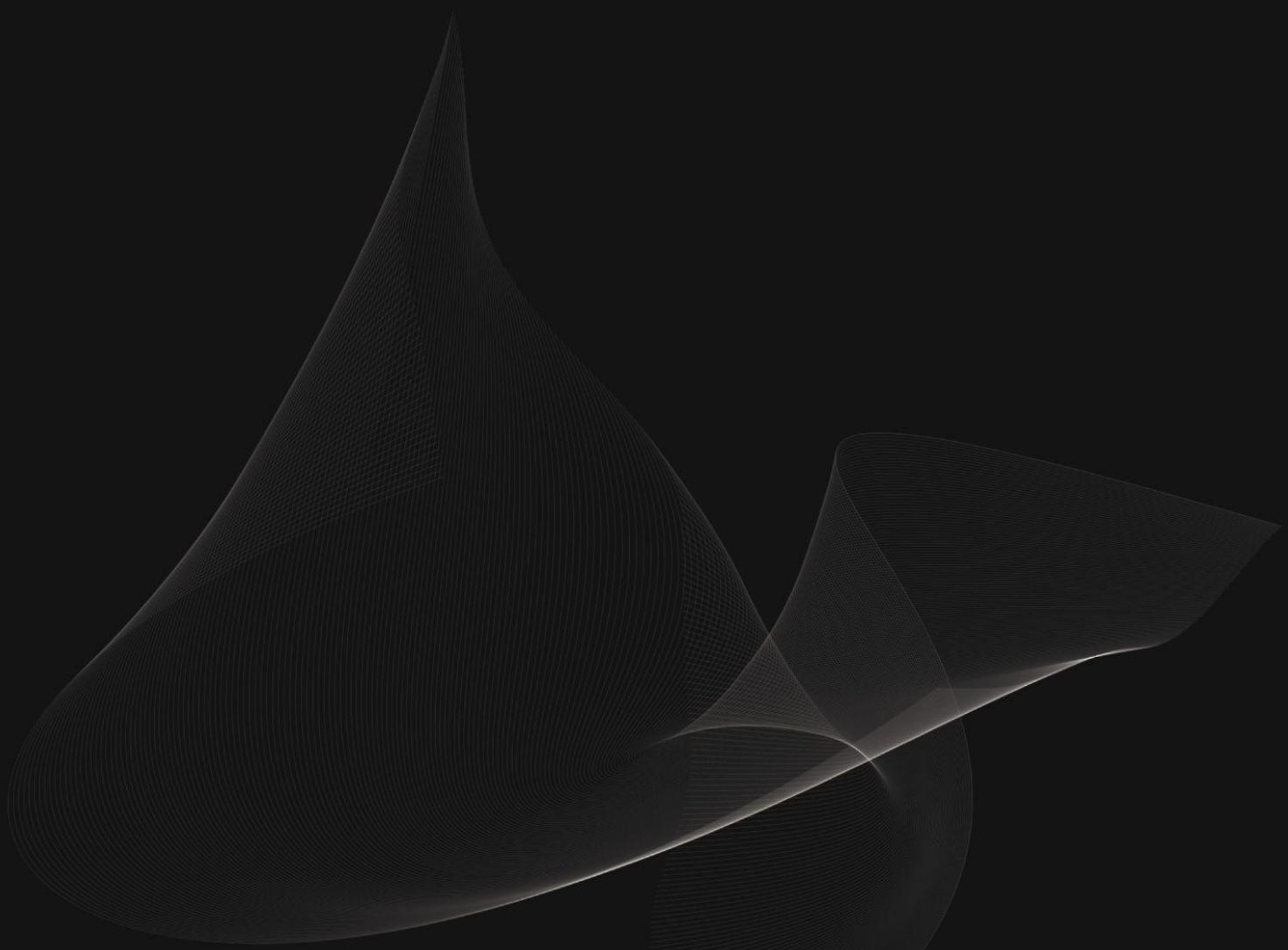

OFAC Cannot Shut Down Open-Source Software

October 18, 2022

—

Steve Engel
Brian Kulp
Dechert LLP

Overview

OFAC's decision to sanction Tornado Cash—thereby blocking U.S. persons from using the application and, in some cases, trapping their property—raises serious legal questions about OFAC's power over open-source software. While OFAC undoubtedly has the authority to sanction bad foreign persons and entities, Tornado Cash does not appear to be either a person or an entity. Rather, it is an open-source protocol built to protect financial privacy. In other words, Tornado Cash does not appear to be owned by anyone, foreign actor or otherwise.

Because cyber criminals and other illicit actors, like everyone else, can use virtual mixers like Tornado Cash to protect their financial privacy, OFAC very understandably has concerns about its misuse. Indeed, evidence suggests that proceeds from state-sponsored cyberattacks were being laundered through Tornado Cash.[1] Yet the most commonly used blockchains today have far greater transparency than the legacy financial system. OFAC's identification of a technological pathway that provides its users with a modicum of privacy does not mean that OFAC necessarily has the power to shut it down.

The truth is that, if Tornado Cash is just open-source software, then OFAC lacks power to sanction it. Federal law allows OFAC to sanction foreign persons and entities who engage in cybercrimes, which may include blocking wallets or blockchain addresses controlled by those persons, just like any other property. But no one gave OFAC the power to skip that first step and shut down infrastructure outside of any actor's ownership or control.

The stakes here go well beyond Tornado Cash or virtual currency mixers. Certainly, regulators may have legitimate concerns when it comes to pathways for laundering illicit assets—regardless of whether they run through the legacy financial system or the most commonly used blockchains. But the real question is whether OFAC can target these pathways themselves, rather than the actors using them. Because what can be done to one kind of open-source software can be done to any open-source software, if OFAC determines that it has been used for nefarious purposes.

This is not just a question of OFAC's statutory powers, but of the Constitution as well. OFAC's efforts to target Tornado Cash raise serious constitutional questions in three respects. First, because innocent Americans who deposited cryptocurrency into Tornado Cash are now prohibited from withdrawing their assets (absent OFAC's permission), they may have been deprived of their property without due process of law. Second, the asset freeze may have also violated those same individuals' Fourth Amendment rights to not have their property unreasonably seized. And third, OFAC's effort to prevent U.S. persons from using open-source software raises First Amendment questions. OFAC has since publicly stated that U.S. persons may review, study, and copy the open-source code, so long as they do

[1] *See U.S. Treasury Sanctions Widely Used Crypto Mixer Tornado Cash*, TRM Labs (Aug. 8, 2022), https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash.

not engage in a "prohibited transaction" with Tornado Cash.[2] Such guidance is hardly clear, and it borders on the tautological—any interaction that is not a "prohibited transaction" is "not prohibited."

We think that OFAC has overstepped, and that it should fix that mistake sooner rather than later. The first Tornado Cash lawsuits have already been filed against OFAC, and they will probably not be the last. We believe OFAC can and should focus its sanctions efforts on the bad actors who abuse blockchain technology, not on the neutral software tools themselves. And if there are gaps in the law that warrant additional regulation, OFAC should look to Congress for action. But what OFAC cannot do is what it did here: direct its sanctions power against open-source architecture.

The Tornado Cash Privacy Protocol

The global transparency underlying the most commonly used blockchains, is in many cases, a crucial security feature. But it comes at the cost of financial privacy. If someone knows the identity of the sender or recipient in just a single transaction, that person can easily link the public key associated with the wallet to the owner. The third party can then use that link to gain access to the owner's entire transaction history. This is untenable for everyday use.

Enter Tornado Cash. Developed in 2019, Tornado Cash is a virtual currency mixer built on Ethereum. It is a fully open-source, decentralized privacy protocol that consists of self-executing code—otherwise known as smart contracts. In Tornado Cash's case, the smart contracts by and large are immutable. So the autonomous code cannot be altered, edited, or controlled.

Briefly, here's how the Tornado Cash application works: users deposit specified amounts of ETH (or other supported tokens) and in exchange receive a randomized key, which they must use later to withdraw their assets. After a user makes a deposit, her crypto assets are pooled with the deposited assets of other users. Then, Tornado Cash uses an algorithm known as a zero-knowledge proof, which protects and keeps private transaction information.[3] At no point does Tornado Cash take control of users' tokens, and all deposits and withdrawals are recorded and fully visible on the blockchain. But when one withdraws their funds from the Tornado Cash pool into another wallet using the randomized key, the on-chain link between the source and the destination is broken, thereby anonymizing the transaction. As a result, a user can access her funds without exposing her entire financial history to third parties.

It bears repeating that there is nothing inherently illegal or improper about Tornado Cash. The tool can be and is used by those who want to maintain their financial privacy for legitimate reasons. For example, an employee paid in cryptocurrency needs to provide her wallet address to her employer, who in the absence of a privacy-preserving protocol could then search and view each and every transaction

[2] *See Frequently Asked Questions 1076*, U.S. Dep't of the Treasury (Sep. 13, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1076.

[3] *See* Alex Wade et al., *How does Tornado Cash work?*, Coin Center (Aug. 25, 2022), https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ (detailing the zero-knowledge proof algorithm and other technical features of Tornado Cash).

she makes with her wallet. By leveraging Tornado Cash, however, the employee can keep private her future transactions from the prying eyes of her employer or anyone else.

Anyone who has shared her wallet address to buy or sell something using cryptocurrency has exposed her financial history—past, present, and future—to the party on the other side of the deal. Imagine if every time you ran your credit card at a store, the merchant could view everything you ever bought with that credit card, and also everything you bought in perpetuity following that one transaction. For the same reasons why people reasonably want and expect privacy when it comes to their traditional financial arrangements, crypto users may want to periodically sever their on-chain links to shield private transactions from their counterparties.

It goes without saying that, just as legitimate users may want privacy on the blockchain, criminals may want it even more. Most conspicuously, the North Korean state-sponsored organization Lazarus Group appears to have leveraged Tornado Cash to launder nearly half a billion dollars' worth of stolen cryptocurrency, with other criminal organizations following suit.

It is not surprising then that such illegal activities would place Tornado Cash squarely within the federal government's investigative crosshairs. And that appears to be why OFAC decided to sanction "Tornado Cash" on August 8, 2022, invoking the President's authority under the International Emergency Economic Powers Act (IEEPA).[4] Specifically, the Treasury Department added the website "tornado.cash," 37 Tornado Cash smart contracts, and the address for a wallet used to accept donations for supporting the Tornado Cash project to the Specially Designated Nationals and Blocked Persons (SDN) list.[5] The designations mean that "all property and interests in property of the entit[ies]" just described are "blocked and must be reported to OFAC." Press Release, *supra* note 4. In addition, "[a]ll transactions by U.S. persons" or those "within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt." *Id.*; *see* 31 C.F.R. § 578.201. Effectively, OFAC's action blocks U.S. citizens from using Tornado Cash, including citizens whose digital assets are presently deposited with the protocol. *See* Press Release, *supra* note 4; *Frequently Asked Questions 1076*, *supra* note 2. Those who violate the agency's sanctions order face significant monetary penalties and, for willful violations, up to 20 years in prison. *See* 50 U.S.C. § 1705(b)–(c).

OFAC's action is unprecedented. Never before has the agency added open-source software (which, again, is all that the smart contracts are) to the SDN list. It has deployed the executive's IEEPA powers to sanction individuals like Russian senior officials, cyber criminals, and state entities like the Iranian Ministry of Intelligence. It has also gone after another virtual currency mixer in the past—sanctioning Blendor.io in May 2022. But the difference there was that Blendor.io was a centralized and custodial mixer, run and controlled by foreign persons, who could therefore be subject to sanctions. By contrast, Tornado Cash appears to be simply privacy-enabling software—neither a person nor an entity, nor

[4] *See* Press Release, U.S. Dep't of the Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[5] *See* Wade et al., *supra* note 3 (describing the sanctioned smart contracts).

anybody's property. That distinction, if true, would be fatal to OFAC's claimed authority to sanction the Tornado Cash addresses.

There is a group of real persons, "relayers," who "provide an optional service for Tornado Cash users." Wade et al., *supra* note 3 (emphasis omitted). Relayers "allow users to process withdrawals without needing to pre-fund their withdrawal accounts" in order to pay requisite transaction fees. *Id.*[6] This arrangement provides Tornado Cash users with an additional layer of privacy, and, for those users who opt in, it is possible that they could be described as engaging in transactions with the relayers. But OFAC's sanctions do not appear to target the Tornado Cash relayers; they target the Tornado Cash smart contracts, and the relayers do not have control over the smart contracts that OFAC has sanctioned. So even if particular relayers might qualify as foreign persons who could be sanctioned—meaning their property could be blocked—their participation would not seem to provide any justification for targeting the smart contracts themselves.

OFAC Lacked Statutory Authority to Sanction the Tornado Cash Smart Contracts

OFAC sanctioned Tornado Cash based upon authority delegated to Treasury by the President under IEEPA. IEEPA is a federal law that gives the President the authority, upon the declaration of a "national emergency," to "block during the pendency of an investigation . . . any property in which any foreign country or a national thereof has any interest," if that property is "subject to the jurisdiction of the United States." 50 U.S.C. §§ 1701(b), 1702(a)(1)(B). The President commonly exercises this power by declaring a national emergency on a particular subject, identifying the types of foreign persons who should be sanctioned, and then delegating authority to the Secretary of the Treasury, who through OFAC investigates and identifies the particular persons and property to be blocked.

In 2015, former President Barack Obama declared a national emergency to deal with the threat of "malicious cyber-enabled activities" from foreign states and hackers. Exec. Order No. 13694, 80 Fed. Reg. 18,077 (Apr. 1, 2015). President Obama directed the Secretary of the Treasury to identify "person[s]" responsible for or complicit in such cyberattacks. *Id.* And he ordered that the "property and interests in property" of those persons that make their way under the United States' jurisdiction would be "blocked." *Id.* That is, the property could "not be transferred, paid, exported, withdrawn, or otherwise dealt in." *Id.* Executive Order 13694 delegated the President's sanctioning authority to the Secretary of the Treasury, *id.* at 18079, who in turn delegated those powers to the Director of OFAC, *see* 31 C.F.R. § 578.802.

OFAC invoked this authority under Executive Order 13694 to "sanction[] virtual currency mixer Tornado Cash," alleging that the privacy protocol had been "commonly used by illicit actors to launder funds, especially those stolen during significant heists." Press Release, *supra* note 4. OFAC's concerns in this respect are undoubtedly legitimate. But in issuing broad, indiscriminate sanctions against the

[6] *See also Gas and Fees*, Ethereum (Sep. 27, 2022), https://ethereum.org/en/developers/docs/gas/#why-do-gas-fees-exist (explaining the concept of gas fees).

open-source software writ large, the agency overstepped its legal authority to sanction the foreign hackers and their property.

The fundamental flaw in OFAC's action is that Tornado Cash—and by that, we mean the set of designated smart contracts that comprise the core Tornado Cash application—was not itself sanctionable. Recall that the open-source software constitutes an automated privacy protocol. Unlike other currency mixers, it is not run by or under the control of natural persons. And that's important. For again, unless Tornado Cash is the "property" of some person—some foreign national or entity—it cannot be blocked under IEEPA.

Take first the issue of whether Tornado Cash could be considered a sanctionable "person," which the Treasury Department's regulations define as an "individual" or "partnership, association, trust, joint venture, corporation, group, subgroup, or other organization." 31 C.F.R. §§ 578.303, 578.308. The smart contracts are self-evidently not encompassed by any of those terms. They are just lines of code that autonomously execute on the distributed Ethereum blockchain. So OFAC is off to a bad start.[7]

The key question, then, is whether the Tornado Cash smart contracts are the "property" of a foreign national. On this front, OFAC fares no better. "It is a 'fundamental canon of statutory construction' that, 'unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.'" *Sandifer v. U.S. Steel Corp.*, 571 U.S. 220, 227 (2014) (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)). The word "property" is well understood to mean "something owned or possessed" or "something to which a person or business has a legal title." Property, *Merriam-Webster's Dictionary* (online ed.);[8] *see also* Property, *The Wolters Kluwer Bouvier Law Dictionary Desk Edition* (2012) ("What may be owned and the relationship of owning and using it."). Property interests, moreover, do not spring naturally from the air (or the ether, as it were). They consist of enforceable rights which are created by the legal systems that govern us. *See Bd. of Regents v. Roth*, 408 U.S. 564, 577 (1972). Or, put differently, "property" is that "species of right or interest protected by law" that has an "exchangeable value." *Drye v. United States*, 528 U.S. 49, 56 (1999) (quoting *Jewett v. Commissioner*, 455 U.S. 305, 309 (1982)).[9]

The Tornado Cash smart contracts don't fit that ordinary conception of "property," no matter how broadly you define it. As non-proprietary, fully open-source software, the code isn't owned or possessed by anybody. Nor does anybody have legal title to it. Indeed, to our knowledge, even the original developers lack the ability to edit, maintain, or otherwise control the smart contracts that are presently

[7] We do not rule out here the possibility that there could be some entity called "Tornado Cash" that is controlled by one or more foreign persons. And the OFAC-sanctioned website and wallet that accepted donations might be considered either pseudonyms for or the property of those persons. But while it is possible that such an entity could be a proper target of sanctions, that entity must be distinguished from the Tornado Cash smart contracts—*i.e.*, the code itself. That code does not appear to be either a person or the property of any entity. And that's why OFAC's sanctions are so strange. Perhaps OFAC failed to recognize this distinction between the ostensible Tornado Cash entity and the autonomous code. Perhaps not. Either way, the agency has overstepped its IEEPA authority insofar as it sanctioned the code.

[8] *See* https://www.merriam-webster.com/dictionary/property (last visited Oct. 5, 2022).

[9] The Treasury Department's own definition, which consists of a non-exclusive list of items that are considered "property" or "property interest[s]," tracks that commonsense understanding. The regulation lists dozens of legally protected interests that have an exchangeable value. *See* 31 C.F.R. § 578.309. None of them is like the open-source software at issue, which, as explained above the line, doesn't look to be owned by anyone.

used to facilitate Tornado Cash transactions. *See* Wade et al., *supra* note 3. The perpetually self-executing code is simply strings of characters that perform specific functions on the Ethereum blockchain. The Tornado Cash code therefore isn't the "property" of any foreign national under any sensible reading of that term.

Ignoring the ordinary meaning of "property" to empower OFAC to sanction the Tornado Cash code also makes little—which is to say, no—sense when read in the context of the Treasury Department's regulations. As those regulations explain, a sanctioned person may "seek administrative reconsideration of his, her or its designation" on the SDN list, "or assert that the circumstances resulting in the designation no longer apply, and thus seek to have the designation rescinded." 31 C.F.R. § 501.807. But at least at the current stages of artificial intelligence, a computer program designed to facilitate cryptocurrency transactions is simply unable to "submit arguments or evidence that [it] believes establishes that insufficient basis exists for the designation." *Id.* § 501.807(a). Nor can it possibly "request a meeting with [OFAC]" to discuss its designation on the SDN list. *Id.* § 501.807(c).[10] Of course, these regulations make perfect sense when it comes to persons whose property has been blocked. As applied to the designated smart contracts, though, the regulations become nonsense. That's further evidence that OFAC has overstepped its authority.

Finally, while IEEPA's text definitively resolves the inquiry against the government, the constitutional-avoidance canon provides "extra icing on a cake already frosted." *Van Buren v. United States*, 141 S. Ct. 1648, 1661 (2021) (quoting *Yates v. United States*, 574 U.S. 528, 557 (2015) (Kagan, J., dissenting)). That rule of statutory interpretation is premised on the "reasonable presumption that Congress [does] not intend" to enact statutes "which raise[] serious constitutional doubts." *Clark v. Suarez Martinez*, 543 U.S. 371, 381 (2005). The canon accordingly instructs courts to construe statutes so as "to avoid constitutional difficulties . . . if such a construction is fairly possible." *Boos v. Barry*, 485 U.S. 312, 331 (1988). As explained below, construing the word "property" to extend to open-source code like Tornado Cash would raise significant constitutional difficulties. And that is yet another reason for adhering to IEEPA's plain text and concluding that OFAC transgressed its authority.

It isn't clear how OFAC will attempt to justify its unprecedented sanctions in court. Perhaps it will argue that the Tornado Cash smart contracts are the intellectual "property" of their developers. But that would be mistaken. By opting for a fully open-sourced model, the Tornado Cash creators have evidently abandoned any intellectual property interest that they may have once had in the software. *See* 4 Nimmer on Copyright § 13.06 (2022) (observing that creators can abandon their copyrights); David Fagundes & Aaron Perzanowski, *Abandoning Copyright*, 62 Wm. & Mary L. Rev. 487, 490, 498–99 (2020) (same). The Tornado Cash code, in other words, has been released into the public domain. Anybody can run the code without restriction. Anybody can copy and improve upon it. And nobody has to pay for it. Simply put, the software project belongs to no one, and nobody can assert a "right or

[10] The Treasury Department's regulations don't provide a mechanism for third parties to petition for SDN delisting. Only blocked persons may petition for their own removal. *See* 31 C.F.R. § 501.807. Even so, there is an alternative outlet to judicial review for certain third parties. Namely, individuals who have had their assets frozen in Tornado Cash or who have concrete plans to use the software without subjecting themselves to the pain of fines and imprisonment will likely have standing to challenge the final agency action under the Administrative Procedure Act.

interest protected by law" in the string of characters that comprise the lines of code. *Drye*, 528 U.S. at 56 (quotation omitted). So it is no one's "property," and it therefore cannot be blocked under IEEPA.[11]

Lacking any foothold in the statutory text, OFAC may alternatively attempt to defend its action by appealing to IEEPA's purposes. Those statutory objects ostensibly include empowering the executive to enact commercial measures designed to mitigate threats to our national security. And OFAC claimed that its sanctions furthered that goal. *See* Press Release, *supra* note 4. But "no legislation pursues its purposes at all costs." *Rodriguez v. United States*, 480 U.S. 522, 525–26 (1987) (per curiam). It is therefore "quite mistaken to assume" that "'whatever' might appear to 'further[] the statute's primary objective must be the law.'" *Henson v. Santander Consumer USA Inc.*, 137 S. Ct. 1718, 1725 (2017) (alteration in original) (quoting *Rodriguez*, 480 U.S. at 526). The American people are instead "entitled to rely on the law as written." *Bostock v. Clayton County*, 140 S. Ct. 1731, 1749 (2020). For that reason, our courts cannot be expected to ignore that "the textual limitations upon [IEEPA]'s scope are no less a part of its 'purpose' than its substantive authorizations." *Kucana v. Holder*, 558 U.S. 233, 252 (2010) (quotation marks omitted). The law permits the President to block only the "property" of foreign actors from moving through U.S. commerce. It provides no roving license to block anything—such as the Tornado Cash code—that might conceivably protect our national security.

Accordingly, IEEPA's text makes clear that OFAC exceeded its legal authority in sanctioning the Tornado Cash smart contracts. As things stand, they do not appear to be the "property" of any foreign entity.

OFAC's Sanctions Also Raise Substantial Constitutional Questions

In addition to overstepping its statutory authority, OFAC's placement of the Tornado Cash smart contracts on the SDN list raises some serious constitutional issues. First, by freezing innocent Americans' assets tied up in Tornado Cash, OFAC arguably deprived those individuals of their property without due process of law. Second, by indiscriminately freezing the assets of those innocent Americans, OFAC may have also violated the Fourth Amendment's prohibition on unreasonable seizures. And third, by forbidding the use of an application that can facilitate protected speech, OFAC's sweeping sanctions order raises significant First Amendment concerns. We think these are all serious constitutional issues. Though, in all likelihood, a court would strike down OFAC's action on statutory grounds before it even got to the constitutional grounds.

[11] Nor, as discussed above, could OFAC justify the Tornado Cash sanctions based on the role played by relayers in providing an optional, additional layer of privacy protection for Tornado Cash users. If OFAC determined that certain relayers were foreign persons involved in "malicious cyber-enabled activities," then those relayers could potentially be subject to sanctions, and American Tornado Cash users could be prohibited from engaging in transactions with them. But it is not clear to us that OFAC in fact has made the necessary findings or targeted the relayers themselves. And even if they could be sanctioned, that would not justify targeting the Tornado Cash smart contracts, which are not and cannot be viewed as the property of the relayers, let alone anyone else.

I. OFAC Failed to Provide Americans with Notice or a Hearing Before Depriving Them of Their Property

Starting with due process, the problem is that—without any notice or a hearing—OFAC prohibited Americans from accessing lawfully owned funds that they had deposited into Tornado Cash prior to the sanctions. That frozen ETH is undoubtedly the users' property. And by restricting the users' ability to legally access and transact using their cryptocurrency, the government has "deprived" them of that "property." U.S. Const. amend. V; *see also* Keith Werhan, *Principles of Administrative Law* 159 (3d ed. 2019) ("Ordinarily, any government action that adversely affects an individual's interest in . . . property qualifies [as a deprivation].").

Granted, the Constitution doesn't prohibit all deprivations of property. It forbids only those accomplished "without due process of law." U.S. Const. amend. V. So having determined that the sanctions deprived citizens of their crypto assets, "the question remains what process is due" under the Fifth Amendment. *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972).

The answer: Probably more than what OFAC afforded here. In determining what process is "due," courts consider three factors: "(1) the nature of 'the private interest that will be affected,' (2) the comparative 'risk' of an 'erroneous deprivation' of that interest with and without 'additional or substitute procedural safeguards,' and (3) the nature and magnitude of any countervailing interest in not providing 'additional or substitute procedural requirement[s].'" *Turner v. Rogers*, 564 U.S. 431, 444–45 (2011) (alteration in original) (quoting *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976)). Employing that tripartite framework, the Supreme Court has tended to require that the government afford "notice and a hearing"—two requirements "central to the Constitution's demand of due process"—to affected individuals "prior" to depriving them of their property. *United States v. James Daniel Good Real Prop.*, 510 U.S. 43, 53 (1993). That is, the Court has "tolerate[d] some exceptions to the general rule requiring predeprivation notice and hearing, but only in *extraordinary* situations where some valid governmental interest is at stake that justifies postponing the hearing until after the event." *Id.* (emphasis added) (quotation marks omitted). This rule helps to avoid "mistaken deprivations of property," and it "reflects the high value" that American society has always "place[d] on a person's right to enjoy what is his, free of governmental interference." *Fuentes v. Shevin*, 407 U.S. 67, 81 (1972).

As of yet, though, there is no evidence that the government provided any pre-deprivation process to those whose assets have been blocked. Instead, the only available recourse is for each of those Americans to individually apply for a post hoc license from OFAC to access their respective funds—or face the risk of significant fines and jail time. *See* 31 C.F.R. § 501.801. That process will cost law-abiding citizens time and, for some, anxiety and legal fees. Even more troubling, licensing decisions are subject to the OFAC Director's discretion, and so there's no guarantee that one will be provided upon the satisfaction of any specified conditions. Perhaps

recognizing this problem, on September 13, OFAC announced that it at least nominally "would have a favorable licensing policy" for applications that provide, "at a minimum, all relevant information regarding" the intended transaction.[12] That is a step in the right direction. But time will tell how that vague policy actually operates in practice.

In any event, whether or not OFAC ultimately grant licenses, the lack of pre-deprivation safeguards raises the specter of a due process violation. And a close inspection of the three factors set forth above reveals that the government's post-deprivation licensing mechanism for restoring affected Americans' property rights may not pass constitutional muster.

First consider the private interests affected by the sanctions. On one hand, an individual who has deposited only $100 worth of ETH into Tornado Cash may not have a particularly weighty interest. But compare the situation of our hypothetical employee from above who receives her wages in cryptocurrency, and a very different picture emerges. If a significant fraction of her assets have been funneled through Tornado Cash and she doesn't have sufficient "independent resources," then OFAC's sanctions will have effectively deprived her "of the very means by which to live while [s]he waits" for a decision on her license application. *Goldberg v. Kelly*, 397 U.S. 254, 264 (1970); *see also Sniadach v. Family Fin. Corp.*, 395 U.S. 337, 341–42 (1969). Due process doesn't countenance such significant deprivations of property prior to notice and a hearing. Further, notwithstanding OFAC's announced policy, it is unclear just how long the licensing process will take. There is no statutory or regulatory deadline for reviewing applications, and the magnitude of the private interests at stake only increases with each passing day. *See Fusari v. Steinberg*, 419 U.S. 379, 389 (1975) (explaining that "the possible length of wrongful deprivation . . . is an important factor in assessing the impact of official action on the private interests").

On the other side of the scale, one must acknowledge that "the government's interest in national security" and protecting our economy "cannot be understated." *Al Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury*, 686 F.3d 965, 980 (9th Cir. 2012). In the ordinary sanctions context, OFAC needs to act quickly and with secrecy to block the sanctioned property. If it gives the bad actors a heads up, then they can just go ahead and move their property outside the jurisdiction of the United States. By that logic, if the government had alerted Tornado Cash users that it was considering sanctioning the application, then perhaps cyberhackers might have similarly taken steps to withdraw their ETH before the sanctions took effect.

But it is not at all clear that such a rationale would be justified here, where OFAC has adopted a solution that was both (1) unlawful, and (2) poorly tailored to its goal of impeding cyberhackers. Indeed, due to the Ethereum blockchain architecture and the open-source nature of the Tornado Cash smart contracts, the code remains useable for illicit actors like the Lazarus Group—even to this day. The OFAC sanctions may prevent law-abiding U.S. persons from taking advantage of the Tornado Cash application in the future—since they could face criminal penalties for doing

[12] *See Frequently Asked Questions 1079*, U.S. Dep't of the Treasury (Sep. 13, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1079.

so—but the sanctions may not have furthered the government's interest in combatting sophisticated foreign cyberhackers.

At the same time, the haphazard sanctions have undoubtedly operated at the expense of honest Americans, who, despite no wrongdoing, are now subject to steep penalties if they so much as attempt to retrieve frozen assets that are rightfully theirs. *Cf. also Goldberg*, 397 U.S. at 266 (suggesting that the government likewise has an interest in seeing that its citizens aren't wrongfully deprived of their property). This isn't to suggest that the government has no interest at stake in dispensing with pre-deprivation procedures. It certainly does. It is just that the magnitude of that interest might be significantly less than appears at first blush.

The final factor—which is "critical when the governmental and private interests both have weight"—is the risk of erroneous deprivation. *Kaley v. United States*, 571 U.S. 320, 338 (2014). Though details are still emerging, at this point, that factor looks to cut sharply against the government. As stated above, even though a large chunk of the funds run through Tornado Cash is attributable to criminal money laundering, most of it is not. And after accounting for the fact that a sizable fraction of the illicit funds looks to be attributable to just a few groups, the proportion of legal users is likely even higher. Accordingly, there is no "substantial assurance that the deprivation is not baseless or unwarranted" for the vast majority of Americans who simply value their privacy and have used Tornado Cash for lawful means. *Fed. Deposit Ins. Corp. v. Mallen*, 486 U.S. 230, 240 (1988). Unfortunately, OFAC's poorly tailored sanctions apply to them just the same, and the collateral damage has already been done.

Because the risk of erroneous deprivation may be intolerably high in light of the competing interests, a court could reasonably hold that this "is not one of those extraordinary instances that justify the postponement of notice and hearing." *James Daniel Good Real Prop.*, 510 U.S. at 62.

II. The Blanket Seizure of Crypto Assets Implicates the Fourth Amendment

Moving along, OFAC's action also raises some serious questions under the Fourth Amendment, which protects the people against "unreasonable . . . seizures" of their property. U.S. Const. amend. IV; *see United States v. Jones*, 565 U.S. 400, 405 (2012). OFAC's sanctions arguably violated this command too.

As an initial matter, OFAC's designation of Tornado Cash on the SDN list resulted in the "seizure" of Americans' crypto assets within the meaning of the Fourth Amendment. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). And so it is here. As a result of OFAC's sanctions, Americans who have deposited their ETH into the Tornado Cash mixer are now forbidden from accessing the cryptocurrency that belongs to them. That indefinite freeze of their financial assets is undoubtedly a "meaningful interference" with their possessory interests. *See, e.g.*, *United States v. Cosme*, 796 F.3d 226, 235 (2d Cir. 2015).

The harder question is whether the seizure of the crypto assets was "unreasonable." "In the ordinary case, the Court has viewed a seizure of personal property as per se unreasonable within the meaning of the Fourth Amendment unless it is accomplished pursuant to a judicial warrant issued upon probable cause and particularly describing the items to be seized." *United States v. Place*, 462 U.S. 696, 701 (1983). Of course, OFAC didn't obtain a warrant here—much less one that described the crypto assets seized with any degree of particularity. It instead unilaterally—and indiscriminately—blocked the Tornado Cash application.

Still, the Court has disposed of the need for a warrant "if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present." *Id.* And it remains to be seen whether the government could successfully point to any such exception here. If challenged, OFAC will most likely attempt to justify its action through the "special needs" exception. *See Al Haramain Islamic Found.*, 686 F.3d at 990–95. That exception applies in situations that present special needs "beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements." *Griffin v. Wisconsin*, 483 U.S. 868, 874 (1987).

But even accepting that there is an important government interest in thwarting the efforts of foreign money launderers to hide their crypto assets, such a "sensitive subject matter" isn't always a valid "excuse for the dispensing altogether with domestic persons' constitutional rights." *Al Haramain Islamic Found.*, 686 F.3d at 993. And so far as the Fourth Amendment is concerned, the basic shortcoming in OFAC's action is the sheer breadth of its sanctions order. Absent any individualized suspicion of wrongdoing, the government has indiscriminately seized the assets of Americans who use Tornado Cash for wholly legitimate purposes. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000) (explaining that there are only "limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion").

True, aggrieved parties may apply for specific licenses to withdraw their cryptocurrency. *See* 31 C.F.R. § 501.801. This renders the seizure potentially temporary and somewhat less unreasonable. But the Treasury Department has represented that it "cannot predict how long" it will take for such licenses to issue—if at all.[13] It is also worth noting that the very act of applying for a license defeats the privacy features that Tornado Cash users legitimately seek. That's because OFAC has instructed applicants to provide their wallet addresses in order to receive a license, and that information will expose the applicant's entire transaction history to government eyes. In view of these considerations, it is at least plausible that those whose assets are tied up in Tornado Cash have a valid Fourth Amendment claim.[14]

[13] *See Frequently Asked Questions 58*, U.S. Dep't of the Treasury (Sept. 10, 2002), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/58.

[14] One last point on the Fourth Amendment. It isn't yet clear whether and to what extent the government has or intends to comb through electronic data associated with Tornado Cash. If it does, though, then the Fourth Amendment's parallel protection against unreasonable "searches" will be in play too. U.S. Const. amend. IV. The Supreme Court has recognized that individuals may have a reasonable expectation of privacy—and thus a protected Fourth Amendment interest—in certain electronic data, even where the technology requires that such data be shared with third parties. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (cell site location information); *Riley v. California*,

III. OFAC's Sanctions Burden Constitutionally Protected Speech

That brings us to the final constitutional concern implicated by OFAC's unprecedented actions. The First Amendment prohibits the government from "abridging the freedom of speech." U.S. Const. amend. I. And OFAC's sanctions plausibly violate that fundamental guarantee.

Shortly after OFAC added the Tornado Cash smart contracts to the SDN list, some feared that the sanctions impermissibly chilled the publication of First Amendment-protected speech contained in the code itself. That fear was understandable. Courts across the country have held that "computer code, and computer programs constructed from code, can merit First Amendment protection." *Universal City Studios v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *see also, e.g.*, *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *DVD Copy Control Ass'n, Inc. v. Bunner*, 75 P.3d 1, 10 (Cal. 2003); *Green v. U.S. Dep't of Justice*, 392 F. Supp. 3d 68, 86 (D.D.C. 2019); *Def. Distributed v. U.S. Dep't of State*, 121 F. Supp. 3d 680, 692 (W.D. Tex. 2015). After all, just like the spoken word, code "convey[s] information capable of comprehension and assessment by a human being." *Universal City Studios*, 273 F.3d at 448.

If OFAC were to threaten punishment for the mere creation or publication of the Tornado Cash code (or something similar), that would surely pose a serious threat to First Amendment freedoms. But the agency has now clarified that it hasn't gone that far—at least not yet. It has announced that its sanctions are limited to blocking transactions with Tornado Cash. *See Frequently Asked Questions 1076*, *supra* note 2. "U.S. persons [will] not be prohibited by [the] sanctions regulations from copying the open-source code and making it available online for others to view, as well as discussing, teaching about, or including open-source code in written publications, such as textbooks, absent additional facts." *Id.* So, although OFAC still faces a plausible First Amendment challenge—as we discuss below—it has at least retreated from a position that would have raised additional free-speech concerns.

Still, the fact that OFAC will not block U.S. persons from copying or making available the Tornado Cash source code does not mean that OFAC's action has no other First Amendment costs. OFAC's sanctions may burden the free-speech rights of Tornado Cash's users who seek to anonymously engage in certain transactions—such as donating to controversial advocacy groups—that enable important, socially valuable expression.

Here's why that's problematic. The "decision to remain anonymous" is "an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). And indeed, there are "a significant number of persons who support causes anonymously," "motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." *Watchtower*

573 U.S. 373, 386 (2014) (data stored on cell phones). And because the whole point of using Tornado Cash is to protect information about financial transactions, the legitimate privacy expectations of the application's users are similarly strong. Therefore, the government must "generally obtain a warrant supported by probable cause before acquiring such records." *Carpenter*, 138 S. Ct. at 2221. If the government elects not to follow that path before searching the electronic data, it will risk a constitutional violation.

Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166 (2002) (quotation marks omitted).

The Tornado Cash privacy protocol facilitates that anonymity. And that anonymity allows people to freely engage in socially and politically valuable speech, which they may otherwise not be willing to do if their identities were exposed. *See Talley v. California*, 362 U.S. 60, 64 (1960) (observing that throughout history, many have been willing to speak out "anonymously or not at all"). One could imagine a host of scenarios wherein users rely on Tornado Cash to anonymously donate to controversial causes without the fear of political or social reprisal. But the OFAC sanctions limit users' ability to engage in that constitutionally protected expressive activity.

The government may respond that its sanctions don't forbid "speech" in the traditional sense; rather, they ban the use of a tool that facilitates private transactions. But "virtually every means of communicating ideas in today's mass society requires the expenditure of money." *Buckley v. Valeo*, 424 U.S. 1, 19 (1976). So it is no answer that a government regulation burdens expenditures made to fund worthy causes, as opposed to the speech perpetuated by the causes themselves. Reducing the former effectively reduces the latter. Thus, by burdening the provision of private donations, the OFAC sanctions operate to "restrict[] the voices of people and interest groups who have money to spend" and thereby "reduce[] the quantity of expression" and diversity of ideas that those donations enable. *Id.* at 17, 19.[15]

At this point, however, it is difficult to predict exactly how a court faced with a First Amendment challenge to the OFAC sanctions will rule. Not all burdens on speech violate the Constitution. *See, e.g.*, *Ward v. Rock Against Racism,* 491 U.S. 781, 791 (1989). And some of the details that bear on the interests at stake are not yet publicly available. But suffice it to say that the sanctions do burden protected speech to some extent and, as a result, expose the agency to a risk that its designation of the Tornado Cash code on the SDN list will be held to be "contrary to constitutional right." 5 U.S.C. § 706(2)(B).

Conclusion

In sum, we think that OFAC went too far when it came to sanctioning Tornado Cash. OFAC appears to have blocked open-source, self-executing software that isn't a person or the "property" of any foreign national or entity. IEEPA doesn't grant the executive such broad, roving authority to target open-source software architecture, and that is true no matter how noble OFAC's intentions may have been. Our system of government "does not permit agencies to act unlawfully even in pursuit of desirable ends." *Ala. Ass'n of Realtors v. Dep't of Health & Human Servs.*, 141 S. Ct. 2485, 2490 (2021) (per curiam).

[15] In much the same way, the OFAC sanctions could "also impinge on protected associational freedoms." *Buckley*, 424 U.S. at 22. Contributing to a political or social cause "enables like-minded persons to pool their resources" and expend those resources on expressive activities. *Id.*; *see also NAACP v. Ala. ex rel. Patterson*, 357 U.S. 449, 460 (1958) ("Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association . . . ."). But by removing an effective means for anonymous donations to controversial causes, the sanctions have the "practical effect of discouraging the exercise" of associational freedom. *See NAACP*, 357 U.S. at 461 (quotation marks omitted); *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2389 (2021) (holding that "[t]he risk of a chilling effect on association is enough" to trigger the protections of the First Amendment).

What's more, the agency has exposed itself to constitutional attack on multiple fronts. Its sanctions resulted in an asset freeze that deprived innocent Americans of their property—likely without due process of law. And it may have violated the Fourth Amendment's prohibition on unreasonable seizures too. Finally, while OFAC's recent guidance shows that it recognizes the First Amendment problems inherent in banning the publication of code altogether, its prohibition on the use of Tornado Cash code burdens the ability of Americans to use the privacy-enabling application to facilitate anonymous speech. That itself raises a substantial First Amendment issue.

We certainly support OFAC's efforts to target cybercriminals and other forms of bad actors who misuse cryptocurrency networks. But the government's efforts to combat money laundering need to focus upon the money launderers themselves. If more regulation is needed, then OFAC should look to Congress to provide it. What OFAC cannot do is shut down the tools that legitimate users rely upon to protect their financial privacy on the blockchain. OFAC should own up to its mistake before the federal courts tell it to do so.