UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF ONE ADDRESS IN WASHINGTON, D.C., UNDER RULE 41	**Case No. 20-sw-314 (ZMF)**

MEMORANDUM OPINION

To seize or not to seize, that is the question. On December 15, 2020, the government submitted an Application for a Warrant ("Application") to search a residence (the "Target Premises") in Washington, D.C., and to seize from the Target Premises items related to suspected violations of the child pornography statute. *See* ECF No. 6 (Application for Search & Seizure Warrant and Accompanying Documents) at 4, 6 ("Warrant"). Among the specific properties the government sought for seizure were all cryptocurrency and information necessary to access such cryptocurrency. *See* Warrant at 6–7, 12. For the below reasons, this Court granted the Application.

I. Background

In or around April 2019, agents with U.S. Homeland Security Investigations ("HSI") began investigating a marketplace on the darknet ("Website 1")[1] "dedicated to the advertisement and distribution of child pornography." Warrant at 46. Darknet marketplaces frequently act as "the Amazon for contraband." Vicki Chou et al., *Prosecuting Darknet Marketplaces: Challenges and Approaches*, 67 DOJ J. Fed. L. & Prac. 65, 66 (2019). To access darknet marketplaces, users must download anonymizing software called "The Onion Router" (also referred to as "Tor"). Warrant at 41. "Tor-based websites 'anonymize[ ] [i]nternet activity by routing [a] user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-

[1] While law enforcement knows the name of Website 1, this information has not been disclosed to avoid alerting "its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or to destroy evidence." Warrant at 46 n.2.

protocol ("IP") address of the user.'" *United States v. Harmon*, No. 19-cr-395, 2020 WL 4251347, at *3 (D.D.C. July 24, 2020) (quoting *United States v. Galarza*, No. 18-mj-146, 2019 WL 2028710, at *2 (D.D.C. May 8, 2019). "Tor is not in and of itself illegal. Indeed, it is partially supported by the United States government and is used around the world to promote free speech and privacy. But the anonymity that Tor brings has a darker side, as it is also used by criminals and others who would seek to evade law enforcement detection." Chou et al., *supra*, at 67.

Nothing is free, including on the darknet. Payments on darknet marketplaces frequently occur via "cryptocurrenc[y]," which is "a virtual currency traded over the Internet and controlled through computer software rather than issued by a bank or government." *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d 1, 3 (D.D.C. 2020). Bitcoin ("BTC") is the most widely-used cryptocurrency.[2] "Individuals can acquire BTC through cryptocurrency exchanges, cryptocurrency ATMs, or directly from other people." Warrant at 43. BTC transactions "require[] an address, a public encryption key, and a private encryption key." *Harmon*, 2020 WL 4251347, at *2. These encryption keys generally are stored in unhosted wallets (*e.g.*, paper or electronic media retained by the owner), or hosted wallets (account held by a third party financial-institution, known as a cryptocurrency exchange).[3] *See* Jai Ramaswamy, *How I Learned to Stop Worrying and Love Unhosted Wallets*, Coin Center (Nov. 18, 2020), available at

[2] Bertram Gilfoyle created an informative slide deck on the history of money and cryptocurrency. *See* http://www.piedpiper.com/app/themes/pied-piper/dist/images/Gilfoyle_s_Crypto_PowerPoint_-_Digital_Edition.pdf.

[3] BTC in an unhosted wallet is like cash in a personal safe or hidden under the mattress, while BTC in a hosted wallet is like money in a bank account. In fact, cryptocurrency exchanges are subject to the Bank Secrecy Act. *See Harmon*, 2020 WL 4251347, at *21–22 (classifying cryptocurrency exchanges as money transmitting businesses under 18 U.S.C. § 1960). Thus, cryptocurrency exchanges are "required by U.S. law to collect identifying information on [their] customers." *Galarza*, 2019 WL 2028710, at *2.

https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/. "Most [darknet] marketplaces assign users a cryptocurrency wallet to make purchases or receive payments." Warrant at 43. "Darknet marketplace users can transfer cryptocurrency from an external [hosted or unhosted] wallet into their marketplace wallet by sending [BTC] to a deposit address assigned to their account." *Id.*

Transfers of fiat currency[4] are not recorded in any centralized location. However, every transfer of BTC is documented in real time on a public ledger called the "blockchain." *See Harmon*, 2020 WL 4251347, at *2. "The [BTC] blockchain contains only the sender's address, the receiver's address, and the amount of Bitcoin transferred." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Although "[t]he owners of the addresses are anonymous on the [BTC] blockchain," *id.*, law enforcement can use publicly-available software[5] to analyze the BTC blockchain by "forensically examining, tracing, and mapping data on the blockchain . . . to unmask the identities of specific users of a given cryptocurrency wallet." Warrant at 44. Ironically, the public nature of the blockchain makes it exponentially easier to follow the flow of cryptocurrency over fiat funds. *See Gratkowski*, 964 F.3d at 312 ("Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private, thus undercutting their claim of a legitimate expectation of privacy.") (internal quotation marks and citation omitted).

Website 1 advertised child-exploitation material to subscribers who paid using BTC. *See* Warrant at 46–47. Law enforcement, acting in an undercover capacity, purchased videos from

[4] "Fiat money is a currency (a medium of exchange) established as money, often by government regulation, that does not have intrinsic value." https://en.wikipedia.org/wiki/Fiat_money.

[5] Examples of such blockchain analytic tools include, *inter alia*: Chainalysis (https://www.chainalysis.com/), Eliptic (https://www.elliptic.co/), and TRM Labs (https://trmlabs.com/).

Website 1. *See id.* at 47. The downloaded videos depicted children, ranging from infant to 6 years of age, being sexually abused. *See id*. at 46–47.

Blockchain analysis revealed that Website 1 used a "payment processing service . . . operated by a known cryptocurrency exchange service (the 'Exchange') located in the United States" to effectuate the illicit transactions. *Id.* at 47–48. By subpoenaing the Exchange, law enforcement obtained documents revealing the identity of the Subject. *See id.* at 48, 51. Records from the Exchange further detailed what law enforcement saw on the blockchain: the sending of BTC by the Subject to Website 1 in November 2019. *See id.* at 51–52. Subpoena returns further revealed that the Subject resided at the Target Premises. *See id.* at 57.

On December 15, 2020, the government submitted an Application requesting authority to search the Target Premises for: "evidence of a crime;" "contraband, fruits of crime, or other items illegally possessed;" and "property designed for use, intended for use, or used in committing a crime" related to violations of 18 U.S.C. §§ 2252A(a)(2) (receipt of child pornography) and 2252A(a)(5)(B) (possession and/or access with intent to view child pornography) ("Target Offenses"). Warrant at 1. The undersigned magistrate judge signed the warrant that day, authorizing the search and seizure of any material that constituted "fruits, evidence, information, contraband, or instrumentalities in whatever form and however stored, related to violations of [the Target Offenses]." *Id.* at 1, 6. Pursuant to 18 U.S.C. § 2253, the Court further authorized seizure of all unhosted wallets and any information used to access hosted or unhosted cryptocurrency wallets.[6] *See id.* at 12. The Court also authorized the government "to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency

[6] This kind of information would include "wallet recovery seeds, and usernames, passwords, mnemonic pins, PGP keys and 2FA devices." Warrant at 6.

address controlled by the United States . . . [, and] copy any wallet files and restore them onto computers controlled by the United States . . . [which would allow the government] to collect cryptocurrency transferred into the [Subject's] wallets as a result of transactions that were not yet completed at the time that the [Subject's] devices were seized" (collectively, the "Target Properties"). *Id.* at 7.

II. Legal Standards

A. Pretrial Seizure of Property

The pretrial seizure of forfeitable property is authorized by 21 U.S.C. § 853(f). *See United States v. Bikundi*, 125 F. Supp. 3d 178, 184 (D.D.C. 2015). The Court shall issue a warrant authorizing the seizure of such property if there is probable cause to believe: "(1) that 'the defendant has committed an offense permitting forfeiture;' and (2) that 'the property at issue has the requisite connection to that crime.'" *Id.* (quoting *Kaley v. United States*, 571 U.S. 320, 323–24 (2014). The standard of probable cause "is 'not a high bar.'" *Id.* (quoting *Kaley*, 571 U.S. at 338). Rather, it means a "fair probability." *Id.* (quoting *United States v. Jackson*, 415 F.3d 88, 91 (D.C. Cir. 2005)). There is a "strong governmental interest in obtaining full recovery of all forfeitable assets." *Caplin & Drysdale, Chartered v. United States*, 491 U.S. 617, 631 (1989). "Forfeiture serves important punitive and deterrence functions, and forfeited property often is put to productive use in assisting crime victims and improving communities damaged by criminal behavior." *Bikundi*, 125 F. Supp. 3d at 183 (citing *Kaley*, 571 U.S. at 323).

B. Forfeiture Authority for Child Pornography Violations

Violations of 18 U.S.C. § 2252A give rise to forfeiture of three categories of property: (1) the child pornography itself; (2) proceeds traceable to the offense; (3) and "any property, real or personal, used or intended to be used to commit or to promote the commission of such offense."

18 U.S.C. § 2253(a)(1)–(3).[7] This third prong covers two sub-categories—property used to (1) commit or (2) promote the offense. *See* § 2253(a)(3). These terms are to be "liberally construed to effectuate [the] remedial purposes [of forfeiture]." *United States v. Rivera*, 884 F.2d 544, 546 (11th Cir. 1989) (quoting 21 U.S.C. § 853(o)).

"To 'use' is to 'convert to one's service, to employ, to avail oneself of, and to carry out a purpose or action by means of.'" *Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 7 (citing *United States v. Hull*, 606 F.3d 524, 527 (8th Cir. 2010)).

The first subcategory, property used to commit the offense, has no analogue in other forfeiture statutes. It includes: (1) cryptocurrency wallets used to access a darknet child pornography site, *see Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 7; (2) a home from which a person accessed child pornography, *see Hull*, 606 F.3d at 527–28; and (3) electronic devices used to view child pornography, *see United States v. Gleason*, 277 F. App'x 536, 539 (6th Cir. 2008). It is irrelevant that such tools are not inherently illegal or may have been used for legitimate purposes. *See United States v. Heldeman*, 402 F.3d 220, 222 (1st Cir. 2005). Rather, courts consider the nature of the property. *See id.* For example, while a person could not effectively download child pornography "in a library, coffee shop, or senior center," doing so is easily possible from the seclusion of a home. *Hull*, 606 F.3d at 528.

Courts treat the second subcategory, property used to promote the offense, as analogous to "facilitating property." *United States v. Jalaram, Inc.*, 599 F.3d 347, 351 (4th Cir. 2010); *see also Gleason*, 277 F. App'x at 539 (6th Cir. 2008) ("forfeiture of certain facilitating equipment, such as Gleason's computer and cellular phone, pursuant to 18 U.S.C. § 2253(a)(3)"). Facilitating property makes "the prohibited conduct less difficult or more or less free from obstruction or

[7] Section 2253(b) incorporates the seizure provisions of 21 U.S.C. § 853.

hindrance." *United States v. Schifferli*, 895 F.2d 987, 990 (4th Cir. 1990) (quoting *United States v. Premises Known as 3639-2nd Street, N.E., Minneapolis, Minn.*, 869 F.2d 1093, 1096 (1989) (internal quotation marks omitted).[8] Facilitating property includes: (1) a home from which a person accesses child pornography, because the home provides privacy that makes the crime harder to detect, *see Hull*, 606 F.3d at 527;[9] (2) an office from which a dentist illegally dispensed narcotics, as the office "provided an air of legitimacy and protection from outside scrutiny," *Schifferli*, 895 F.2d at 991; and (3) horses, when the horse breeding business helped conceal underlying drug trafficking activities at a farm, *see Rivera*, 884 F.2d at 546. "[T]here is no requirement that the property's role in the crime be integral, essential, or indispensable, . . . nor does the property need to be exclusively used for criminal activity to be subject to forfeiture." *United States v. Seher*, 574 F. Supp. 2d 1368, 1370 (N.D. Ga. 2007), *aff'd in part, vacated in part, remanded*, 562 F.3d 1344 (11th Cir. 2009) (citing *Schifferli*, 895 F.2d at 990–91).

III. Discussion

A. Probable Cause the Subject Committed an Offense Permitting Forfeiture

There is probable cause to believe the Subject violated the Target Offenses. *See generally* Warrant at 13–59. On November 7, 2019, the Subject purchased child pornography from Website 1 using BTC. *See id.* at 49, 52. "[S]everal circuit courts have held that membership in a child

[8] The civil forfeiture statute requires that facilitating property have a "substantial connection between the property and the offense." 18 U.S.C. § 983(c)(3). Many courts have assumed without deciding that there is similar requirement in criminal forfeitures, *see, e.g.*, *Hull*, 606 F.3d at 527, while other courts have sidestepped this question because there was such a strong nexus between the forfeitable property and the offense, *see, e.g.*, *United States v. Reid*, 732 Fed. App'x 14, 18 (2d Cir. 2018). Given that § 983(c) explicitly limits this requirement to "civil forfeiture," there is no statutory basis to apply such test to criminal forfeiture. Yet, the issue is moot here where the is a strong nexus between the Target Properties and the Target Offenses. *See id.*

[9] Property can be used both to commit and promote child pornography offenses. *See, e.g.*, *Hull*, 606 F.3d at 527.

pornography website alone sufficiently establishes probable cause, reasoning that an individual who took the affirmative steps necessary to become a member probably accessed or contributed to the site's illegal content." *United States v. Taylor*, 250 F. Supp. 3d 1215, 1230 (N.D. Ala. 2017), *aff'd*, 935 F.3d 1279 (11th Cir. 2019) (collecting cases). "Any user logging into [Website 1] would have had to take these steps: (1) download Tor software; (2) acquire the website's unique algorithm-generated address (most likely from a [website] user or from another Tor hidden service page . . .); (3) navigate to [the website], featuring suggestive images . . . with directions regarding file uploading and posting; (4) create a [website] account . . . ; and (5) arrive at the main [website] directory, which included forum titles that clearly alluded to illicit pornographic content of children," *id.* at 1230. These "numerous affirmative steps" provide probable cause to believe that any user sending BTC to Website 1 "did so with the intent to access, view, and/or [posses] child pornography; *i.e.*, to engage in criminal conduct." *Id.*

B. Target Properties Have Requisite Connection to the Crime

There is probable cause to believe the Target Properties have the requisite connection to these alleged crimes.[10] *See Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 7. The Subject relied on the pseudonymous nature of cryptocurrency to send funds to a website concealed by Tor. *See* Warrant at 46, 48, 51. The (perceived) anonymity of cryptocurrency writ large was "crucial and necessary" to the commission of the offense because it concealed the purchase of child pornography. *United States v. 7046 Park Vista Rd.*, 537 F. Supp. 2d 929, 941 (S.D. Ohio 2008); *see also Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 7. As with a home,

[10] The specific BTC the Subject used to purchase child pornography was property used "to commit" the crime. 18 U.S.C. § 2253(a)(3). However, that property left the possession of the Subject when he sent it to Website 1, and as such, is not the subject of the government's instant request.

cryptocurrency allowed the Subject to operate without fear of discovery. *See Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 7 (citing *Hull*, 606 F.3d at 527–28); *see also United States v. Wilk*, No. 04-cr-60216, 2007 WL 2263942, at *1 (S.D. Fla. Aug. 6, 2007). Although the Subject could have used a bank account to wire fiat funds to a child pornography website, doing so would have risked attention from bank compliance officers "[c]onducting ongoing monitoring to identify and report suspicious transactions," Bank Secrecy Act Manual, available at: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/02. *See Hull*, 606 F.3d at 528 (forfeiting home even though crime could have been operated from a motel, because home avoided attention that would be attracted by frequent visits to a motel).

All cryptocurrency, not just BTC, at the Target Premises are subject to seizure and forfeiture because it was the pseudoanonymous *nature* of cryptocurrency—rather than the particular type used—that allowed for the commission and promotion of the crime.[11] Moreover, the wallets in which the BTC was held provided the means to store and transmit payments to

[11] The horror story of unhosted wallets is fiction, not fact. "Unhosted wallets are more like a personal billfold than a Swiss bank account[.]" Ramaswamy, *supra*. Indeed, cash poses a greater challenge to law enforcement than cryptocurrency in unhosted wallets. *See United States v. One Parcel of Real Prop. Located at 19 Mountain Ave., New London, Conn.*, No. 3:18-cv-00471, 2020 WL 6729261, at *4 (D. Conn. Nov. 16, 2020). First, forfeiture is foreclosed where cash did not facilitate the child pornography offense, which may often be the case. *See id.* Yet, the pseudoanonymity of cryptocurrency automatically justifies seizure of *all* unhosted funds as facilitating property. *See supra* Part III(B). Second, even if cash is connected to the crime, proving so is difficult as "[c]ash is anonymous, fungible, and portable; it bears no record of its source, owner, or legitimacy; it is used and held around the world; and is difficult to trace once spent." *Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform*, Senate Hearing 115-212 before the Comm. on Banking, Hous., and Urb. Affs., 115th Cong. (Jan. 17, 2018) (statement of M. Kendall Day, Acting Deputy Assistant Att'y Gen., Crim. Div., Dep't of Just.). This is in stark contrast to cryptocurrency where *every* transaction is publicly documented from cradle to grave on the blockchain. The instant Application is yet another example that cryptocurrency—be it in hosted or unhosted wallets—is traceable *and* seizeable, which ultimately is to the benefit of "crime victims." *Bikundi*, 125 F. Supp. 3d at 183 (citing *Kaley*, 571 U.S. at 323).

Website 1. Thus, the Subject's "non-contraband [cryptocurrency—whether BTC or otherwise—] is intertwined with its contraband counterparts." *United States v. Wernick*, 148 F. Supp. 3d 271, 276 (E.D.N.Y. 2015), *aff'd*, 673 F. App'x 21 (2d Cir. 2016). This Court's refusal to divorce the "tainted" from "untainted" Target Properties is consistent with how courts treated a house and related acreage in *Hull*, *see* 606 F.3d at 528, and electronic media in *Wernick*, *see* 148 F. Supp. 3d at 276.[12]

IV. Conclusion

The answer is to seize.

2021.01.06
08:10:09 -05'00'

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE

[12] "The forfeiture of proceeds relieves the defendant of his illegal gain, and therefore cannot be excessive." *See United States v. Powell*, 2 F. App'x 290, 294 (4th Cir. 2001). However, other categories of forfeitable property are subject to Eighth Amendment analysis. *See Heldeman*, 402 F.3d at 223. "A forfeiture will violate the Eighth Amendment's prohibition only if it is 'grossly disproportional to the gravity of the defendant's offense.'" *Id.* (quoting *United States v. Bajakajian*, 524 U.S. 321, 336–37 (1998)). Forfeitures related to child pornography offenses are rarely grossly disproportional given that "[t]he damage done by child pornography offenses is well documented, . . . and distribution of child pornography is especially serious." *Hull*, 606 F.3d at 530 (citing *United States v. Goff*, 501 F.3d 250, 258–60 (3d Cir. 2007) and *United States v. Kerr*, 472 F.3d 517, 523 (8th Cir. 2006); *see also United States v. Ownby*, 926 F. Supp. 558, 560–61, 570 (W.D. Va. 1996) (forfeiture of defendant's home not excessive because of nature of child pornography offenses), *aff'd*, 131 F.3d 138 (4th Cir. 1997). Regardless, Eighth Amendment challenges are not ripe until forfeiture is imposed after a finding of guilt. *See United States v. Hernandez-Gonzalez*, No. 16-cr-20669, 2017 WL 2954676, at *8 (S.D. Fla. June 26, 2017), *report and recommendation adopted*, No. 16-cr-20669, 2017 WL 3446815 (S.D. Fla. Aug. 10, 2017) (citing *United States v. Talebnejad*, 460 F.3d 563, 573 (4th Cir. 2006))