amicus_brief99_3.pdf;

arguments here could implicate their own work on tools both inside and far outside the cryptocurrency industry. That is because nearly all privacy and anonymity protective software tools are dual-use tools. Like a physical mask or paper cash, they provide needed, often critical protections for users, but can also be used by bad actors to help hide their crimes.

The community developing security, privacy and anonymity tools needs and deserves bright, unambiguous lines about when their actions can be the basis for prosecution. This is especially true for the open-source developer community that EFF has long supported, which includes many people who develop dual-use tools but who don't have corporate backing or counsel.[3] Of course, this is the very reason that the rule of lenity exists: to give people clarity about when their actions could subject them to criminal prosecution. We urge the court to take these considerations into account as part of its reconsideration of the Motion to Dismiss.

ARGUMENT

I. *Van Loon* forecloses the government's effort to stretch IEEPA to create liability.

We agree with Mr. Storm that, given the limits that *Van Loon* imposed on the reach of IEEPA, the case supports dismissal of the indictment. EFF writes separately to underscore how the government's arguments push even further beyond the statutory limits imposed by *Van Loon* and how those arguments threaten an even wider range of software developers.

The government argues that, even if *Van Loon* means that the Tornado Cash tool itself is not subject to IEEPA, it can still prosecute Mr. Storm based on interpreting the statute to reach

---

Kurt Opsahl, *Code, Speech, and the Tornado Cash Mixer*, EFF Deeplinks (Aug. 22, 2022) https://www.eff.org/deeplinks/2022/08/code-speech-and-tornado-cash-mixer.

[3] "Security and encryption researchers help build a safer future for all of us using digital technologies, but too many legitimate researchers face serious legal challenges that prevent or inhibit their work." *Coders' Rights Project*, EFF, https://www.eff.org/issues/coders.

designing and operating ancillary technologies that provide "enhanced anonymity for" Tornado Cash users and earning a fee from the use of those ancillary technologies. Government Op. at 9.

Specifically, the government seeks to base criminal liability not on the actual alleged Tornado Cash mechanism of cryptocurrency mixing — which it says it does not need to rely on after *Van Loon* — but instead on the broader range of technologies it calls the "Tornado Cash service." These include two general categories: first, the creation of a website, user interface and what it calls "back office plumbing." Government Op. at 4-5. Second, it includes the receipt of payment based on "tokens" for use of the relays. *Id.* The result of this attempt to save the prosecution in the wake of the *Van Loon* decision is that the prosecution now threatens an even wider array of developers and programmers further removed from the creators of the core Tornado Cash software.

The Court should not let the novel and technical nature of the tools here blind it to the implications of the government's arguments. It should clearly reject the implication that any tool that allows (or supports) people having "enhanced anonymity" is inherently suspect. These arguments are akin to placing criminal liability on a shop because it had window blinds or a protected entryway that shields people engaging in both legal and illegal transactions.

Without proof of actual willfulness like criminal intent or a shared criminal purpose — neither of which appears on this record — creating a website, user interface or back-office software for a dual-use tool should not be a basis for liability. At bottom, the government's theory for these suggests that liability is triggered not because of the money laundering, but instead because of the specific work that Tornado Cash did to make it easier for non-technical people to use the dual-purpose core tool. The implication is that if Tornado Cash required users to open their computer's command line and be familiar with how to execute transactions, rather than using a web browser,

the law would not have been violated. Yet criminal liability should not rise or fall based on whether a dual-use toolmaker shipped its product with a user manual in the hopes of making it easier to use. Digital privacy protections that safeguard lawful and important activity would be quite limited if only those with deep technical knowledge could use them.[4]

The government's second argument, that liability is also created because Tornado Cash received fees from relayers that processed transactions, strains basic principles of criminal culpability. What the government describes as some nefarious scheme by which Mr. Storm received kickbacks based on illegal transactions is nothing more than the decentralized cryptocurrency program working as it was intended. The "gas" fee that the relayers paid is the built-in cost required to make a transaction on the Etherium blockchain.[5] The argument is akin to claiming that Visa or MasterCard would be criminally liable based solely on receiving transaction fees whenever its customers transferred money as part of some underlying criminal activity.

More generally, the government's theories attempting to bootstrap the defendant's role in setting up the specific function of relays and tokens used by the users of Tornado Cash show just how much they are using the digital nature of the system to expand their prosecutorial reach. In the offline world, this argument would be akin to the government claiming that it could prosecute FedEx for illegal drugs sent through FedEx from a corner store because FedEx set up and

[4] Internet users' need for robust anonymization and privacy tools is particularly acute given the growth of vast amounts of personal data held by both government agencies and private entities. *See* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, in Proc. of the 2008 Ieee Symp. on Security and Privacy (demonstrating how to de-anonymize movie ratings in Netflix data), https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; Paul Ohm, *Broken Promise of Privacy: Responding to the surprising failure of anonymization*, 57 UCLA L. Rev. 1701, 1720 (2010), https://www.uclalawreview.org/pdf/57-6-3.pdf.

[5] *See* The Investopedia Team, *Gas (Etherium): How Gas Fees Work on the Etherium Blockchain*, Investopedia, https://www.investopedia.com/terms/g/gas-ethereum.asp.

"supports" a process for local pack and ship corner stores to let their customers ship via FedEx, with payment remitted to FedEx.

The ancillary tools for ease of use and payment that are now the basis of the prosecution's arguments are all features of a dual-use tool that can provide much-needed security and privacy for ordinary users. That use should not be cast aside because those same protections can also make it more difficult for the government to investigate crime. We urge this court to apply *Van Loon* directly to dismiss this case.

II. Due process and the rule of lenity counsel in favor of dismissing the indictment.

In the alternative, EFF asks this Court to apply due process and the rule of lenity to dismiss the indictment and prevent the government from relying on the creation and general support for ancillary, dual-use tools as a basis for liability. The government's arguments here, if adopted, would potentially subject software developers, especially those engaged in development of tools that can be used to provide anonymity, to uncertain legal footing with severe criminal consequences.

There is no question that the statutes at issue here were written long before the emergence of privacy and anonymity-protective tools for cryptocurrency transactions. As a result, the court must tread carefully to be sure that the statutory language and framework can be extended to these facts. The rule of lenity calls for ambiguous criminal statutes to be interpreted narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008). The rule "ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). *See also U.S. v. Plaza Health Laboratories, Inc.,* 3 F.3d 643 (2d Cir. 1993) ("in criminal prosecutions the rule of lenity requires that ambiguities in the statute be resolved in the defendant's favor.").

We do understand that the central feature of Tornado Cash that the Fifth Circuit recognized — the immutable nature of the software once launched — is worrisome to the government. Yet it is no answer for the government to stretch the reach of existing criminal laws beyond their breaking point to include ancillary tools even when the core functionality is not available as a basis for liability. And this is especially true when those stretches leave software developers inside and outside the cryptocurrency industry uncertain about when they can be subject to serious criminal penalties.

If Congress wishes to pass a law that is intended to reach a tool like Tornado Cash, it can do so. The legislative process allows the opportunity to carefully and clearly differentiate illegal from legal behavior, and to give developers and users clear notice when they step over that line. The prosecution's arguments in this case do neither.

Here, the statutes are ambiguous as applied to Storm because, as explained in the previous section, the government's theory of liability results in many of those who endeavor to make privacy tools broadly available to the public risking direct and secondary criminal liability. Put another way, the government's theory turns basic features of technology, such as the websites, user interfaces and fees paid to conduct transactions on a blockchain, into criminal acts. Under such an expansive reading of both IEEPA's text and criminal liability more broadly, software developers would be at the mercy of the government's vast and potentially unbounded discretion. Yet that is precisely what the Constitution prevents by requiring courts to narrowly construe vague statutes. EFF submits that the government's prosecution chills First Amendment activity by discouraging the development of privacy protective software, and thus the due process concerns are heightened by this prosecution. *See U.S. v. Stevens*, 559 U.S. 460, 480 (2010). But "[e]ven when speech is not at issue, the void for vagueness doctrine addresses at least two connected but discrete due process

concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way." *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). Those twin due process concerns are present here, for all the reasons discussed above, and require this Court to dismiss the indictment.

CONCLUSION

We urge this court to apply *Van Loon* directly to dismiss this case, or in the alternative, to apply due process and the rule of lenity principles to prevent the government from relying on the creation and general support for ancillary, dual-use tools as a basis for liability. The government's arguments here, if adopted, would potentially subject software developers, especially those engaged in development of tools that can be used to provide anonymity, to uncertain legal footing with severe criminal consequences.

Dated: January 28, 2025

Respectfully submitted,

/s/ Mitchell L. Stoltz
Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Fax: 415-436-9993
mitch@eff.org

Counsel for amicus curiae Electronic Frontier Foundation