THE MAGAZINE OF THE LOS ANGELES COUNTY BAR ASSOCIATION

Los Angeles Lawyer

SEPTEMBER 2018 / $5

CORPORATE COUNSEL'S GUIDE TO CALIFORNIA LAW FIRMS AND ATTORNEYS

EARN MCLE CREDIT

EMPLOYEE DEFINITION AFTER *DYNAMEX*

page 28

Influencers' Equity
page 15

Legality of Amazon's Wristbands
page 19

OnDirect: Madeline Bernstein spcaLA
page 12

PLUS

DARK WEB CURRENCY

page 36

Bring It HOME

Los Angeles lawyers Paul Sczudlo and Megan Lisa Jones analyze provisions of the Tax Cuts and Jobs Act that relate to foreign income and investments

page 22

by Nina Marino, Jennifer Lieser, and Casey Clark

To shut down illicit dark web markets and their criminal currencies, the feds have been largely successful relying on old-fashioned police work

The Dark Side OF BITCOIN

[T]here is something special about Bitcoin that makes it inherently resistant to government control. It is built on code. It lives in the cloud. It is globalized and detached from the nation state, has no…institutional owner, operates peer to peer, and its transactions are inherently pseudonymous. It cannot be regulated in the same way as the stock market, government currency markets, insurance, or other financial sectors.[1]

So observed the editor of a liberterian publication in May 2013. Not long afterward, however, the U.S. Department of Justice began its active shutdown of dark web marketplaces and investigations into individuals who use and operate them. In October 2013, the FBI shut down Silk Road, the first and most famous market operating on the dark web—a series of websites accessible through a special browser that allows users and operators to remain anonymous. Since their inception, dark web marketplaces have been a platform for buying and selling illegal drugs in addition to any and all black market items. The founder of Silk Road, Ross Ulbricht, was convicted on charges of engaging in a continuing criminal enterprise (the Kingpin statute), narcotics trafficking, money laundering, and computer hacking.[2] He was sentenced to life in prison without the possibility of parole.[3]

Upon Silk Road's shutdown, dark web vendors and users relocated to other sites. The two largest successors, AlphaBay and Hansa Market, were recently shut down by law enforcement and their operators arrested.[4] In July 2017, when the founder and administrator of AlphaBay, Alexandre Cazes, was arrested, his laptop was open and logged into AlphaBay, allowing authorities to gain access to all of the website's hidden servers and financial accounts.[5] That same month, the U.S. Attorney's office issued a 21-count indictment against Alexander Vinnik, a Russian citizen believed to be the operator of the digital currency exchange, BTC-e, which handled more than $4 billion in unlicensed bitcoin exchanges as a means for laundering money.[6]

Nina Marino is a partner, and Jennifer Lieser and Casey Clark are attorneys, at Kaplan Marino in Beverly Hills. The firm specializes in complex criminal and white collar matters.

HADI FARAHANI

Money laundering prosecutions have long been an effective tool in the government's law enforcement arsenal. Attacking the criminal proceeds that sustain contraband operations on the dark web proves to be no exception.[7] During 2012 and 2013, when Silk Road was operational, the estimated value of the transactions was over $1.2 billion given the 2012-13 rate of bitcoin, with around 900,000 users per day worldwide.[8] A financial investigation into dark web marketplaces like Silk Road means going after Bitcoin and "examining the ways that individuals and criminal organizations earn, move, store, and launder their illicit proceeds."[9]

The once hidden and unregulated dark web is at the forefront of the government's investigative efforts. Of particular interest is the currency used to facilitate these dark web transactions: Bitcoin.

What is Bitcoin?

Bitcoin[10] is the most dominant form of decentralized convertible digital currency, or "cryptocurrency."[11] The Bitcoin network, created less than a decade ago, was conceptualized as a value transfer system.[12] Bitcoin was the first and is now the most widespread, readily accepted cryptocurrency; however, there are currently over 900 "Altcoins" or "virtual currencies."[13] Digital currency is generally defined as an electronically sourced unit of value that can be used as a substitute for fiat currency. The pseudonymous digital currency is not issued, nor is it backed, by any government, bank, financial institution, or company but is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.[14] Users maintain their bitcoin on an electronic wallet, which may be kept either on their computer or through an online wallet service such as Coinbase.[15] Each wallet is accessed using both the public and private key.[16] The public key operates in the same manner as a username or e-mail address and the private key as a password.

Bitcoin is not stored in any physical form, rather, it exists within a record of transactions. Its operation as a peer-to-peer network facilitates the creation and maintenance of a public ledger, known as the "blockchain." The blockchain is a public record of all Bitcoin transactions permanently maintained in chronological order. Each transaction is recorded on a block with both transactors' public keys (or wallet addresses) and is independently verified through a process called "mining."[17] Both parties authorize the transaction using their private keys.

While Bitcoin operates like money on a digital platform, it fails to meet the definition of currency. Money, as termed by the U.S. government, is "the coin and paper money of the United States or of any other country that [1] is designated as legal tender and that [2] circulates and [3] is customarily used and accepted as a medium of exchange in the country of issuance."[18] Bitcoin, on the other hand, is not financially backed or regulated by any governmental agency and transcends borders as a global currency solely operating on a peer-to-peer network.

Bitcoin, by its very design, makes it attractive for illicit transactions, so much so that it has been termed "criminal currency." Bitcoin has been viewed as a powerful tool for criminal activity because it can function as a means to move and store illicit funds while circumventing regulatory and law enforcement scrutiny.[19] Because it is not backed by any country or central bank, there is no central authority or oversight body. The difficulties in tracking and tracing funds create inordinate challenges for law enforcement as there are no readily accepted or widely recognized mechanisms to pinpoint the particular acts involved in laundering funds or to impede their progression.[20]

Bitcoin is characterized by its pseudonymous nature, which means that it is entirely anonymous other than the owner's public key on the blockchain—which can simply be changed with each transaction through the creation of a new account. Bitcoin transactions can be further camouflaged through the process of "bitcoin tumbling" or "bitcoin mixing," a process by which the user's bitcoin is sent through a complex series of dummy transactions in order to create a disconnect between the sender (user) and the receiver on the blockchain.[21] The user's privacy is safeguarded because Bitcoin is based entirely on and backed solely by peer-to-peer transactions, thus making law enforcement detection and investigation challenging. The individual's identity remains anonymous as long as the wallet address remains unconnected to its user.

Users of Bitcoin may access dark websites operating on The Onion Router, or TOR network, which is a publicly downloadable router network designed to conceal the Internet Protocol address for the users.[22] This network protects the privacy of its users and, in so doing, serves to conceal the identity and location of those using Bitcoin on the dark web. In fact, law enforcement typically orchestrate searches and takedowns to try to catch a suspect while he or she is working on a laptop. The second the laptop shuts, the information is likely encrypted and extremely difficult to retrieve.[23]

Dark web marketplaces, like Silk Road and AlphaBay, operate as a platform for buying and selling illicit goods and services. These dark web platforms conceptually emulate an actual marketplace with multiple vendors selling any illegal item imaginable. The government is fighting what seems to be a never-ending battle against these dark web marketplaces, for as one gets shut down, numerous others pop up to fill the void.

Often Bitcoin is the only source of currency used and accepted in these marketplaces. In order to convert funds that are generated by illicit activity from bitcoin to dollars, users utilize the services of a bitcoin exchanger. A licensed money transmitter is an unlikely option for those conducting business on the dark web because licensed money transmitters must comply with and report to the Financial Crimes Enforcement Network (FinCEN).[24] Unlicensed exchanges such as Alexander Vinnik's BTC-e allow users to maintain anonymity throughout the currency exchange process. In this type of transaction, both the user seeking to convert the currency as well as the unlicensed money transmitter are subject to criminal prosecution.

Regulatory Framework

The lack of a universal definition or conception for Bitcoin has forced each regulatory agency to classify it through the lens consistent within its own purview. Nevertheless, whether through a formal policy announcement or through a case of first impression, each of the four agencies has ultimately found that it can, indeed, regulate Bitcoin.

The most significant in terms of enforcement is FinCEN, a bureau within the U.S. Treasury Department that is charged with implementing, administering, and enforcing compliance with the Bank Secrecy Act (BSA)[25] and the first agency to address precisely how virtual currencies fit within its area of governance. Despite the fact that FinCEN distinguished virtual from real currency,[26] it still found that those who operate as administrators or exchangers of virtual currency are money services businesses (MSBs) and therefore subject to BSA regulations, including registration, reporting, and recordkeeping requirements.[27]

The other federal agencies serve to establish regulatory guidelines. The Internal Revenue Service classifies virtual currencies for federal taxation purposes as property,[28] similar to stocks and bonds as opposed to currency.[29] The Commodity Futures Trad-

ing Commission has determined that the definition of a commodity within the Commodities Exchange Act is broad enough to encompass Bitcoin.[30] Finally, the chairman of the Securities and Exchange Commission issued a December 2017 statement classifying cryptocurrencies as purported "items of inherent value (similar, for instance, to cash or gold) that are designed to enable purchases, sales and other financial transactions."[31]

The breadth of each regulatory agency's singular focus on oversight and regulation has as much potential to open doors to defenses as it does to close them. Despite the unique challenges arising from the inherent structure of Bitcoin—in addition to the need for international cooperation and the difficulties in obtaining user records—in November 2013, during a congressional hearing, the Department of Justice stated its intention to include Bitcoin within the current anti-money laundering regulatory framework.[32] Thus far in its regulation, the DOJ has relied upon its current—yet outdated—definitions of money services businesses and money transmission as well on anti-money laundering (AML) statutes that are also outmoded. The government targets dark web vendors who exclusively sell contraband in exchange for bitcoin and those who use unlicensed money transmitters to convert the bitcoin into cash.

Because of the decentralized nature of Bitcoin, the easiest and most effective way to regulate virtual currency is to regulate the bitcoin exchanges since these are subject to the BSA. The BSA requires financial institutions, namely MSBs, to assist government agencies in detecting and preventing money laundering.[33]

The enactment of the USA PATRIOT Act broadened the scope of the BSA with Title III of the act—the Intentional Money Laundering Abatement and Anti-Terrorist Financing Act of 2001—expanding the number of AML obligations imposed on money transmitters.[34] Among these requirements are AML compliance programs, customer identification programs, due diligence, mandatory information-sharing with federal law enforcement, and monitoring, detecting, and filing reports of suspicious activity.[35]

Money transmitters conducting exchanges with individuals on the dark web remain unlicensed in an attempt to avoid detection by and compliance with these stringent reporting requirements, opening themselves up to criminal culpability as an unlicensed money transmitter in violation of Section 1960 under Title 18 of the U.S. Code.

Typically, the money transmitter is distinct from the dark web vendor. The most common charging scheme involves prosecution of money laundering in violation of Sections 1956 and 1957 of the code. The criminal enterprise may be additionally prosecuted for conspiracy as well as the underlying criminal activity, which typically involves the distribution of controlled substances.[36]

Money Laundering Statutes

While Bitcoin operates like currency, it does not have the legal characteristics of real currency, namely, it does not have legal tender status. Therefore, it is not surprising that much of the current case law (of which there is very little and is almost exclusively prosecuted out of the New York district courts) focuses on the question of whether Bitcoin fits within the current constructs of the money laundering statutes.

In order to decide whether criminal activity involving Bitcoin may be prosecuted under the traditional money laundering statutes, the district courts have unanimously determined that the issue turns on whether the definition of Bitcoin falls within the ordinary meaning of "funds" as interpreted under Sections 1956 and 1960.

However, the courts diverge in their application of these statutes to Bitcoin and, more specifically, in what actually constitutes the ordinary meaning of "funds."

The line of cases stemming from *United States v. Ulbricht*[37] have determined that Bitcoin falls within the meaning of "funds" because "money" and "funds" are synonymous, and the general understanding of money is as a medium of exchange—to which Bitcoin qualifies,[38] thus making it subject to the money laundering statutes.[39] However, in *United States v. Petix*,[40] a magistrate judge in the Western District of New York determined the opposite, finding that Bitcoin does not fall within the ordinary meaning of "money" and therefore could not be prosecuted under the money laundering statutes because money gains its value from its connection to a sovereign power. Bitcoin, by design, is not backed by any country.[41] This divergence has the potential to open the door for creative defense attorneys.

Fifth Amendment: A Viable Defense?

Since cryptocurrencies have no centralized or regulatory authority, law enforcement face unique challenges in their investigative efforts and are commonly thwarted by serious impediments to obtaining transaction records as there is no financial intermediary to serve and process subpoenas or warrants.[42] While the public blockchain is always accessible to law enforcement without the necessity of probable cause to search or issue a subpoena, the only information recorded on the blockchain is the public key, not the private one containing personal identifying information.

The inherent structure of Bitcoin makes investigation difficult both in terms of tracking the criminal activity and in seizing the assets. The essential transaction records displaying evidence of criminal activity are stored within encrypted digital wallets outside the reach of the government. To access the information in the wallets, the government must issue a subpoena compelling the owner to turn over either his or her private key or a decrypted version of the wallet. However, compelling an individual to disclose his or her private key raises serious self-incrimination concerns.

The Fifth Amendment provides that "[n]o person…shall be compelled in any criminal case to be a witness against himself."[43] However, this protection is not absolute; it only "protects a person…against being incriminated by his own compelled testimonial communications."[44] For evidence to be testimonial in nature, and in turn implicate the self-incrimination clause of the Fifth Amendment, there must be an "attempt to force [an accused] 'to disclose the contents of his own mind.'"[45]

The specific self-incrimination implications for compelled disclosure of private keys to decrypt bitcoin wallets have yet to be addressed by the courts; nonetheless, apt parallels may be drawn with cases in which defendants have been compelled to divulge their decryption keys to their hard drives and/or computer files. Whether the Fifth Amendment may be triggered in these decryption cases is a fact-heavy analysis turning on whether the government is aware that the defendant has asserted ownership over the encrypted file.

Boucher Case

The first case to address this issue was *In re Grand Jury Subpoena to Sebastien Boucher* out of a Vermont district court in 2009.[46] Boucher was stopped by U.S. Customs and Border Protection officers who consequently found child pornography on his laptop—to which Boucher readily admitted ownership. Upon seizing the laptop, the government was unable to copy the hard drive containing the pornographic images because it was encrypted. When the government served Boucher with a subpoena to provide the decryption password, he moved to quash on the basis that production would violate his Fifth Amendment rights against self-incrimination.

The Vermont district court applied the foregone conclusion doctrine and determined that compliance with the subpoena

did not constitute compelled testimonial communication. Because Boucher had previously admitted ownership over the files to law enforcement, their existence and location were already known to the government. Therefore, the incriminating information was a foregone conclusion and the divulging of the password was not testimonial in nature.

A year later, a Colorado district court made the same finding in *United States v. Fricosu*.[47] After the government seized an encrypted computer pursuant to a search warrant, the subject of the investigation made a phone call to her incarcerated ex-husband during which she admitted ownership of the computer and knowledge of the password. The phone call was lawfully recorded by the prison facility and later discovered by the government. The court held that the existence of evidence, therefore, was again a foregone conclusion and thus not enough to trigger Fifth Amendment protection.

The *Fricosu* court, however, made clear that it was not ruling that there would never be a Fifth Amendment privilege against compelled disclosure of a password. Rather, the court indicated there are specific circumstances in which the government is already apprised of the suspect's ownership (in many cases because of the subject's own proactive assertion).[48]

The most recent case on compelled decryption comes out of a 2012 Eleventh Circuit decision and illustrates a set of facts in which the Fifth Amendment may properly be invoked.[49] While investigating John Doe for child pornography, the FBI seized his electronic devices, most of which contained encrypted files. The court ultimately upheld John Doe's argument that compelled disclosure would violate his right against self-incrimination because "by decrypting the contents, he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[50] The court found the decryption and production to be testimonial in nature and, given the facts of the case, the government was not already aware of the files' ownership and was thus unable to prove such evidence was a foregone conclusion.

The Eleventh Circuit employed a two-step analysis in reaching its conclusion: 1) determine if what the government seeks to compel is testimonial in nature, and then 2) determine whether the purported testimony is a foregone conclusion. When looking at the first prong, the court found that decryption and production were testimonial in nature because it was "tantamount to…his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[51]

In deciding whether the testimony was a foregone conclusion under prong two, the court developed two mechanisms in which the doctrine applies. The first consists in looking at the record as a whole to determine whether there is any indication that the government had knowledge as to the ownership of the existing files on the hard drive. In the second, without the government's knowledge of ownership, "the location, existence, and authenticity of the purported evidence [must be] known with reasonable particularity, [otherwise] the contents of the individual's mind [cannot be] used against him" in violation of the Fifth Amendment privilege.[52]

The court ultimately found that John Doe's testimony was not a foregone conclusion because the government was unable to demonstrate either knowledge of ownership or knowledge of the contents of the drives described with reasonable particularity, and, therefore, the protections afforded under the Fifth Amendment were viable.

It is inevitable that the government will seek to employ its subpoena power in future Bitcoin money laundering cases to compel the divulgence of private keys or decryption of digital wallets. While this is largely a fact-based analysis—given the inherent anonymity of Bitcoin—the strongest defenses may lie in challenging the government's lack of knowledge over ownership of the digital wallet and/or knowledge of the illicit transactions described with reasonable particularity. Without either, the foregone conclusion doctrine is inoperable, allowing suspected individuals to avail themselves of the protections afforded under the Fifth Amendment's self-incrimination clause.

Government's Tried and True Approach

Despite the unique challenges of catching and prosecuting dark web vendors and unlicensed money transmitters in the modern technological era, the government has nonetheless been largely successful in its reliance on old-fashioned police techniques. Because the vendors operating on the dark web marketplaces heavily encrypt their activities, these sites and their vendors' activities are nearly impossible for law enforcement to crack. Rather, law enforcement have had to rely upon old-fashioned, low-tech investigatory tools to infiltrate these criminal enterprises. Instead of being able to access the vendor's administrator dashboard to expose the internal operations and transaction history, law enforcement may attempt to track the physical packages containing illicit items by noting distinguishing features and/or unusual quantities of packages being shipped by a single individual or group of individuals.

Further techniques can include the cultivation of confidential informants (CIs) and cooperating witnesses as an entry point into the dark web enterprises. Cooperating witnesses are typically individuals with criminal exposure but minimal culpability with the respect to the larger scheme who can provide valuable insights into the functioning of the operation in exchange for leniency on a criminal sentence or no sentence at all.

Over time, some of these cooperating witnesses may also become CIs who operate on an undercover level while still perceptively maintaining their role in the larger criminal scheme. This is particularly effective with unlicensed money transmitters who, while criminally culpable, are viewed as less of a threat to society than the individuals running the illicit operations on the dark web. The unlicensed money transmitter can identify the individual with whom the exchange is being made and verify the deposit of bitcoin into his or her wallet, thus tying the particular vendor to a particular wallet. This provides the government with the ability to achieve two crucial investigative goals.

First, the unlicensed money transmitter may permit law enforcement to access his or her wallet, thereby showing the deposit of bitcoin into the wallet from a particular public key, which can then be traced back on the blockchain to show its source. This public key can be further used to identify prior transactions on the blockchain conducted by the same user. However, it should be noted that law enforcement's ability to trace these transactions on the blockchain may be hindered by the use of tumblers, thereby calling into question the government's ready assertion of its ability to do so.

The government is limited to the dark web vendor's bitcoin wallet that was used in a particular transaction with the CI. Given the fact that these vendors make every effort to obscure their activities, the bitcoin wallet the government is able to directly tie to them may be representative of only a small fraction of the wallets used by the dark web vendor. This severely cripples the government's ability to track and trace the full picture of the criminal proceeds, thereby limiting the government's charging ability.

Additionally, it is possible that once

the government becomes aware of the vendor's asserted ownership over a particular wallet, the government may then potentially be able to subpoena the vendor's decryption or private key, thereby circumventing the vendor's claim to Fifth Amendment protection.

While the inherent anonymity, use of tumblers, the inconsistency in regulatory definitions of the currency, the failure of Congress to step into today, and a host of other impediments, stand in the way of toppling dark web marketplaces that exist beyond the government's pale, the government has been able to compensate through the use of proven investigative techniques. Thus, essentially, the dark web marketplace and its vendors are nothing more than a modern criminal drug enterprise. ■

---

[1] Jeffrey Tucker, *Should Bitcoin Be Regulated Like Dollars?*, Laissez Faire (May 20, 2013), https://lfb.org/should-bitcoin-be-regulated-like-dollars.

[2] United States v. Ulbricht, No. 14-cr-00068 (S.D. N.Y. May 29, 2015), ECF No. 269 (Judgment in a Criminal Complaint).

[3] *Id.*

[4] Nathaniel Popper & Rebecca R. Ruiz, *2 Leading Online Black Markets Are Shut Down by Authorities*, N.Y. Times (July 20, 2017), *available at* https://www.nytimes.com.

[5] *Id.*

[6] United States v. Vinnik, No. 16-00227 SI (N.D. Cal. Jan. 17, 2017) (Motion to Seal Superseding Indictment), *available at* https://www.justice.gov/usao-ndca/press-release/file/984661/download.

[7] *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*: *Hearing Before the Comm. on Homeland Security and Governmental Affairs*, 113th Cong. 146 (2013) [hereinafter *Silk Road Hearing*]. In its most recent National Money Laundering Risk Assessment report, the U.S. Treasury estimated that more than $64 billion of the total $300+ billion generated through illicit finance was attributed to the trafficking of illegal drugs.

[8] *Id.*

[9] *Id.*

[10] Bitcoin is both a currency and a protocol. Throughout this article, the term "bitcoin," lower case, refers to the virtual currency that is digitally traded between users. "Bitcoin," when capitalized, refers to both the open source software used to create the virtual currency and the peer-to-peer network formed as a result.

[11] U.S. Dep't of Homeland Sec., Risks and Threats of Cryptocurrency (2014) [hereinafter DHS Report 2014]; Fin. Action Task Force, Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014) [hereinafter FATF Report 2014].

[12] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

[13] DHS Report 2014, *supra* note 11, at xi. Altcoin is the collective name for cryptocurrencies offered as alternatives to Bitcoin. The current market cap for cryptocurrencies is over half a trillion dollars.

[14] FATF Report 2014, *supra* note 11, at 5.

[15] coinbase Home Page, https://www.coinbase.com/about.

[16] Jay Palmer Fawcett, Bitcoin Regulations and Investigations: A Proposal for U.S. Policies 12 (2016) [hereinafter Fawcett].

[17] DHS Report 2014, *supra* note 11, at xi-xiii. Bitcoin miners are compensated with newly created bitcoin by verifying each transaction on the blockchain. *Id.* at xiii.

[18] 31 CFR §1010.100(m).

[19] DHS Report 2014, *supra* note 11, at 2.

[20] It appears law enforcement is turning to the use of third party vendor's source code to assist in their ability to track and trace these illicit transactions on the blockchain.

[21] Jon Matonis, *The Politics of Bitcoin Mixing Services*, Forbes (June 5, 2013), *available at* https://www.forbes.com; Joan Murphy et al., *Silk Road 101: How the "Darknet" Works*, USA Today (Jan. 27, 2015), *available at* https://www.usatoday.com/story/tech/2015/01/16/silk-road-ross-ulbricht/21824475.

[22] DHS Report 2014, *supra* note 11, at xiv.

[23] Nick Bilton, American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road (Portfolio 2017).

[24] *See infra* Financial Crimes Enforcement Network.

[25] FinCen, FinCEN's Mandate from Congress, https://www.fincen.gov/resources/fincens-mandate-congress.

[26] FinCen, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. "In contrast to real currency, 'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."

[27] *Id.*

[28] I.R.S. Notice 2014-21, 2014-16 I.R.B 938, Sec. 4, Q/A 1.

[29] *Id.* at Sec. 4, Q/A 7.

[30] *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 CFTC LEXIS 20, 2015 WL 5535736 (Sept. 17, 2015), *available at* https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.

[31] Public Statement, U.S. Securities and Exchange Commission, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017).

[32] Fawcett, *supra* note 16; *Silk Road Hearing*, *supra* note 7.

[33] 31 U.S.C. §§5311 et seq.

[34] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, §§301-77, 115 Stat. 296 (2001).

[35] *Id.*

[36] *See e.g.*, 18 U.S.C. §371; 21 U.S.C. §§841, 846.

[37] United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D. N.Y. 2014).

[38] *See e.g.*, United States v. Faiella, 39 F. Supp. 3d 544, 545 n.2 (S.D. N.Y. 2014).

[39] *See e.g., id.* at 544; United States v. Murgio, 209 F. Supp. 3d 698 (S.D. N.Y. 2016).

[40] United States v. Petix, No. 15-CR-227A, 2016 U.S. Dist. LEXIS 165955 (W.D. N.Y., Dec. 1, 2016).

[41] *Id.* at *18.

[42] DHS Report 2014, *supra* note 11, at 8.

[43] U.S. Const. amend. V.

[44] Fisher v. United States, 425 U.S. 391, 408 (1976).

[45] Doe v. United States, 487 U.S. 201, 211 (1988).

[46] In re Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009).

[47] United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Col. 2012).

[48] *Id.*

[49] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F. 3d 1335 (11th Cir. 2012).

[50] *Id.* at 1339-40.

[51] *Id.* at 1346.

[52] *Id.* at 1344.