Boston College Law Review

Volume 56 | Issue 5 Article 10

12-1-2015

Reaching Within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions

Alice Huang
Boston College Law School, alice.huang@bc.edu

REACHING WITHIN SILK ROAD: THE NEED FOR A NEW SUBPOENA POWER THAT TARGETS ILLEGAL BITCOIN TRANSACTIONS

Abstract: With the rise of Bitcoin and other virtual currencies, it has become crucial for government regulatory bodies to catch up. Black market sites like the now-defunct Silk Road have continued to exploit the anonymity of Bitcoin to engage in illegal transactions. In order to identify criminal Bitcoin users, the government must respond with an updated criminal subpoena standard that addresses virtual currencies. This Note argues that the gap should be filled by combining current e-discovery standards from Rule 26 of the Federal Rules of Civil Procedure with elements of the Digital Millennium Copyright Act's subpoena powers.

INTRODUCTION

In the increasingly public digital age, virtual currencies, such as Bitcoin, have become very attractive to those seeking online privacy.[1] Although some users purchase Bitcoin for the novelty value, others opt in because of the heightened confidentiality and security Bitcoin provides.[2] Bitcoin transactions are protected by electronic encryptions that ensure the user's identity is well

[1] *See* Derek A. Dion, Note, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y 165, 167 (explaining the decentralized nature of Bitcoin and its advantages); Jonathan Lane, Note, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 520 (2014) (noting that privacy is "integral" to Bitcoin's popularity); *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq [http://perma.cc/728R-U449] [hereinafter BITCOIN] (listing reasons why people trust and use bitcoins by highlighting the lack of third party reliance or control over the Bitcoin network); *see also* Prableen Bajpai, *The 5 Most Important Virtual Currencies Other Than Bitcoin*, INVESTOPEDIA (Dec. 10, 2014), http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-currencies-other-bitcoin.asp [http://perma.cc/ECW2-JCK6] (describing the benefits of other popular virtual currencies). Throughout this Note, the term "Bitcoin" refers to the virtual currency system, while the term "bitcoin" refers to the units of the virtual currency.

[2] Dion, *supra* note 1, at 169; *see* BITCOIN, *supra* note 1 (listing financial security and transparency among the benefits of Bitcoin); Cameron Graham, *Out of the Spotlight, Bitcoin Gains Legitimacy*, WIRED (Sept. 15, 2014, 2:34 PM), http://www.wired.com/insights/2014/09/bitcoin-gains-legitimacy/ [http://perma.cc/PC8H-2GKF] (analyzing the ebb and flow of interest in Bitcoin as the virtual currency's novelty value wears off).

hidden.[3] This anonymity not only prevents exploitation of user information and online activity, but it also allows many individuals to partake in easy and untraceable illicit transactions.[4] As a result, individuals who flock to Bitcoin use it for both legal and criminal purposes.[5]

The government has struggled to eliminate illegal Bitcoin marketplaces.[6] Despite shutting down Silk Road and arresting its operator, the government has been unable to reach the website's account holders.[7] Even though Silk Road has closed, other black market sites remain unfazed.[8] In-

[3] *See* Dion, *supra* note 1, at 168 (describing Bitcoin's use of a public key in order to maintain user anonymity); Lane, *supra* note 1, at 520 (explaining that Bitcoin's public key hides the user's identity); Jonathan B. Turpin, Note, *Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework*, 21 IND. J. GLOBAL LEGAL STUD. 335, 338 (2014) (stating that Bitcoin does not compromise user identity during transactions); *see also* Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13, 8 (2014) (calling Bitcoin's encryption-provided anonymity a challenge for law enforcement).

[4] *See* Trautman, *supra* note 3, at 2 (linking virtual currencies to a list of crimes facilitated by its anonymity benefits); Dion, *supra* note 1, at 169 & n.2 (discussing the ways in which users can conduct illegal transactions through Bitcoin exchanges); Lane, *supra* note 1, at 524 (acknowledging that Silk Road's anonymity is tied to its policy of solely accepting Bitcoin transactions).

[5] *See* Larry McIntyre, Staff Article, *Cyber-Takings: The War on Crime Moves into the Cloud*, 14 PITT. J. TECH. L. POL'Y 333, 342 (2014) (mentioning Bitcoin's ties to the black market website Silk Road); BITCOIN, *supra* note 1 (discussing the various businesses that accept Bitcoin payments and addressing the potential for illegal use).

[6] *See* McIntyre, *supra* note 5, at 343 (mentioning government monitoring of Silk Road); Joon Ian Wong, *Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust*, COINDESK (Oct. 6, 2014, 8:00 PM), http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust [http://perma.cc/PZ6M-P56W] (examining the impact of the government takedown of Silk Road on black market Bitcoin sites); *see also* Daniel Palmer, *How Deep Web Scams Helped Silk Road 2.0 Turn Crisis into Opportunity*, COINDESK (May 1, 2014, 3:23 PM), http://www.coindesk.com/dark-web-scams-helped-silk-road-2-0-turn-crisis-opportunity [http://perma.cc/S2A8-TVAT] (noting the continued proliferation of websites that promulgate black market Bitcoin transactions). Silk Road and Mt. Gox, two popular illegal Bitcoin marketplaces, are now defunct but many other black market websites remain operational in their place. *See* Palmer, *supra*.

[7] *See* McIntyre, *supra* note 5, at 344 (detailing the government's actions against the owner of Silk Road and the government's inability to reach individual users of the website); *see also* Press Release, U.S. Attorney's Office, S. Dist. of N.Y., Manhattan U.S. Attorney Announces Forfeiture of $28 Million Worth of Bitcoins Belonging to Silk Road (Jan. 16, 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php [http://perma.cc/5MJC-GYNQ] (indicating that the government prefers using civil forfeiture to target Silk Road users rather than attempting to unmask individual violators). Silk Road was one of the most prevalent online marketplaces that facilitated criminal Bitcoin interactions. *See, e.g.*, McIntyre, *supra* note 5, at 343 (identifying Silk Road as an underground market for illegal activity); Turpin, *supra* note 3, at 357–58 (describing Silk Road's illicit transactions); David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES (Jan. 18, 2014), http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html [http://perma.cc/94L6-ASCT] (characterizing Silk Road as "the world's largest and most notorious black market for drugs").

[8] *See* Palmer, *supra* note 6 (calling the shutdown of Silk Road an opportunity for other sites); *see also* JERRY BRITO & ANDREA CASTILLO, MERCATUS CTR., GEORGE MASON UNIV., BITCOIN: A PRIMER FOR POLICY MAKERS 25 (Dec. 19, 2013), http://mercatus.org/sites/default/files/Brito_

deed, many other replacement sites have appeared to fill the gap left by Silk Road.[9] Black market websites will continue to operate and exploit Bitcoin until the government begins to target the individual Bitcoin users who sell and purchase goods and services using these sites.[10]

To alleviate the problem of these illegal transactions, the U.S. Supreme Court and Congress must create a subpoena power that specifically aims to unmask the identity of individual Bitcoin users.[11] Without the ability to subpoena third parties to gain access to the documentation that identifies the Bitcoin users engaged in illegal transactions, the government will face difficulty in limiting the growth of illegal activity among Bitcoin users.[12] But, because of the lack of e-discovery standards in criminal litigation, targeting individual Bitcoin users may lead to an overreach of government power.[13]

BitcoinPrimer_v1.3.pdf [http://perma.cc/9E7L-RK48] (stating that Silk Road's shutdown did little to prevent other black market sites from flourishing).

[9] Palmer, *supra* note 6 (remarking that Silk Road's closure did not lead to the shutdown of other black market sites); Wong, *supra* note 6 (stating that a number of dark markets appeared after the government closed down Silk Road). *But see* BRITO & CASTILLO, *supra* note 8, at 25 (acknowledging that sites have opened hoping to replace Silk Road but pointing out that some have been unsuccessful and are now defunct due to internal security reasons).

[10] *See* Palmer, *supra* note 6 (illustrating that the government's takedown of Silk Road has not alleviated the problem of online marketplaces for illegal Bitcoin transactions); Wong, *supra* note 6 (describing the flourishing black market one year after Silk Road's demise).

[11] *See* BRITO & CASTILLO, *supra* note 8, at 25 (discussing the closure of some black market sites due to security issues rather than any governmental interference); Palmer, *supra* note 6 (indicating that the government has not been able to substantively prevent illegal Bitcoin transactions). *Compare* Press Release, U.S. Attorney's Office, *supra* note 7 (showing the government's indirect targeting of illicit Bitcoin use), *with* BITCOIN, *supra* note 1 (noting that it is possible for the government to directly target Bitcoin users abusing the virtual currency).

[12] *See* Palmer, *supra* note 6 (discussing the return of multiple new black market sites after the shutdown of Silk Road).

[13] Daniel B. Garrie et al., *"Criminal Cases Gone Paperless": Hanging with the Wrong Crowd*, 47 SAN DIEGO L. REV. 521, 527 (2010). *See generally* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (discussing a First Amendment right to anonymity). This Note does not address how the government should regulate the Bitcoin market to overcome its anonymity features. *See infra* notes 161–200 and accompanying text. For a discussion of the necessary regulatory measures, see Lane, *supra* note 1, at 553–56 (analyzing the financial regulations that state legislatures should impose upon Bitcoin wallet providers and exchanges). Once such regulations are in place, government entities will then have the ability to subpoena sites for access to Bitcoin user information. *See* I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (signaling the IRS's recognition of Bitcoin and indicating how general tax principles apply to virtual currency); FIN. CRIMES ENF'T NETWORK, DEP'T OF THE TREASURY, GUIDANCE: APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES, FIN-2013-G001, at 1–6 (Mar. 18, 2013), https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [http://perma.cc/7EWF-NNR9] (providing guidance on the applicability of FinCEN regulations to virtual currency users); *see also* Lane, *supra* note 1, at 554–55 (arguing that financial regulation of Bitcoin will help facilitate criminal investigations). It is unlikely legislators will focus on shutting down the entire Bitcoin network. *See* Jim Harper, *Bitcoin Foundation Lobbying*, BITCOIN FOUNDATION (July 9, 2014), http://bitcoinfoundation. org/forum/index.php?/topic/ 1043-bitcoin-foundation-lobbying/ [http://perma.cc/5XPD-7686] (positing that it is impossible to

Therefore, it is also necessary to create a standard limiting this new power—a standard that is tailored to ensure that the constitutional rights of Bitcoin users who are not engaged in illegal activity remain intact.[14]

In constructing a criminal subpoena standard, it is important to look to existing civil e-discovery rules, which address the use of electronically stored information.[15] Parties can look to Rule 26 and Rule 45 of the Federal Rules of Civil Procedure for guidance on the use of e-discovery.[16] Perhaps most importantly, these standards include limitations on e-discovery that rein in the moving party's ability to request a burdensome amount of information.[17] Furthermore, the Digital Millennium Copyright Act ("DMCA")

eliminate Bitcoin and implying that legislative action would only impede Bitcoin's growth); Timothy B. Lee, *Bitcoin Has Become Too Powerful for Regulators to Shut It Down*, VOX (Dec. 16, 2014, 2:20 PM), http://www.vox.com/2014/12/16/7403507/bitcoin-has-become-too-powerful-for-regulators-to-shut-it-down [http://perma.cc/8WTK-A4ZY] (arguing that regulators have been convinced to keep Bitcoin around); *see also* Jon Russell, *Coinbase Is Opening the First Regulated Bitcoin Exchange in the U.S.*, TECHCRUNCH (Jan. 25, 2015), http://techcrunch.com/2015/01/25/coinbase-us-bitcoin-exchange [http://perma.cc/E9NG-U27J] (reporting Coinbase's announcement that it will be opening a regulated Bitcoin exchange). *But see* Henry Farrell, *Bitcoin's Financial Network Is Doomed*, WASH. POST (Dec. 16, 2014), http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/12/16/bitcoins-financial-network-is-doomed [http://perma.cc/3Q3J-SFBA] (responding to Lee's contention that Bitcoin will succeed by arguing that government regulators will turn against the virtual currency). This Note will go through next steps once the government is capable of easily targeting individual users. *See infra* notes 161–200 and accompanying text.

[14] *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 314 (2010) (conflating money with speech through a discussion of how speakers have a First Amendment right to use money to fund political speech); *McIntyre*, 514 U.S. at 334 (indicating that anonymous speech rights are an important part of the First Amendment); Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) (holding that the First Amendment protects anonymous Internet speakers).

[15] Garrie et al., *supra* note 13, at 526–27.

[16] *See* FED. R. CIV. P. 26, 45 (providing the standards for e-discovery in civil litigation); Garrie et al., *supra* note 13, at 523 (analyzing the impact of e-discovery on criminal litigation and the need to regulate e-discovery in a criminal context); *see also* Steven C. Bennett, *E-Discovery: Reasonable Search, Proportionality, Cooperation, and Advancing Technology*, 30 J. INFO. TECH. & PRIVACY L. 433, 433 (2014) (discussing the application of discovery to electronically stored information). Congress updated the Rules of Civil Procedure on December 1, 2006, implementing the changes proposed by the Advisory Committee on Federal Rules of Civil Procedure—whose members are appointed by the U.S. Supreme Court. *See* FED. R. CIV. P. 26 advisory committee's note to 2006 amendment; FED. R. CIV. P. 45 advisory committee's note to 2006 amendment; Garrie et al., *supra* note 13, at 526 (indicating the amendments were a response to the growing need for regulation of e-discovery); *Committee Membership Selection*, U.S. CTS., http://www.uscourts.gov/rules-policies/about-rulemaking-process/committee-membership-selection [http://perma.cc/U62B-WXBJ] (providing an overview of how Rules Advisory Committee members are appointed); *How the Rulemaking Process Works*, U.S. CTS., http://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works [http://perma.cc/W62G-B7BT] (discussing the process for amendment of the Rules of Civil Procedure, the Rules of Criminal Procedure, and other federal rules). Rule 26 addresses general provisions governing discovery and Rule 45 regulates civil subpoena standards. FED. R. CIV. P. 26, 45.

[17] *See* FED. R. CIV. P. 26 (presenting limitations on the scope of e-discovery); *see also* Bennett, *supra* note 16, at 435–40 (reviewing two new limits on e-discovery: reasonableness and proportionality).

sets aside specific subpoena powers that allow plaintiffs to obtain the identities of anonymous Internet users from third parties.[18]

This Note argues that the U.S. Supreme Court and Congress should create a criminal subpoena standard to target Bitcoin users who abuse the virtual currency in illegal ways.[19] This standard should be broader than the subpoena powers within § 512(h) of the Digital Millennium Copyright Act but more restrictive than overall criminal subpoena powers to prevent abuse of subpoenas duces tecum.[20] Part I examines the development, functionality, and uses of Bitcoin as well as basic civil and criminal discovery standards.[21] Part II explores developments in e-discovery and how civil and criminal procedural rules address electronically stored information.[22] Part III argues that the U.S. Supreme Court and Congress should create a new criminal subpoena standard, modeled from current e-discovery laws, that targets criminal Bitcoin use but protects the constitutional rights of legitimate Bitcoin users.[23]

I. The New Gold Rush: The Rise of Bitcoin and Its Use and Abuse in the Criminal World

This Part discusses the rise of Bitcoin and its popularity in legitimate and criminal contexts.[24] Section A explains how to obtain bitcoins as well as the security features that allow Bitcoin to protect the anonymity of its users.[25] Section B addresses Bitcoin's various advantages and its increasing legitimacy.[26] Section C explores both the exploitation of Bitcoin and the events that led to the dissolution of Silk Road.[27]

A. Bitcoin and Other Virtual Currencies

Bitcoin is a type of virtual currency.[28] Many virtual currencies exist as computer files; similar to actual cash, virtual currency can be destroyed or

[18] *See* Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012) (detailing the subpoena standard under the DMCA); Patricia L. Bellia et al., Cyberlaw: Problems of Policy and Jurisprudence in the Information Age 408–11 (4th ed. 2011) (describing the use of the DMCA's § 512(h) subpoenas).

[19] *See infra* notes 161–200 and accompanying text.

[20] *See infra* notes 186–200 and accompanying text.

[21] *See infra* notes 24–95 and accompanying text.

[22] *See infra* notes 96–160 and accompanying text.

[23] *See infra* notes 161–200 and accompanying text.

[24] *See infra* notes 24–95 and accompanying text.

[25] *See infra* notes 28–57 and accompanying text.

[26] *See infra* notes 58–68 and accompanying text.

[27] *See infra* notes 69–95 and accompanying text. Silk Road was an underground black market that operated solely through the exchange of bitcoins. *See* McIntyre, *supra* note 5, at 342–43 (describing the misuse of Bitcoin on Silk Road).

[28] Turpin, *supra* note 3, at 339; *see also* Bajpai, *supra* note 1 (listing other common types of virtual currencies).

lost.[29] Typically, individuals exchange or transmit virtual currency over the Internet for goods or services and leave no physical trace of each transaction.[30] What separates Bitcoin from other virtual currencies is its adoption of peer-to-peer networking and cryptography.[31] As the first cryptocurrency, Bitcoin is decentralized and is not controlled by a bank or government entity.[32] It survives purely in an intangible electronic medium.[33]

In 2008, Satoshi Nakamoto created Bitcoin in response to rising worries about the amount of control governments have over traditional currencies.[34] A

[29] *See* Nikolei M. Kaplanov, Student Article, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 116 (2012) (explaining what Bitcoin is and how it works); CAL. DEP'T OF BUS. OVERSIGHT, WHAT YOU SHOULD KNOW ABOUT VIRTUAL CURRENCIES 1–2 (2014), http://www.dbo.ca.gov/Consumers/Advisories/Virtual_Currencies_0414.pdf [http://perma.cc/SS5U-SGWB] (defining virtual currency and clarifying the associated risks); *see also* Mike Belshe, *Are Consumer Bitcoin Balances Especially Vulnerable to Hacking?*, COIN CTR. (Dec. 1, 2014), http://coincenter.org/2014/12/consumer-safety [http://perma.cc/J6GW-AJJ2] (providing an overview of Bitcoin).

[30] *See* Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 442–43 (2014) (detailing how virtual currencies function); Dion, *supra* note 1, at 183 (emphasizing Bitcoin's intangible nature); Turpin, *supra* note 3, at 352 (promoting Bitcoin as an option that ameliorates the risks associated with physical currencies).

[31] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2012); *see* Bryans, *supra* note 30, at 443 ("Bitcoin is a decentralized, virtually anonymous (commonly called pseudonymous), peer-to-peer (transactions occur directly between users) network."). Cryptography is "the art or practice of writing in code or cipher." *Cryptography*, OXFORD ENG. DICTIONARY, http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography#eid [http://perma.cc/8PCR-TF74].

[32] Grinberg, *supra* note 31, at 162; BITCOIN, *supra* note 1 (confirming that Bitcoin is the first cryptocurrency); *accord* Mariella Moon, *A Brief Attempt at Explaining the Madness of Cryptocurrency*, ENGADGET (Jan. 21, 2015, 10:00 AM), http://www.engadget.com/2015/01/21/cryptocurrency-explainer/ [http://perma.cc/MH9K-JMRU] (providing information on cryptocurrencies in general); *see* Bryans, *supra* note 30, at 443 (outlining Bitcoin's decentralized structure); *Definition of Cryptocurrency*, COINPURSUIT, https://www.coinpursuit.com/pages/what-is-cryptocurrency/ [http://perma.cc/36BV-2ABH] (defining cryptocurrency as encrypted currency). Bitcoin is a cryptocurrency because it uses code for encryption protection. *See Cryptography*, *supra* note 31 (defining cryptography as "writing in code"); Kaplanov, *supra* note 29, at 117 (outlining Bitcoin's use of public key encryption).

[33] *See* Dion, *supra* note 1, at 167 ("Bitcoin is an electronic form of floating currency.").

[34] Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529, 530–31 (2014) (stating that these worries grew from distrust of centralized monetary authorities); Turpin, *supra* note 3, at 342 (citing the lack of government control as one of Bitcoin's attractive attributes). Nakamoto's actual identity remains uncertain; many posit that his name is merely an alias. *See* Lane, *supra* note 1, at 514 n.9 (reviewing the existing information on the Bitcoin creator); *see also* Bryans, *supra* note 30, at 444 n.19 (acknowledging Nakamoto as a pseudonym); Dion, *supra* note 1, at 167 n.11 (contending that Nakamoto is likely a pseudonym). Others contend Nakamoto is actually a group of individuals because it is seemingly impossible for a single person to have created something as complex as Bitcoin. Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED (Nov. 23, 2011, 2:52 PM), http://www.wired.com/2011/11/mf_bitcoin/ [http://perma.cc/YWJ5-DGRS] (examining different hypotheses on Nakamoto's identity).

year later, Nakamoto released Bitcoin, making it an open source code.[35] By allowing other developers to review and update the code, Nakamoto ensured that no single user could control or own the Bitcoin network.[36] Bitcoin can only operate if all users agree on the Bitcoin protocol.[37] This creates a strong sense of community for Bitcoin users and strengthens the idea that the people control Bitcoin as opposed to the government.[38] Unlike traditional currencies, which governments regulate and valuate using monetary policy, Bitcoin derives its worth solely from the open marketplace.[39]

In order to obtain bitcoins, users either "mine" for them or purchase them with real currency.[40] Bitcoin miners are paid in bitcoins for executing complicated computations that are essential for implementing Bitcoin transactions.[41] Bitcoin miners download a software program that allows them to connect to the Bitcoin network.[42] It also allows miners to verify Bitcoin trans-

[35] BITCOIN, *supra* note 1 (detailing the creation of Bitcoin); *see also* Lane, *supra* note 1, at 514–15 (stating that Nakamoto published Bitcoin code on the Internet).

[36] BITCOIN, *supra* note 1 (explaining who controls the Bitcoin network); *see also* Bryans, *supra* note 30, at 471 (emphasizing that Bitcoin does not depend on any single developer); Lane, *supra* note 1, at 515 (stating that the peer-to-peer nature of Bitcoin cuts out intermediaries and relies on trust within the Bitcoin community); Turpin, *supra* note 3, at 361 (indicating that Bitcoin's decentralized nature means it lacks a controlling entity).

[37] BITCOIN, *supra* note 1; *see* Pamela J. Martinson & Christopher P. Masterson, *Bitcoin and the Secured Lender*, BANKING & FIN. SERVS. POL'Y REP., June 2014, at 13, 14 (affirming that Bitcoin users have to adopt a single protocol). Similar to how different versions of a program have to be compatible with a computer's operating system to run properly, users of Bitcoin must maintain consistent iterations of Bitcoin. BITCOIN, *supra* note 1. Unless all users maintain the same version of the software, transactions would not work properly because the different versions would be incompatible. *Id.*

[38] *See* BITCOIN, *supra* note 1 (discussing the idea that Bitcoin users are incentivized to work in consensus); *see also* Bryans, *supra* note 30, at 471 (examining the longevity of Bitcoin due to its open source nature and active community).

[39] *See* Kaplanov, *supra* note 29, at 115 (detailing why users favor the virtual currency). For example, governments can inflate prices through increased cash production. *See* Grinberg, *supra* note 31, at 169 (looking at the Federal Reserve's ability to inflate the value of the dollar).

[40] *See, e.g.*, Penrose, *supra* note 34, at 531, 534 (discussing ways to mine and purchase bitcoins); Turpin, *supra* note 3, at 340 (mentioning how users can acquire bitcoins); BITCOIN, *supra* note 1 (specifying methods of obtaining bitcoins). Another alternative is to accept bitcoins as payment in a transaction. *See* Turpin, *supra* note 3, at 340; BITCOIN, *supra* note 1.

[41] *See, e.g.*, Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 17TH INTERNATIONAL CONFERENCE 34, 36–37 (Ahmad-Reza Sadeghi ed., 2013), http://book.itep.ru/depository/bitcoin/User_privacy_in_bitcoin.pdf [http://perma.cc/5E8A-98B4] (describing the payout of Bitcoin mining); Penrose, *supra* note 34, at 533 (discussing the incentives for a Bitcoin miner); BITCOIN, *supra* note 1 (explaining that Bitcoin networks reward miners for creating bitcoins). Thus, miners can sidestep the need to convert traditional currency into bitcoins. Penrose, *supra* note 34, at 531, 534 (describing the different ways to obtain bitcoins); BITCOIN, *supra* note 1 (providing mining as an alternative to using a Bitcoin exchange).

[42] Penrose, *supra* note 34, at 531–32 (detailing the mining process); *see* Turpin, *supra* note 3, at 341 (discussing how a user mines bitcoins).

actions.[43] For their efforts in reviewing and ensuring that transactions are valid, miners receive Bitcoin rewards for each completed block of transactions.[44] The miners' work ensures that no users are spending their bitcoins more than once.[45] This setup creates a system of self-regulation of Bitcoin use.[46]

Since mining is a complicated process, most individuals obtain bitcoins through purchase.[47] Users can buy bitcoins from a local cash exchange or an online Bitcoin exchange.[48] Similar to traditional currency exchange systems such as banks, they are third-party services that facilitate transfer of government-based currency for bitcoins.[49]

[43] Penrose, *supra* note 34, at 532–33; *see* Turpin, *supra* note 3, at 341 (discussing how a user mines bitcoins). Users employ an algorithm to solve a mathematical problem to add transactions onto blocks. *See* Penrose, *supra* note 34, at 532 (outlining the Bitcoin mining process). These block chains are made public to everyone on the Bitcoin network. *Id.*

[44] Penrose, *supra* note 34, at 533; Lane, *supra* note 1, at 519 (commenting on how Bitcoin incentivizes users to become miners).

[45] *See* Penrose, *supra* note 34, at 533 (stating that Bitcoin miners prevent "double spending" by rejecting transactions if the user's balance does not have sufficient funds); *see also* Lane, *supra* note 1, at 519 (asserting that miners prevent users from spending bitcoins more than once). This is known as "double spending." Penrose, *supra* note 34, at 533. Because Bitcoin transactions are public once they have been added to blocks, miners will be able to reject future transactions that attempt to use the same set of bitcoins again. *Id.* at 532, 533. This solves the need for third party involvement from a service such as PayPal to prevent double spending. BRITO & CASTILLO, *supra* note 8, at 4.

[46] *See* Penrose, *supra* note 34, at 533 (outlining the process Bitcoin miners use to verify transactions); *see also* BRITO & CASTILLO, *supra* note 8, at 6 (indicating that Bitcoin's protocol depends on miners to authenticate transactions and thus maintain the virtual currency's infrastructure).

[47] Penrose, *supra* note 34, at 534; *see* Kaplanov, *supra* note 29, at 121 (noting that using an online exchange is an alternate way of getting bitcoins).

[48] *See* Penrose, *supra* note 34, at 534 (explaining how users can obtain bitcoins through third-party exchange services); Kaplanov, *supra* note 29, at 121–22 (mentioning that users can use traditional currencies on exchange sites to get bitcoins). Local exchanges using cash add a degree of risk, as there is no guarantee a user will transfer the funds after receiving cash. Penrose, *supra* note 34, at 534; *see also* Kaplanov, *supra* note 29, at 123 (providing an example of a typical face-to-face exchange).

[49] *E.g.*, Grinberg, *supra* note 31, at 166 (discussing the creation and existence of online Bitcoin exchanges); Penrose, *supra* note 34, at 534 (explaining how Bitcoin exchanges function); Kaplanov, *supra* note 29, at 122 (listing various Bitcoin exchanges and their exchange policies). For a few years, Bitcoin transactions remained unregulated by the U.S. government. *See* Penrose, *supra* note 34, at 534 (acknowledging the lack of Bitcoin exchange regulation prior to the Financial Crimes Enforcement Network's guidance); Lane, *supra* note 1, at 531, 537 (analyzing the changes in financial regulatory structure to accommodate Bitcoin). As legal issues surrounding Bitcoin emerged, different sectors of the government began addressing virtual currencies. *See* I.R.S. Notice 2014-21, *supra* note 13 (advising on the taxation of virtual currencies); FIN. CRIMES ENF'T NETWORK, *supra* note 13 (providing guidance for following FinCEN regulations with regard to virtual currencies); Joon Ian Wong, *CFTC Chairman: We Have Oversight of Bitcoin Derivatives*, COINDESK (Dec. 11, 2014), http://www.coindesk.com/cftc-chairman-oversight-bitcoin-derivatives/ [http://perma.cc/Z5M8-QFWD] (reporting that the Commodity Futures Trading Commission has taken charge of regulatory oversight of Bitcoin); *see also* Penrose, *supra* note 34, at 529 (positing that FinCEN's regulatory measures are only the beginning and that more regula-

After obtaining bitcoins, individuals can spend the virtual currency in two different ways.[50] They can run a program on their own personal computer or use an account on a website to hold their Bitcoin "wallet."[51] Much like a regular wallet, this electronic wallet stores a user's virtual currency.[52] Bitcoin wallets use sets of encrypted keypairs—a public key and a private key—for security.[53]

A wallet's public key provides or receives payments while the buyer or seller retains the private key.[54] The public key acts as an address and provides information that any Bitcoin user will be able to access; however, only a Bitcoin user's private key can approve transactions.[55] Although the public key is traceable, it contains no user information.[56] Thus, by using only the public key to maintain transaction records, the owners of the addresses can remain anonymous.[57]

B. Advantages and Legal Uses of Bitcoin

Due to Bitcoin's growing popularity and its advantages over traditional payment methods, many businesses have begun accepting the virtual currency.[58] One crucial advantage is the payment freedom that Bitcoin pro-

tion is necessary to address a virtual currency as complex as Bitcoin). FinCEN is the U.S. Treasury Department's Financial Crimes Enforcement Network. BRITO & CASTILLO, *supra* note 8, at 2.

[50] Grinberg, *supra* note 31, at 162–63 (providing two methods of using bitcoins).

[51] *Id.*; *see* Bryans, *supra* note 30, at 446 (explaining how a digital wallet works); BITCOIN, *supra* note 1 (detailing how to make a Bitcoin payment). There are several programs users can utilize to run the Bitcoin protocol, which allows them to use their bitcoins in transactions. Grinberg, *supra* note 31, at 162 n.15.

[52] *See* Grinberg, *supra* note 31, at 163 (describing the wallet as a file where users store their bitcoins); Bryans, *supra* note 30, at 446 (discussing how an individual uses a wallet to make Bitcoin payments).

[53] *E.g.*, Dion, *supra* note 1, at 167–68 (analyzing the keypairs that make up a Bitcoin user's wallet); Lane, *supra* note 1, at 516 (explaining how Bitcoin software uses public and private keys); Kaplanov, *supra* note 29, at 117 (examining the public key encryption Bitcoin uses to ensure secure online transactions).

[54] *See* Dion, *supra* note 1, at 168 (analogizing the public key to an address and characterizing the private key as an authorization tool); Kaplanov, *supra* note 29, at 117 (describing how Bitcoin's public and private key system operates).

[55] Dion, *supra* note 1, at 168; Kaplanov, *supra* note 29, at 117; *see also* BRITO & CASTILLO, *supra* note 8, at 5 (explaining that a public key verifies that a Bitcoin user authorized a transaction with his or her private key).

[56] *See* BRITO & CASTILLO, *supra* note 8, at 8 (reiterating that the public key does not reveal an individual's identity); Dion, *supra* note 1, at 168 (emphasizing that having both public and private keys helps maintain a user's anonymity).

[57] *See* BRITO & CASTILLO, *supra* note 8, at 8 (clarifying that although user identity is not revealed by the public key, all transactions from that public key "address" are traceable, and thus once a key is linked to a user, the transaction history of that user becomes apparent); Kaplanov, *supra* note 29, at 117 (affirming that keypair encryptions maintain user privacy).

[58] *See* Dion, *supra* note 1, at 169; BITCOIN, *supra* note 1; COINMAP, http://coinmap.org [http://perma.cc/MS35-V6NW] (showing over 2000 businesses that accept Bitcoin as payment);

vides.[59] Transactions are instantaneous and borderless; unlike banks, which restrict users by business hours, holidays, and transfer limits, Bitcoin does not impose any limitations on the time, place, or amount of its transactions.[60] Furthermore, Bitcoin has very low transaction fees and sellers have the ability to bypass the usual cost of accepting a credit card payment.[61]

Bitcoin transactions are irreversible and do not involve any identifying personal information, which helps minimize fraudulent activity, prevent identity theft, and shield merchants from fraudulent chargebacks.[62] Some businesses value the additional security so much that they offer discounted rates

e.g., Pete Rizzo, *Industry Views: What Does Microsoft Mean for Bitcoin?*, COINDESK (Dec. 11, 2014, 10:55 PM), http://www.coindesk.com/industry-views-microsoft-mean-bitcoin [http://perma.cc/KY9D-TE69] (discussing Microsoft's announcement that it will accept Bitcoin payments for digital content purchases); Matthew Sparkes, *Britons Can Now Buy Dell Computers with Bitcoin*, TELEGRAPH (Feb. 22, 2015, 4:00 PM), http://www.telegraph.co.uk/technology/news/11425250/Britons-can-now-buy-Dell-computers-with-Bitcoin.html [http://perma.cc/H5AP-GKAA] (reporting Dell's decision to accept bitcoins in the United Kingdom and Canada, following its 2014 decision to allow Bitcoin payments in the United States as a result of a deal with payment processor Coinbase); Peter Vieth, *Law Firm Pioneers Use of Bitcoin*, VA. LAW. WKLY. BLOG (Feb. 16, 2015), http://valawyersweekly.com/2015/02/16/law-firm-pioneers-use-of-bitcoin [http://perma.cc/V3TN-VMQV] (relaying a law firm's decision to accept Bitcoin as payment). Non-profit organizations and charities such as WikiLeaks accept Bitcoin as a currency for donations. Dion, *supra* note 1, at 167–68; *see also* BRITO & CASTILLO, *supra* note 8, at 16 (identifying why Bitcoin is attractive to charities and organizations in need of funding). Braintree, a subsidiary of online electronic payment vendor PayPal, has also started letting its merchants accept bitcoins. Graham, *supra* note 2 (contending that this news increases Bitcoin's credibility with the public). Not only is Bitcoin popular with online sites, such as Reddit and WordPress, but it also has expanded offline to various businesses. BITCOIN, *supra* note 1 (discussing the rapidly increasing number of Bitcoin users and businesses); *see also* BRITO & CASTILLO, *supra* note 8, at 1 (noting that various types of business are beginning to accept Bitcoin payments). As of 2015, the value of bitcoins in circulation has exceeded $4.45 billion. *Bitcoin Network*, BITCOIN CHARTS, http://bitcoincharts.com/bitcoin [http://perma.cc/NW65-J3ZZ].

[59] *See* Trautman, *supra* note 3, at 38 (highlighting the instantaneous nature of Bitcoin); Turpin, *supra* note 3, at 337 (mentioning the ability to move bitcoins across borders); BITCOIN, *supra* note 1 (listing the advantages of using Bitcoin).

[60] *See* BITCOIN, *supra* note 1 (noting that Bitcoin provides many advantages in terms of payment freedom); *e.g.*, Trautman, *supra* note 3, at 38; Kaplanov, *supra* note 29, at 126 (describing the ease of moving bitcoins across jurisdictions); Turpin, *supra* note 3, at 337.

[61] *See* Kaplanov, *supra* note 29, at 172 n.385 (noting that the 1–2% fee merchants pay per credit card transaction results in higher prices for consumers); BITCOIN, *supra* note 1 (emphasizing a Bitcoin service's ability to implement lower fees than PayPal or a credit card company); *accord* BRITO & CASTILLO, *supra* note 8, at 10–11 (describing why Bitcoin's low transaction costs are attractive to users). These low transaction costs are especially attractive to many small businesses. *See* BRITO & CASTILLO, *supra* note 8, at 10.

[62] BRITO & CASTILLO, *supra* note 8, at 12 (explaining how Bitcoin solves the issue of chargebacks); Turpin, *supra* note 3, at 343 (stating that Bitcoin transactions eliminate chargebacks); BITCOIN, *supra* note 1 (mentioning this as a benefit to using bitcoins). Fraudulent chargebacks are "consumer-initiated payment reversals based on a false claim that a product has not been delivered." BRITO & CASTILLO, *supra* note 8, at 12. Since Bitcoin payments are not reversible, this problem is eradicated. *Id.*

for payment in bitcoins.[63] Those who dislike government-based currencies are also attracted to the security of Bitcoin without the barrier of third party control.[64]

One of the main reasons Bitcoin has become popular is the near anonymity it offers.[65] Users are virtually anonymous because its public key encryptions only reference the locations of bitcoins without disclosing any other information about the user.[66] In this sense, Bitcoin is analogous to cash.[67] Each transaction is neatly recorded but it becomes difficult for government officials to identify the individuals behind the transactions.[68]

[63] *See* BRITO & CASTILLO, *supra* note 8, at 12 (providing Greene Avenue Market as an example of a business that gives Bitcoin users a discount); Sarah Jenn, *Lawyer.com Gives Discounts for Bitcoin Transactions*, NEWSBTC (Aug. 6, 2015), http://www.newsbtc.com/2015/08/06/lawyer-com-gives-discounts-for-bitcoin-transactions/ [http://perma.cc/4WVL-8WTP] (reporting that Lawyer.com offers discounts for Bitcoin users because the virtual currency has helped the website reduce transaction costs).

[64] *See* BITCOIN, *supra* note 1 (emphasizing that a Bitcoin user has control over each transaction); *see also* Lane, *supra* note 1, at 515 (noting that Bitcoin removes intermediaries from a transaction).

[65] *See* Bryans, *supra* note 30, at 444–45 (comparing the near anonymity Bitcoin provides with the use of cash); Kaplanov, *supra* note 29, at 126 (citing Bitcoin's anonymity as an advantage that appeals to users); *see also* Dion, *supra* note 1, at 168 (detailing Bitcoin's virtually anonymous features). Although some users exploit Bitcoin's anonymity, others are taking advantage of financial privacy for legitimate reasons. *See* BRITO & CASTILLO, *supra* note 8, at 18 (listing reasons why people might need payment anonymity, including "[s]pouses fleeing abusive partners [who] need some way to discreetly spend money without being tracked," and [p]eople seeking controversial health services").

[66] *See* BRITO & CASTILLO, *supra* note 8, at 12 (explaining that Bitcoin is pseudonymous because its transactions are recorded and traceable even though a user's identity is not revealed by his or her public key); Dion, *supra* note 1, at 168 (establishing that although transactions are recorded, account holders stay anonymous); Kaplanov, *supra* note 29, at 117 (stating that public key encryption protects user identity); BITCOIN, *supra* note 1 (clarifying that bitcoins are only near anonymous because of the publicly accessible ledger of transactions that are recorded on the public key—even though the public key does not reveal any identifying user information). As bitcoins are exchanged between parties, the transactions are made public for authentication purposes but the only information linked to each transaction is the bitcoins' digital address. Kaplanov, *supra* note 29, at 126 (noting that while bitcoins reveal a digital address, they do not reveal user account information).

[67] Kaplanov, *supra* note 29, at 126 (comparing the use of bitcoins to cash transactions); *see* BRITO & CASTILLO, *supra* note 8, at 8 (detailing similarities and differences between Bitcoin and cash payments). Much like cash exchanges, when sellers and buyers use Bitcoin, they only exchange location and amount information. Kaplanov, *supra* note 29, at 126. The only difference is each user's public key saves and records his or her Bitcoin transactions, while cash can remain completely anonymous. BRITO & CASTILLO, *supra* note 8, at 8; *see* BITCOIN, *supra* note 1 (commenting on the records Bitcoin transactions leave behind).

[68] *See* Kaplanov, *supra* note 29, at 118–19 (calling the compilation of a Bitcoin block chain a "publicly available ledger"); Lane, *supra* note 1, at 530 (pointing to the low number of arrests of Silk Road users and concluding that the government is struggling with the complicated process of decrypting and uncovering Bitcoin transactions). Every computer on the Bitcoin network can access records of all Bitcoin transactions, back to the very first transaction. *See* Kaplanov, *supra* note 29, at 118; *see also* BRITO & CASTILLO, *supra* note 8, at 9 (acknowledging that these records

C. Illegal Uses of Bitcoin

Although Bitcoin has many benefits, it is also easily exploited for illegal uses.[69] Because Bitcoin allows individuals to engage in near anonymous and instantaneous monetary transactions, some have exploited the virtual currency for criminal use.[70] This abuse of the Bitcoin system has overshadowed legitimate Bitcoin use.[71]

Silk Road and its well-known black market dealings are a striking example of illegal Bitcoin use.[72] The now-defunct website operated as a marketplace that linked sellers and buyers in a similar fashion to eBay or Craigslist.[73] Unlike those legitimate websites, Silk Road provided users the opportunity to participate in illegal exchanges and in return pocketed a percentage of the sale price as commission.[74] A seller would create a listing of a good for sale and send the purchased item to the buyer upon receipt of an electronic payment.[75] Users could sell and obtain drugs, counterfeit IDs, stolen credit cards, and much more.[76] Silk Road also facilitated transactions

can go back for years). A timestamp records every time a user creates a bitcoin and every time a user exchanges bitcoins. Kaplanov, *supra* note 29, at 118.

[69] *See* McIntyre, *supra* note 5, at 343 (noting that Silk Road accepted only Bitcoin payments); Wong, *supra* note 6 (indicating that Bitcoin is the preferred payment on most dark market sites).

[70] *See* Trautman, *supra* note 3, at 7 (discussing the reasons why acting U.S. Assistant Attorney General Mythili Raman believed virtual currencies were used for illegal activity); Kaplanov, *supra* note 29, at 128 (pointing to the reasons why Bitcoin is enticing for those engaged in criminal activity).

[71] *See* BITCOIN, *supra* note 1 ("Bitcoin is money, and money has always been used both for legal and illegal purposes."); *see also* Palmer, *supra* note 6 (noting the proliferation of black market use of Bitcoin); Wong, *supra* note 6 (discussing the Bitcoin dark market since Silk Road closed).

[72] *See* McIntyre, *supra* note 5, at 342–43. A study showed that over the course of eight months between 2011 and 2012, Silk Road users exchanged 1.35 million bitcoins. Wong, *supra* note 6 (citing Nicholas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, *in* PROCEEDINGS OF THE 22ND INTERNATIONAL WORLD WIDE WEB CONFERENCE 213, 213–24 (2013)) (synthesizing the results of the aforementioned study). This only amounted to approximately 4.5% of bitcoins traded on other exchanges during that time, though that number likely increased as Silk Road's popularity grew in 2013. *See id.* ("Christin also found that at the time, 24,000 items were being sold on Silk Road over a six-month period. Contrast that to the 13,000 in drug listings alone on Silk Road that the [Digital Citizens Alliance] recorded in just one October day, before the bust.").

[73] United States v. Ulbricht, 31 F. Supp. 3d 540, 547 (S.D.N.Y. 2014) (identifying how the Silk Road website functioned); McIntyre, *supra* note 5, at 342–43.

[74] *Ulbricht*, 31 F. Supp. 3d at 547; McIntyre, *supra* note 5, at 343 (discussing the 8–15% commission that Silk Road retained for each illegal transaction).

[75] *Ulbricht*, 31 F. Supp. 3d at 549; *see* Lane, *supra* note 1, at 525 (enumerating the number and types of listings available on Silk Road); McIntyre, *supra* note 5, at 343 (providing examples of listings on Silk Road).

[76] *Ulbricht*, 31 F. Supp. 3d at 549–50 (denying Ulbricht's motion to dismiss his multi-count indictment for facilitating a list of illegal activities); *see* Trautman, *supra* note 3, at 6–15 (detailing various illicit uses of Bitcoin).

involving assassinations, hacker attacks against specific websites, sex trafficking, corporate espionage, and many other illegal activities.[77]

Silk Road accepted only Bitcoin payments and relied on Bitcoin's anonymity capabilities to prevent exposure of criminal activity.[78] Furthermore, only those who used an untraceable Internet browsing network were able to access the site.[79] During its first year of operation, Silk Road generated more than twenty-two million dollars of revenue.[80] Ross Ulbricht, the alleged owner and operator of Silk Road, did not directly sell items in the exchanges but profited off the illegal activities taking place on his website through commissions.[81] Overall, Ulbricht made over eighty million dollars during the two plus years he operated Silk Road.[82]

It took the U.S. government over two years to uncover the individual behind Silk Road.[83] Eventually, the FBI shut down Silk Road after successfully identifying Ulbricht as the owner and operator.[84] On October 1, 2013, the government apprehended Ulbricht and charged him with narcotics trafficking and money laundering conspiracies through creating and operating Silk Road.[85] The FBI seized the bitcoins stored on the website—not only Ulbricht's bitcoins, but also the bitcoins stored in every single Silk Road user

[77] *See Ulbricht*, 31 F. Supp. 3d at 550; Trautman, *supra* note 3, at 6–15.

[78] *See Ulbricht*, 31 F. Supp. 3d at 547 (explaining that Silk Road exclusively used Bitcoin payments due to Bitcoin's anonymity features); McIntyre, *supra* note 5, at 343 (describing the benefits of Bitcoin and stating that Silk Road capitalized on these benefits by requiring the site's users to pay with the virtual currency).

[79] *Ulbricht*, 31 F. Supp. 3d at 547 ("Ulbricht . . . made the site available only to those using Tor, software and a network that allows for anonymous, untraceable Internet browsing.").

[80] McIntyre, *supra* note 5, at 342 (citing Andy Greenberg, *Black Market Drug Site 'Silk Road' Booming: $22 Million in Annual Sales*, FORBES (Aug. 6, 2012, 2:28 PM), http://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales [http://perma.cc/8VXC-9TRK]).

[81] *See id.* (stating that Ulbricht did not personally sell anything on Silk Road); *see also Ulbricht*, 31 F. Supp. 3d at 550 (reiterating that Ulbricht was not being charged with participating on his own website by selling illegal substances).

[82] McIntyre, *supra* note 5, at 342; *see also Ulbricht*, 31 F. Supp. 3d at 550 (contending that Ulbricht received "tens of millions" of dollars in commission).

[83] *See* Martinson & Masterson, *supra* note 37, at 16 (attributing the slow movement of the FBI investigation to Bitcoin's anonymity); *see also* Segal, *supra* note 7 (mentioning that Silk Road was online for two-and-a-half years before Ulbricht was arrested).

[84] *See* Martinson & Masterson, *supra* note 37, at 16 (stating that the FBI shutdown Silk Road and arrested Ulbricht in October 2013); *see also* Segal, *supra* note 7 (chronicling the series of events that led to Ulbricht's arrest).

[85] *See Ulbricht*, 31 F. Supp. 3d at 540 ("Ulbricht conspired with narcotics traffickers and hackers to buy and sell illegal narcotics and malicious computer software and to launder the proceeds using Bitcoin."); Rachel Cruse, *Money Laundering, Narcotrafficking, and the End of the Silk Road Web Site*, 30 INT'L ENFORCEMENT L. REP. 1, 1 (2014) (reporting that Ulbricht was arrested and charged in a local library).

account.[86] Following seizure of the bitcoins, the government posted a notice of forfeiture.[87] No individual, other than Ulbricht, stepped forward to claim ownership of any of the twenty-eight million bitcoins taken from user accounts.[88]

The FBI was able to prosecute Ulbricht for starting Silk Road because he accidentally exposed his identity online.[89] The government found Ulbricht only after he posted his e-mail information on a Bitcoin discussion forum.[90] Although the government obtained a substantial amount of bitcoins used in illegal transactions on Silk Road, it was unable to identify the individuals who were committing the illegal acts.[91]

[86] McIntyre, *supra* note 5, at 344 (describing the government takedown of Silk Road and Ulbricht); *see* Press Release, U.S. Attorney's Office, *supra* note 7 (announcing civil forfeiture of Silk Road's seized funds).

[87] McIntyre, *supra* note 5, at 344; Press Release, U.S. Attorney's Office, *supra* note 7; *see also U.S. Marshals to Hold Another Bitcoin Auction*, U.S. MARSHALS SERV. (Feb. 18, 2015), http://www.usmarshals.gov/news/chron/2015/021815.htm [http://perma.cc/Q55P-7X4V] [hereinafter U.S. MARSHALS] (indicating the government's intent to auction off the seized bitcoins). By using civil forfeiture, the government was able to sidestep identifying and charging individual users of Silk Road. McIntyre, *supra* note 5, at 344. Civil forfeiture enables the government to take possession of property that is "an instrumentality of crime." *Id.* at 334 (citing Bennis v. Michigan, 516 U.S. 442, 453–55 (1996) (Thomas, J., concurring)). After obtaining the bitcoins in users' Silk Road accounts, U.S. Marshals began auctioning off the seized currency. *See* U.S. MARSHALS, *supra* (releasing details of the Bitcoin auction). The government used the seized bitcoins as stand-ins for defendants to support their conspiracy charges against Ulbricht. *See Ulbricht*, 31 F. Supp. 3d at 547 (analyzing the complicated legal issues in the government's case against Ulbricht in relation to his part in the alleged conspiracy charges); McIntyre, *supra* note 5, at 344–45 (detailing the government's argument that the bitcoins were defendants).

[88] *See* Partial Judgment by Default and Order of Forfeiture at 3, United States v. Ulbricht, No. 13 Civ. 6919 (S.D.N.Y. Jan. 15, 2014), http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2013cv06919/418116/19/0.pdf [http://perma.cc/ZT5Y-4RQQ] (stating that Ulbricht was the sole Silk Road user who attempted to claim his seized bitcoins); *see also* Press Release, U.S. Attorney's Office, *supra* note 7 (relaying news of the government's civil forfeiture seizure). Ulbricht had over $130 million in bitcoins on his computer. McIntyre, *supra* note 5, at 344; *see* Press Release, U.S. Attorney's Office, *supra* note 7.

[89] *See* Martinson & Masterson, *supra* note 37, at 16 (noting that Ulbricht revealed his identity accidentally through an Internet post); McIntyre, *supra* note 5, at 343 (detailing the mistakes that led to Ulbricht's exposure).

[90] Tim Hume, *How FBI Caught Ross Ulbricht, Alleged Creator of Criminal Marketplace Silk Road*, CNN (Oct. 5, 2013, 11:10 AM), http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht [http://perma.cc/R5RL-8X4B] (recounting the blunder that resulted in Ulbricht's arrest); *see also* Martinson & Masterson, *supra* note 37, at 16 (discussing the misstep that made Ulbricht vulnerable to the authorities).

[91] *See* McIntyre, *supra* note 5, at 344 (mentioning that the government gave up going after the actual owners of the bitcoins stored on Silk Road); *see also* Lane, *supra* note 1, at 530 (noting that the number of arrests was negligible when compared with the amount of Silk Road user accounts). It is likely not technologically feasible for the government to unmask each individual user because of the anonymity protections that Silk Road utilized. *See* McIntyre, *supra* note 5, at 344, 344 n.107 (citing the unmanageable number of Bitcoin users on Silk Road and the "impossible task of identifying each and every Silk Road user"). This will change as state legislatures continue moving in the direction of regulating Bitcoin exchange and wallet websites. *See* Request for Comment, Conference

The downfall of Silk Road was not the end of unlawful uses of Bitcoin.[92] Other competing sites rose up to take its place, including one site named Silk Road 2.0.[93] As such, the government's strategy to "take the profit out of crime and signal to those who would turn down the dark web for illicit activity that they have chosen the wrong path" seems to have been completely unsuccessful.[94] The return of these underground marketplaces for the exploitation of

of State Bank Supervisors, State Regulatory Requirements for Virtual Currency Activities: CSBS Draft Model Regulatory Framework and Request for Public Comment (Dec. 16, 2014), https://www.csbs.org/regulatory/ep/Documents/CSBS%20Draft%20Model%20Regulatory%20Framework%20for%20Virtual%20Currency%20Proposal%20--%20Dec.%2016%202014.pdf [http://perma.cc/327L-JN6X] (requesting comments from various institutions to give states recommendations on regulating Bitcoin); *see also* Letter from Robert A. Morgan, Dir. of Emerging Techs., Am. Bankers Assoc., to Emerging Payments Task Force, Conference of State Bank Supervisors (Feb. 16, 2014), http://www.csbs.org/regulatory/ep/Documents/ABA%20Framework%20Comment.pdf [http://perma.cc/3367-ZGAK] (discussing the movement toward state regulation of virtual currencies); Peter Van Valkenburgh, Coin Center, Comments to the Conference Of State Bank Supervisors on the Draft Model State Regulatory Framework for Virtual Currency 2–7 (2014), http://www.csbs.org/regulatory/ep/Documents/Coin%20Center%20Framework%20Comment.pdf [http://perma.cc/6HFK-DJWX] (surveying the current status of state regulation of Bitcoin). Currently, several states are making initial efforts to regulate Bitcoin. *See, e.g.*, Matthew E. Kohen, *Virtual Currencies & the Current State of the Law*, 33(9) Westlaw J. Comput. & Internet 1, *1–4 (2015), http://www.cfjblaw.com/files/uploads/Documents/Articles/WLJ_CMP_3309_Commentary_Kohen.pdf [http://perma.cc/P8YN-NS3N] (describing the current regulatory landscape of Bitcoin, highlighting Texas, New York, and Connecticut); Kurt Mattson, *Bitcoin Bills Making Their Way Through State Legislatures*, BSA/AML Update 2, Sept. 1, 2015 (on file with author) (summarizing pending legislation involving virtual currency); Eric Naing, *New York Issues Final Virtual Currency Rules*, CQ Roll Call Wash. Banking Briefing, June 4, 2015, 2015 WL 3503290 (reporting on the finalized version of New York's virtual currency regulations); Alan Zibel & Michael J. Casey, *New York Tries Again on Bitcoin Licensing*, Wall St. J. (Dec. 18, 2014), http://www.wsj.com/articles/new-york-bank-regulator-unveils-revised-bitcoin-licensing-plan-1418922084 [http://perma.cc/NCR8-WKUL] (detailing the proposal to require Bitcoin payment sites to obtain BitLicenses in order to operate); *accord* Cory Hester, *State Bank Regulators Release Model Virtual Currency Framework*, 33(9) Westlaw J. Comput. & Internet 2, *1–2 (2015) (discussing the Conference of State Bank Supervisors' September 2015 recommendation of a model framework for virtual currency regulation); Request for Comment, *supra* (emphasizing that state regulators are working to create adequate virtual currency legislation and requesting public commentary in order to generate the best regulatory structure); *see also* Van Valkenburgh, *supra* (noting that New York has decided to regulate virtual currency exchanges using a different framework than traditional exchanges). *But see* Craig Mehall, *Digital Currency Dealers Leave New York Market*, CQ Roll Call Wash. Banking Briefing, Aug. 14, 2015, 2015 WL 4776938 (revealing that some Bitcoin vendors have decided to leave New York rather than comply with new BitLicense regulations).

[92] Palmer, *supra* note 6 (discussing the sites that rose up to take over Silk Road's position); *accord* Wong, *supra* note 6 (describing the growth of "dark markets" since the Silk Road shutdown).

[93] *See* Palmer, *supra* note 6; Wong, *supra* note 6. In fact, Silk Road 2.0 has 5% more open listings for illegal drug transactions than Silk Road did when the FBI took down the site. Palmer, *supra* note 6.

[94] *See* Press Release, U.S. Attorney's Office, *supra* note 7 (describing the government's strategy to prevent virtual currency exploitation through civil forfeiture).

bitcoins demonstrates that the government cannot only target those who create and operate websites like Silk Road.[95]

II. Litigation in the Digital Age: How the Courts and Congress Have Addressed the Need for Revised Guidelines on E-Discovery

In order to create a criminal subpoena targeting the abuse of virtual currencies, the U.S. Supreme Court and Congress need to amend current standards to adequately address e-discovery.[96] To guide that discussion, this Part explores existing e-discovery standards.[97] Section A describes how the Federal Rules of Civil Procedure address electronically stored information.[98] Section B examines the Federal Rules of Criminal Procedure and how the current standards would apply to e-discovery.[99] Section C discusses the First Amendment implications of unmasking online speakers.[100] Section D explores the subpoena powers provided by the Digital Millennium Copyright Act for civil litigants.[101]

A. E-Discovery in Civil Litigation

In recognition of the digital age, the U.S. Supreme Court and Congress updated civil discovery rules to include litigant access to electronic information.[102] The new "e-discovery" standards encompass information that

[95] *See* Palmer, *supra* note 6.

[96] *See infra* notes 96–160 and accompanying text. Typically, the relevant Rules Advisory Committee will propose an amendment to the federal rules to the U.S. Supreme Court. *See How the Rulemaking Process Works*, *supra* note 16. The Court will promulgate the revision unless Congress rejects or revises the recommended changes. *Id.*

[97] *See infra* notes 96–160 and accompanying text.

[98] *See infra* notes 102–117 and accompanying text.

[99] *See infra* notes 118–138 and accompanying text.

[100] *See infra* notes 139–147 and accompanying text.

[101] *See infra* notes 148–160 and accompanying text.

[102] *See* 9A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2457 (3d ed. 2008) (providing background information on a subpoena duces tecum). Discovery is a fact-finding procedure that allows litigants to access material facts necessary to establish a cause of action. *See* Burke T. Ward et al., *Electronic Discovery: Rules for a Digital Age*, 18 B.U. J. SCI. & TECH. L. 150, 152 (2012) (comparing discovery rules under criminal and civil standards). The U.S. Supreme Court has promulgated rules of practice for discovery in federal courts. 2 LESTER B. ORFIELD, ORFIELD'S CRIMINAL PROCEDURE UNDER THE FEDERAL RULES § 16:10 (Supp. 2014). Rule 26 of the Federal Rules of Civil Procedure governs the standards of discovery in civil litigation and Rule 16 of the Federal Rules of Criminal Procedure dictates discovery standards in criminal cases. *See generally* FED. R. CIV. P. 26 (providing the duty to disclose and general provisions governing discovery in a civil lawsuit); FED. R. CRIM. P. 16 (detailing the discovery and inspection rules in a criminal case). These rules balance the necessity of discovery against the burdens of producing the requested information. Bennett, *supra* note 16, at 434–35. When determining the scope of discovery and the exact information that should be available to litigants, courts weigh the efficacy of expediting the process against the economic expense of information gathering. *See id.* (stating the goals of discovery). Discovery standards in criminal

exists in an intangible medium and can only be read on a computing device.[103] This broad category includes files saved on a computer as well as those located on the Internet.[104]

The sheer volume of available electronic data on a computer, tablet, or smartphone expands the wealth of information that parties can access through discovery.[105] Discovery has become much more expensive and onerous because of the expansion of discoverable materials from paper files to e-discovery.[106] Due to the sheer volume of available electronic information, companies could spend millions of dollars to remove privileged information or work product documents. [107]

In 2006, the U.S. Supreme Court and Congress addressed the growing need for e-discovery standards and amended the Federal Rules of Civil Procedure to include electronically stored information.[108] Amendments to Rules 26 and 45 added subsections that specifically incorporated new standards

cases tend to be narrower than those in civil lawsuits. *See* 2 ORFIELD, *supra*, § 16:11 (describing the differences between criminal and civil discovery).

[103] *See* Bennett, *supra* note 16, at 433–34 (emphasizing that the wide variety of electronic data makes it difficult to determine the scope of e-discovery rules); Ward et al., *supra* note 102, at 155 (describing the types of information that would be considered "electronic").

[104] *See* FED. R. CIV. P. 34 (describing the scope of e-discovery to include "writing, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations" that are "stored in any medium in which information can be obtained directly or, if necessary, after translation by the responding party into a reasonably useable form"); Ward et al., *supra* note 102, at 155 (including "email, web pages, word processing files, audio and video files, images, computer databases, [and] spreadsheets" in the list of included data).

[105] *See* Bennett, *supra* note 16, at 445–46 (stating that human review is improbable for cases dealing with massive amounts of electronic data); Ward et al., *supra* note 102, at 155 (discussing the volume of information that is accessible with electronic discovery in comparison with conventional paper discovery).

[106] *See* Bennett, *supra* note 16, at 438 (acknowledging the high cost of searching and analyzing obtained documents); Ward et al., *supra* note 102, at 184 (citing Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007)) (describing the expenses associated with e-discovery as potentially "outcome determinative").

[107] *See* Ward et al., *supra* note 102, at 170–71 (citing a study on costs associated with the review of data in the electronic discovery process that revealed "manual review of 30 gigabytes of data would cost up to $3.3 million"); *see also* Bennett, *supra* note 16, at 438 (stating that search and review are the priciest part of e-discovery).

[108] Garrie et al., *supra* note 13, at 526; Ward et al., *supra* note 102, at 179 (discussing the 2006 amendments to the Federal Rules of Civil Procedure); *see* FED. R. CIV. P. 26 advisory committee's note to 2006 amendment; FED. R. CIV. P. 45 advisory committee's note to 2006 amendment (noting that the 2006 amendments include e-discovery). The scope of traditional discovery in civil cases is fairly broad and allows parties to access relevant information that is "nonprivileged matter." *See* FED. R. CIV. P. 26(b) (presenting the scope and limitations on discovery); *see also* Ward et al., *supra* note 102, at 154 (describing the broad reach of discovery that can even extend beyond U.S. borders). This gives plaintiffs the ability to obtain "any matter relevant to the subject involved in the action" if they can show good cause. Ward et al., *supra* note 102, at 153.

regarding electronic data.[109] Rule 26(b)(2)(B) of the Federal Rules of Civil Procedure sets forth limitations upon discovery of electronically stored information.[110] In order to address cost concerns with potentially unreasonable e-discovery requests, Rule 26(b)(2)(B) emphasizes proportionality.[111] When considering these requests, courts tend to weigh cost, relevance, and efficiency; specific determinations are left to the discretion of the judge.[112]

In addition to traditional discovery, litigants can use subpoena powers to obtain information in a civil lawsuit.[113] This power, as set forth in Rule 45 of the Federal Rules of Civil Procedure, has also been amended to include e-discovery.[114] The process to obtain subpoenas duces tecum—a demand requiring recipients to provide requested documents—for electronically stored information remains in line with the treatment of traditional paper discov-

[109] Ward et al., *supra* note 102, at 179; *see also* Garrie et al., *supra* note 13, at 526 (describing the amendment as a result of requests for the rules to reflex the complicated nature of discovery of electronically stored information). *See generally* FED. R. CIV. P. 26, 45 (containing instructions on how to address discovery of electronic material). Congress also amended Rules 16, 33, 34, and 37 to address electronic data. *See id.* rr. 16, 33–34, 37.

[110] FED. R. CIV. P. 26(b)(2)(B); *see* Ward et al., *supra* note 102, at 179 (detailing how the 2006 amendment modified Rule 26 to include e-discovery).

[111] *See* Bennett, *supra* note 16, at 437 (stating that the Federal Rules require proportionality); Ward et al., *supra* note 102, at 170–71 (emphasizing the importance of weighing the burden and reasonableness of an e-discovery request when setting its scope).

[112] *See* Ward et al., *supra* note 102, at 171 ("If a party can prove that the request for documents is an 'undue burden' the court can consider 'cost-shifting' and a number of other factors to determine who must bear the cost."); *cf.* United States v. Int'l Bus. Machines Corp., 62 F.R.D. 526 (S.D.N.Y. 1974) (denying a subpoenaed third party the advancement of reasonable e-discovery costs because the third party, as a member of the public, would be among those affected by the outcome of the litigation and was therefore not simply a disinterested non-party).

[113] *See* Ward et al., *supra* note 102, at 179 (listing Rule 45 as one of the discovery standards that have been updated to address electronically stored information); Michael J. Martin, Note, *The Discoverability of E-Mails: The Smoking Gun of the Modern Era*, 7 U. MASS. L. REV. 182, 196 (2012) (discussing the use of Rule 45 in discovery to obtain emails from third parties); *see also* United States v. Crosland, 821 F. Supp. 1123, 1129 (E.D. Va. 1993) ("[T]he term 'subpoena,' most often encountered in the civil practice or grand jury context, carries with it a strong connotation of 'discovery.'").

[114] FED. R. CIV. P. 45(a) (permitting a subpoena duces tecum to request production of electronically stored information); *see also* Martin, *supra* note 113, at 196 (discussing the amendment of Rule 45 to include electronically stored information). Under Rule 45(a)(1) of the Federal Rules of Civil Procedure, a subpoena can command the recipient to "permit inspection, copying, testing, or sampling of the materials." FED. R. CIV. P. 45(a)(1)(D). Although most limitations on subpoenas duces tecum in civil litigations mirror the ones in criminal cases, there are some additional limits on a civil litigant's ability to obtain a subpoena. *See id.* r. 45(d) ("Protecting a person subject to subpoena . . . ."); FED. R. CRIM. P. 17(c)(2) (stating that a court can choose to quash a subpoena). One of the restrictions in Rule 45(a)(4) requires the moving party to provide prior notice before serving a subpoena duces tecum. FED. R. CIV. P. 45(a)(4). This gives the other party a chance to object and time to file a motion to quash the subpoena. *See* Phalp v. City of Overland Park, No. 00-2354-JAR, 2002 WL 1162449, at *3 (D. Kan. May 8, 2002) (referring to why the prior notice subsection of Rule 45 exists).

ery.[115] Rule 45 requires additional specification within the subpoena regarding how the electronic documents should be produced.[116] Furthermore, the notice restriction on subpoenas duces tecum for documents and tangible things carries over to e-discovery as well.[117]

B. Subpoenas Duces Tecum in Criminal Litigation

In contrast to the updated Federal Rules of Civil Procedure, which have clear-cut procedures on how to deal with electronically stored data, the Federal Rules of Criminal Procedure have not been updated to specifically address these technological developments.[118] For now, since the standard remains unchanged, the government can often easily obtain a grand jury subpoena for electronic material.[119] Rule 17 of the Federal Rules of Criminal Procedure sets forth the standard subpoena process.[120]

[115] *See* FED. R. CIV. P. 45(a)(1)(C)–(D) (adding electronically stored information to the rule); *see also* A. WALLACE TASHIMA & JAMES M. WAGSTAFFE, CALIFORNIA PRACTICE GUIDE: FEDERAL CIVIL PROCEDURE BEFORE TRIAL § 11:2254 (2015) (stating that a party can produce a subpoena duces tecum for electronically stored information). Litigants can issue a subpoena duces tecum in order to compel the recipient, whether it is the opposing party or a third party, to produce documentary evidence and objects. FEDERAL PROCEDURAL FORMS § 20:495 (West 2015).

[116] FED. R. CIV. P. 45(a)(1)(C) ("A subpoena may specify the form or forms in which electronically stored information is to be produced."); *see* TASHIMA & WAGSTAFFE, *supra* note 115, § 11:2240 (describing different possibilities for production, including production with or without a deposition).

[117] *See* FED. R. CIV. P. 45(a)(D)(4) (outlining the standard for notice to other parties before service); TASHIMA & WAGSTAFFE, *supra* note 115, § 11:2251 (citing Biocore Med. Techs., Inc. v. Khosrowshahi, 181 F.R.D. 660, 667 (D. Kan. 1998)) (emphasizing the notice requirement).

[118] Garrie et al., *supra* note 13, at 527; *see also* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543, 552 (2011) (asserting that unlike the civil rules, criminal rules and cases do not provide much guidance for electronically stored information). In the criminal context, the traditional discovery rule focuses on the defendant's ability to gain access to the material documents that the government has gathered. *See* FED. R. CRIM. P. 16 (detailing the materials from the government's case that are subject to disclosure). Although defendants face stricter limitations, there are also restrictions on the government's use of discovery in a criminal case. *See* 2 ORFIELD, *supra* note 102, § 16:11 (citing Degen v. United States, 517 U.S. 820 (1996); Chao v. Fleming, 498 F. Supp. 2d 1034, 1041 (W.D. Mich. 2007)) (discussing cases that show how courts apply discovery restrictions in criminal cases with regard to defendants as well as the government). For example, courts are willing to stay civil proceedings that are filed in connection with a pending criminal case. *See id.* (describing the necessity of not "expos[ing] the defendant's theory to the prosecution in advance of trial"). By granting a stay, courts stop the government from taking advantage of the more lenient civil discovery rules to figure out a defendant's planned defenses in the criminal case. *See id.* ("[The court has authority] to prevent parties from using civil discovery to evade restrictions on discovery in criminal cases."). In addition to prejudicing the criminal case, denying a stay might lead to self-incrimination, which infringes upon a defendant's Fifth Amendment rights. *Id.*

[119] *See* FED. R. CRIM. P. 17 (detailing the current criminal subpoena standards); *cf.* Ward et al., *supra* note 102, at 160 (addressing the criminal electronic discovery by mentioning potential spoliation concerns that may arise with grand jury subpoenas); Kelly E. Stavnes, Note, *Anonymity Protection Versus Subpoena Compliance: What Media Companies Should Consider When De-*

In criminal cases, the government can use subpoenas duces tecum to gain information or documents regarding anything that would be admissible into evidence.[121] The U.S. Supreme Court has established three elements that the moving party has to meet.[122] First, the information must be relevant; this requires courts to analyze the scope and purpose of the request on a case-by-case basis.[123] Second, the information must be admissible, though courts apply a more lenient application of the Federal Rules of Evidence because this

fending User Comments Online, 36 J. CORP. L. 697, 704 (2011) (discussing whether grand jury subpoenas can require reporters to disclose their sources).

[120] FED. R. CRIM. P. 17; *see* 1 ORFIELD, *supra* note 102, § 6:89 (analyzing the scope of subpoena duces tecum in a criminal context).

[121] FEDERAL PROCEDURAL FORMS, *supra* note 115, § 20:495; *see* Gruenspecht, *supra* note 118, at 547 (explaining the long reach of the government with a subpoena duces tecum in a criminal case). A subpoena duces tecum compels a witness to "produce any books, papers, documents, data, or other objects the subpoena designates." FED. R. CRIM. P. 17(c)(1); *see also* United States v. Re, 313 F. Supp. 442, 448 (S.D.N.Y. 1970) ("[A] subpoena duces tecum is generally a legitimate means by which the government may obtain records and documents relevant to criminal investigations or proceedings."). Civil subpoenas requesting document production are sometimes equated with discovery, but in the criminal context, subpoenas duces tecum are more restrictive. *See Crosland*, 821 F. Supp. at 1129 (describing the differences between a civil and criminal subpoena duces tecum). Criminal subpoenas are not used for discovery but are rather meant to allow a party to compel specific relevant documents. *Id.*; *see also* United States v. Green, 857 F. Supp. 2d 1015, 1017 (S.D. Cal. 2012) ("Federal Rule of Criminal Procedure Rule 17(c) is not intended to provide a means of discovery for criminal defendants.").

[122] *See* United States v. Nixon, 418 U.S. 683, 700 (1974) (articulating the three elements for obtaining a subpoena duces tecum); *see also* United States v. Binday, 908 F. Supp. 2d 485, 492 (S.D.N.Y. 2012) (reiterating that the *Nixon* standard places these three limitations on subpoenas). In reaching the three-pronged test, the Court referenced a test established by the District Court of the Southern District of New York in *United States v. Iozia* in 1952. *Nixon*, 418 U.S. at 699; United States v. Iozia, 13 F.R.D. 335, 338 (S.D.N.Y. 1952); *see also Binday*, 908 F. Supp. 2d at 492. In *Iozia*, the district court created a test that allowed the government or a defendant to require production once they showed that: (1) the information is admissible into evidence; (2) the information cannot be otherwise accessed prior to trial through reasonable efforts; (3) the information is necessary in order to properly prepare for trial and lacking these materials could lead to unreasonable delays; and (4) the subpoena has been requested in good faith. *Iozia*, 13 F.R.D. at 338; *see Nixon*, 418 U.S. at 699–700 (referring to the standard that most cases have adopted and creating three hurdles in addition to the ones created in *Iozia*).

[123] *See* Packwood v. Senate Select Comm. on Ethics, 510 U.S. 1319, 1320–21 (1994) (setting a lower bar for pretrial subpoenas duces tecum); Kerr v. U.S. Dist. Court for N. Dist. of Cal., 426 U.S. 394, 399 (1976) (determining that relevancy is broader during discovery than it is at trial).

is a pretrial evaluation.[124] Lastly, the request must be specific, precisely pinpointing the requested documents.[125]

It is generally fairly easy for the government to obtain subpoenas duces tecum.[126] Often times, the government utilizes a grand jury to expedite the issuance of the subpoena.[127] This inquisitorial power is uncertain and its limitations have not been fully established by statute, but it is not restricted by the same considerations that a general subpoena duces tecum would be.[128] Courts are more lenient in allowing the government's grand jury subpoena to move forward.[129]

[124] *See Nixon*, 418 U.S. at 699 (considering the evidentiary value of the request); *see also* Bourjaily v. United States, 483 U.S. 171, 172 (1987) (setting limits on the applicability of the Federal Rules of Evidence to pretrial inquiries). *Nixon* was decided before the implementation of the Federal Rules of Evidence. *See Bourjaily*, 483 U.S. at 172. The U.S. Supreme Court has not expanded upon the admissibility requirement beyond determining that Rule 104 of the Federal Rules of Evidence does not limit pretrial inquiries to the rules of evidence with the exception of restrictions due to privileges. *Id.* (determining that hearsay does not matter in a pretrial inquiry).

[125] *See* Cheney v. U.S. Dist. Court for D.C., 542 U.S. 367, 387 (2004) (interpreting *Nixon*'s specificity prong to require a narrow and targeted subpoena request); *Nixon*, 418 U.S. at 699 (identifying certain enumerated documents within the subpoena).

[126] *See* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041 at *46 (S.D.N.Y. Apr. 4, 2007) (allowing the prosecution to request digital document production for all corporate records because the court found them "relevant" to the fraud claim at issue); Gruenspecht, *supra* note 118, at 552 (citing the few cases where subpoena requests had been challenged and acknowledging that most third parties do not dispute government requests); *see also* United States v. Jannuzzio, 22 F.R.D. 223, 228 (D. Del. 1958) (declining to allow a defendant's subpoena duces tecum request because of a lack of evidentiary value).

[127] *See* Application of Tex. Co., 27 F. Supp. 847, 850 (E.D. Ill. 1939) (acknowledging that a grand jury can subpoena documents in its investigation); Gruenspecht, *supra* note 118, at 547 (discussing the statutory scope of a grand jury subpoena).

[128] United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (holding that *Nixon* does not apply to grand jury proceedings because inquiries into relevancy and admissibility would result in cumbersome delay); *Application of Tex. Co.*, 27 F. Supp. at 850–51 ("Beyond the briefest implications contained in the statutes, the Congress has not seen fit to define the jury's power, or to designate the exact limitations upon it."); *see also* Gruenspecht, *supra* note 118, at 547 (describing the constitutional bounds of a grand jury subpoena as "somewhat vague"). This relegates responsibility to the court's discretion "upon a particular set of facts and circumstances . . . just how far a grand jury may properly go or should be allowed to go." *Application of Tex. Co.*, 27 F. Supp. at 850–51. In the past, courts have permitted subpoenas duces tecum even when the recipient is not the owner of the materials sought but merely possesses them. *See* Burdeau v. McDowell, 256 U.S. 465, 476 (1921) (stating that even if incriminatory documents were in the hands of someone other than the accused, a subpoena could be issued for the production of those papers); *Re*, 313 F. Supp. at 449 ("[S]ervice of a subpoena duces tecum on a person in possession of records belonging to another is proper."). Under certain circumstances, the subpoena can even reach U.S. citizens on international soil. *See* FED. R. CRIM. P. 17(e)(2) (citing 28 U.S.C. § 1783, which governs service of a subpoena in a foreign country).

[129] *See In re* Zuniga, 714 F.2d 632, 642 (6th Cir. 1983) (allowing the subpoena because the grand jury provides a "veil of secrecy"); *Jannuzzio*, 22 F.R.D. at 228 ("A Court should be liberal in a criminal action in holding documents to be evidentiary for the purpose of permitting a party to obtain their production at trial by subpoena."); *see also Application of Tex. Co.*, 27 F. Supp. at 851–52 ("Congress has not seen fit to define the jury's power or to designate exact limitations

The government does face some restrictions on its use of subpoenas duces tecum.[130] A court can deem the subpoena terms to be unreasonable or oppressive and require modification of its terms or quash it entirely.[131] Since the government can subpoena a recipient for documents they do not own, both the recipient and the owner of the requested materials can file a motion to quash the subpoena.[132] It is difficult, however, to quash a subpoena because the recipient bears the burden of proving the government's request is unreasonable.[133]

Another restriction disallows the subpoena power to "violate a valid privilege," which includes infringements upon constitutional rights.[134] If the recipient of the subpoena makes a legitimate constitutional claim, the government must overcome the level of scrutiny protecting such a claim.[135] The court will review the government interest against the recipient's interest and decide whether it will throw out the subpoena.[136] The burden is on the government to show that the subpoena should move forward and can reach the recipient de-

upon it."); 8A BARBARA J. VAN ARSDALE ET AL., FEDERAL PROCEDURE, LAWYERS EDITION § 22:446 (2015) (detailing the requirements of a subpoena for pretrial production of documents).

[130] *See Nixon*, 418 U.S. at 698 (addressing limitations on subpoenas duces tecum set forth in the Federal Rules of Criminal Procedure Rule 17); *In re Zuniga*, 714 F.2d at 636 (citing United States v. Calandra, 414 U.S. 338, 346 (1974)) (discussing the limits on grand jury subpoenas); *see also* Margoles v. United States, 402 F.2d 450, 451 (7th Cir. 1968) (providing courts the discretion to reject subpoenas duces tecum).

[131] FED. R. CRIM. P. 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."); *see Nixon*, 418 U.S. at 698 (reiterating that Rule 17(c) does not allow for oppressive or unreasonable subpoena requests).

[132] 1 ORFIELD, *supra* note 102, § 6:89.

[133] *See R. Enters., Inc.*, 498 U.S. at 301 (discussing the standard of proof in a motion to quash a subpoena); *see also In re* Grand Jury Proceedings, 616 F.3d 1186, 1201 (10th Cir. 2010) (applying the *R. Enterprises, Inc.* standard when considering a request to quash); *In re* Grand Jury, 111 F.3d 1066, 1075 (3d Cir. 1997) (citing and applying *R. Enterprises, Inc.*). In 1991, in *United States v. R. Enterprises, Inc.*, the U.S. Supreme Court interpreted Rule 17(c) to give the government the presumption that the grand jury subpoena was reasonable. 498 U.S. at 301. The Court emphasized the language of the rule, which only allows a subpoena to be quashed if compliance is unreasonable. *Id.*

[134] *Calandra*, 414 U.S. at 346. The Court pointed to cases where a criminal subpoena would have violated defendants' Fourth and Fifth Amendment rights. *Id.* (citing Hale v. Henkel, 201 U.S. 43, 76 (1906); Boyd v. United States, 116 U.S. 616, 631 (1886)).

[135] *See In re* Grand Jury 87-3 Subpoena Duces Tecum (*In re Grand Jury*), 955 F.2d 229, 231 (4th Cir. 1992) (citing Branzburg v. Hayes, 408 U.S. 665 (1972)) (deciding that when a defendant has established a prima facie case, the burden of proof moves to the government); *In re* Subpoenas Served upon Wood (*In re Wood*), 430 F. Supp. 41, 45 (S.D.N.Y. 1977) (citing *Branzburg*, 408 U.S. 665) (stating that the burden shifts onto the government when a valid First Amendment claim has been made).

[136] *See In re Grand Jury*, 955 F.2d at 234 (citing *Branzburg*, 408 U.S. at 709–10 (Powell, J., concurring)) (discussing Justice Powell's opinion in *Branzburg v. Hayes*, which indicated the need for courts to balance governmental interests with possible constitutional infringements); *In re Wood*, 430 F. Supp. at 47 (considering whether governmental interests outweighed defendant's constitutional rights).

spite potential constitutional protections.[137] When dealing with electronically stored information, courts will likely come across First Amendment issues.[138]

C. First Amendment Rights at Issue in E-Discovery

The First Amendment, which provides a constitutional right to free speech, likely covers anonymous online speech.[139] In 1995, in *McIntyre v. Ohio Elections Commission*, the U.S. Supreme Court reaffirmed that the

[137] *See In re* Grand Jury Proceedings, 443 F. Supp. 1273, 1277 (D.S.D. 1978) (detailing the requirements for the government to "lawfully penetrate a constitutionally protected area"). To prove that the subpoena is still lawful, the government must meet four considerations: (1) the grand jury investigation is lawful; (2) a legitimate purpose exists for the grand jury investigation; (3) the grand jury subpoena is seeking relevant information or documents; and (4) the government's interest holds up against the level of scrutiny applied upon the infringement of the recipient's constitutional rights. *Id.* at 1277–78.

[138] *See* Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) (discussing First Amendment protection of online anonymous speech). Although this Note focuses on potential First Amendment concerns, courts also encounter Fourth Amendment arguments when dealing with electronically stored information. *See* United States v. Sawyer, 786 F. Supp. 2d 1352, 1353–54 (N.D. Ohio 2011) (noting the Fourth Amendment issues that arise with online activity); Ann K. Wooster, Annotation, *Expectation of Privacy in and Discovery of Social Networking Web Site Postings and Communications*, 88 A.L.R. 6th 319 (2013) (summarizing the application of the Fourth Amendment expectation of privacy test in relation to Internet communications). If this lenient standard applied to e-discovery, it would create a loophole that the government could use to overstep search warrant requirements and Fourth Amendment rights that may arise with seizure of electronic data. *See* James T. Stinsman, Comment, *Computer Seizures and Searches: Rethinking the Applicability of the Plain View Doctrine*, 83 TEMP. L. REV. 1097, 1102, 1111 (2011) (describing how traditional warrant rules apply to electronic data, courts' attempts to limit the scope of a search, and the problematic "dichotomy between the Fourth Amendment's particularity requirement and the plain view exception . . . in electronic data searches conducted pursuant to search warrants"). Instead of targeting the defendant, the government could simply issue a subpoena duces tecum and compel third parties to disclose similar information. *See* FED. R. CRIM. P. 17(c)(1) (stating that the government can subpoena a witness to produce "any books, papers, documents, data, or other objects the subpoena designates"). Some courts have given limited Fourth Amendment protection to online activity but most have not found a reasonable expectation of privacy in electronic information. *See, e.g.*, United States v. DiTomasso, 56 F. Supp. 3d 584, 594–95 (S.D.N.Y. 2014) (finding that private email correspondence did not affect defendant's expectation of privacy); United States v. Lustig, 3 F. Supp. 3d 808, 827 (S.D. Cal. 2014) (deciding defendant had no reasonable expectation of privacy in advertisements posted on the Internet); *Sawyer*, 786 F. Supp. 2d at 1352, 1356 (determining that defendant did not have a reasonable expectation of privacy over a "closed" peer-to-peer sharing program); Wilson v. Moreau, 440 F. Supp. 2d 81, 117 (D.R.I. 2006), *aff'd*, 492 F.3d 50 (1st Cir. 2007) (accessing email through a workplace computer did not destroy the user's expectation of privacy). *But see* United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332, 338 (D.P.R. 2007) (holding there is no expectation of privacy in emails that have reached the recipient).

[139] *See generally* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (finding a constitutional right to anonymous speech); *Cahill*, 884 A.2d at 454 (providing some constitutional protection for anonymous online speech); Lyrissa Barnett Lidksy, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 B.C. L. REV. 1373, 1376 (2009) (arguing that libel suits intent on unmasking anonymous online speakers threatened the First Amendment right to speak anonymously, but also recognizing the limits of such a right).

First Amendment protects anonymous speakers.[140] Although the Court in *McIntyre* considered political speech contained in a printed pamphlet, lower courts have extended this protection to anonymous online speech.[141]

The First Amendment may protect online data regarding monetary transactions as well.[142] In 2010, in *Citizens United v. Federal Election Commission*, the U.S. Supreme Court held that in certain situations, money could be a proxy for speech.[143] The plaintiffs were challenging campaign finance legislation that limited a corporation's ability to make political expenditures.[144] The Court held that these restrictions violated the First Amendment because they quelled a corporate entity's political speech.[145] In reaching this conclusion, once again the Court acknowledged there is speech value in monetary transactions.[146] Therefore, some believe that *Citizens United* opened the door to a First Amendment speech right in virtual currency transactions.[147]

[140] *See McIntyre*, 514 U.S. at 342 (holding that the First Amendment protects a speaker's right to anonymity).

[141] *See id.* at 344; *see also Cahill*, 884 A.2d at 454 (addressing the standard that should be used in assessing an online speaker's First Amendment right to anonymous speech); Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 380 n.4 (Va. 2001) (referencing the lower court's consideration of the First Amendment rights of anonymous online speakers).

[142] *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 314 (2010) (holding that the First Amendment protects some monetary transactions that are used to fund speech); Sara Jeong, *Is Bitcoin Free Speech?*, SLATE (Feb. 7, 2014, 8:48 AM), http://www.slate.com/articles/technology/future_tense/2014/02/bitcoin_as_free_speech_regulating_cryptocurrency_has_ramifications_for_democracy.2.html [http://perma.cc/947J-DZFQ] (hypothesizing that Bitcoin transactions could be protected by the First Amendment); *see also* Press Release, Electronic Frontier Foundation, EFF, Internet Archive, and Reddit Oppose New York's BitLicense Proposal (Oct. 21, 2014), https://www.eff.org/press/releases/eff-internet-archive-and-reddit-oppose-new-yorks-bitlicense-proposal [http://perma.cc/AQN2-4235] (protesting New York's BitLicense program, which regulates digital currencies, by pointing to a violation of speech rights).

[143] *See Citizens United*, 558 U.S. at 310; *see also* Buckley v. Valeo, 424 U.S. 1, 143 (1976) (holding that limits on an individual's campaign finance expenditures violated First Amendment rights).

[144] *Citizens United*, 558 U.S. at 319–21 (detailing the events that led to plaintiff's challenge of the Bipartisan Campaign Reform Act of 2002's restrictions on political expenditures).

[145] *Id.* at 365.

[146] *See id.* at 351 (noting that speakers "use money . . . to fund their speech . . . [and] the First Amendment protects the resulting speech"); *see also Buckley*, 424 U.S. at 16 (analyzing the use of money as not purely conduct but involving primarily speech, primarily conduct, or a mix of the two).

[147] *See* Jeong, *supra* note 142 (referring to *Citizens United* as placing speech value in monetary transactions and arguing that this creates a possible free speech argument for Bitcoin use); *see also* Danny Bradbury, *Bitcoin Is Crucial for the Future of Free Speech, Say Experts*, COINDESK (Aug. 6, 2013), http://www.coindesk.com/bitcoin-is-crucial-for-the-future-of-free-speech-say-experts/ [http://perma.cc/CP8C-B3V3] (emphasizing the value of Bitcoin in promoting free speech and specifically referencing WikiLeak's use of Bitcoin donations); Kenny Spotz, *If You Support Free Speech, You Support Bitcoin*, COINTELEGRAPH (Jan. 21, 2015, 7:49 AM), http://cointelegraph.com/news/113332/if-you-support-free-speech-you-support-bitcoin-op-ed [http://perma.cc/PG5N-KMSL]

D. Digital Millennium Copyright Act

The Digital Millennium Copyright Act provides a civil option for plaintiffs to access the identities of anonymous Internet speakers.[148] Congress passed the DMCA in an attempt to control and restrict the copying and disseminating of copyrighted works in the digital realm.[149] The DMCA allows plaintiffs to sue anonymous individuals who have violated copyright law on the Internet.[150] Using § 512(h) of the DMCA, copyright holders can subpoena third-party Internet service providers to unmask infringing users.[151]

Over time, courts have interpreted the DMCA's subpoena power to apply only when an Internet service provider has stored the infringing material on its servers.[152] Thus, the ability to subpoena an individual's identity does not apply to providers that act only as conduits and nothing more.[153] One example is a peer-to-peer sharing system, where senders and recipients share files directly without uploading them onto an intermediary server.[154] Moreover, some courts have recognized a limited First Amendment interest in remaining anonymous on the Internet.[155] To a degree, courts have even

(arguing that if money is a form of speech, Bitcoin use promotes free speech because it does not have traditional monetary restrictions such as requiring intermediaries to facilitate transactions).

[148] *See* Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012); BELLIA ET AL., *supra* note 18, at 340–42 (providing an overview of the DMCA).

[149] *See* BELLIA ET AL., *supra* note 18, at 340, 410–11 (articulating the congressional intent behind the DMCA); *see also* H.R. REP. NO. 105-551, pt. 2, at 21–28 (1998) (report from the House Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection detailing the reasons why the DMCA should be passed into law).

[150] *See* 17 U.S.C. § 512(h); BELLIA ET AL., *supra* note 18, at 408–11 (discussing the scope and application of the DMCA).

[151] 17 U.S.C. § 512(h) ("A copyright owner . . . may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.").

[152] Jeannie Roebuck, *BitTorrent Sharing: The Case Against John Does*, 18 INTELL. PROP. L. BULL. 35, 40 (2013) (noting that Congress is worried about chilling innovation by placing liability on intermediary services); *see also* Laura Rogal, *Anonymity in Social Media*, 7 PHOENIX L. REV. 61, 72 (2013) (discussing the scope of the DMCA's subpoena powers); Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 339–40 (2008) (pointing to the DMCA as a method of obtaining a "John Doe subpoena").

[153] *See* Roebuck, *supra* note 152, at 40 (acknowledging a limitation on the DMCA's subpoena power); *see also* Rogal, *supra* note 152, at 72 (confirming the Internet service provider must be storing the infringing content).

[154] *See* Roebuck, *supra* note 152, at 40 (stating that the DMCA does not allow for subpoenas against peer-to-peer sharing systems).

[155] Rogal, *supra* note 152, at 72; *see also* Gleicher, *supra* note 152, at 325 (examining how First Amendment speech rights are affected by what Gleicher refers to as "John Doe subpoenas"). Some courts have found that sharing materials through peer-to-peer networks constitutes speech under the First Amendment. *See* Rogal, *supra* note 152, at 72 (citing Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004)) ("[T]he use of [peer-to-peer] file copying networks to download, distribute, or make available for distribution copyrighted sound recordings

recognized that such an interest exists when it pertains to the use of peer-to-peer sharing systems.[156]

Courts balance a series of criteria in determining whether to quash a subpoena under § 512(h).[157] Due to First Amendment issues that arise when unmasking anonymous speakers on the Internet, many courts are adamant that a factual basis for the request exists before allowing the subpoena.[158] The standard is strict: there must be a legitimate reason to justify the issuing of a subpoena.[159] Courts have even compared subpoenas in a civil context to warrants in a criminal case.[160]

III. UNMASKING BITCOIN'S HIDDEN IDENTITIES: CRAFTING A NEW SUBPOENA POWER USING EXISTING E-DISCOVERY RULES

The absence of criminal subpoena standards for electronically stored information and the continual misuse of Bitcoin highlights the importance of updating government regulations to address this gap.[161] This Part argues

without permission . . . qualifies as speech, but only to a degree."). This protection is limited especially when that speech infringes a rights holder's copyright. *See Sony Music*, 326 F. Supp. 2d at 563. (rejecting an individual's ability to use the First Amendment as a defense to intellectual property infringement).

[156] *See Sony Music*, 326 F. Supp. 2d at 564 (recognizing First Amendment rights in a case involving a peer-to-peer network); Rogal, *supra* note 152, at 72 (analyzing situations where courts have considered peer-to-peer sharing as speech).

[157] Stavnes, *supra* note 119, at 717 (listing the different factors a court balances); *see* Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578–79 (N.D. Cal. 1999) (providing important considerations when evaluating a motion to quash); *see also* 17 U.S.C. § 512. These factors include: (1) whether there is prima facie evidence of unprotected speech in the claim; (2) whether the claim can survive a motion to dismiss or summary judgment; (3) whether the subpoena is relevant to the claim; (4) weighing the interests of both parties; and (5) whether plaintiff has exhausted all means available to identify the defendant. Stavnes, *supra* note 119, at 717.

[158] *See* Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. REV. 833, 850 (2010) (noting that courts place a high burden of proof on plaintiffs before unmasking an Internet speaker's identity); *see also* Rogal, *supra* note 152, at 73 (emphasizing a court's hesitation to unmask an anonymous speaker). Courts are extremely careful because this is "an extraordinary application of the discovery process." *See Columbia Ins. Co.*, 185 F.R.D. at 580–81 (explaining that the court wants to be sure the plaintiff has standing against the defendant before revoking the defendant's anonymity). They have reached this conclusion because they are worried that the subpoena power could be misused to chill speech. *See* Mobilisa, Inc. v. Doe, 170 P.3d 712, 720 (Ariz. Ct. App. 2007) (stating that a more lenient standard "would set the bar too low, chilling potential speakers from speaking anonymously on the internet"); *Cahill*, 884 A.2d at 457 ("We are concerned that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously.").

[159] *See* Mazzotta, *supra* note 148, at 850 (noting that courts require some "evidentiary showing"); *see also* Rogal, *supra* note 152, at 67 (discussing a court's weighing of a litigant's right to legal recourse against an anonymous speaker's First Amendment rights). One court even referred to its review of the subpoena as a "preliminary hearing." Mazzotta, *supra* note 148, at 850.

[160] *Columbia Ins.*, 185 F.R.D. at 579–80; Mazzotta, *supra* note 148, at 850 n.121.

[161] *See infra* notes 161–200 and accompanying text.

that the U.S. Supreme Court and Congress must craft a criminal subpoena power that reaches illicit Bitcoin use without infringing upon a user's First Amendment rights.[162] Section A explains why a new subpoena standard is necessary to target Bitcoin users engaging in criminal transactions.[163] Section B details what that standard should be, using elements of existing discovery and subpoena rules and statutes.[164]

A. Why Is a New Standard Necessary?

In order to combat the criminal exploitation of Bitcoin, the U.S. Supreme Court and Congress must create a new targeted subpoena process to compel individuals or websites to disclose the identity of users conducting illegal transactions.[165] No current statute exists that provides a targeted criminal subpoena standard.[166] Due to Bitcoin's open source nature, it is difficult to identify perpetrators who use the virtual currency to facilitate their criminal acts.[167] There is no single company behind Bitcoin that the government can subpoena or raid; Bitcoin exists only on a network of computers.[168] Thus, the impact of an act like the Silk Road seizure disappears quickly over time.[169]

[162] *See infra* notes 165–200 and accompanying text.

[163] *See infra* notes 165–185 and accompanying text.

[164] *See infra* notes 186–200 and accompanying text.

[165] *See* Palmer, *supra* note 6 (noting the continued use of Bitcoin on black market websites); Wong, *supra* note 6 (mentioning the continuation of black market websites despite the government shutdown of Silk Road and the incarceration of its operator); *see also* Lane, *supra* note 1, at 553–56 (indicating a movement toward government regulation of Bitcoin).

[166] *See* FED. R. CRIM. P. 17 (describing current criminal subpoena standards); Garrie et al., *supra* note 13, at 527 (highlighting the lack of criminal e-discovery standards); *see also* Gruenspecht, *supra* note 118, at 552 (asserting that criminal rules and cases do not provide adequate regulation of e-discovery).

[167] *See* Bryans, *supra* note 30, at 443 (discussing Bitcoin's virtual anonymity); Kaplanov, *supra* note 29, at 167–68 (detailing the anonymous nature of Bitcoin); Lane, *supra* note 1, at 530 (emphasizing the difficulties the government will encounter when attempting to identify Bitcoin users).

[168] *See* Penrose, *supra* note 34, at 530–31 (referring to Bitcoin's decentralized network); Kaplanov, *supra* note 29, at 167–68 (explaining how the decentralized nature of Bitcoin makes it difficult to regulate). Although there is no single company for the government to target, intermediaries such as Bitcoin wallet sites are "susceptible to regulation and enforcement." Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 146 (2014) (describing the ability to reach Bitcoin users despite the lack of a "company or central server").

[169] *See* Palmer, *supra* note 6 (noting the emergence of Silk Road 2.0 immediately following Silk Road's closure).

The standard subpoena process set forth in Rule 17 of the Federal Rules of Criminal Procedure is lacking in several ways.[170] Without amending the standard to adapt to e-discovery, the current interpretation of the rule makes it difficult for the government to obtain desired electronic information.[171] To get a third party subpoena, the government has to show that the information sought is relevant, that it is admissible, and that the subpoena specifically identifies the materials sought.[172]

It is doubtful that the federal government will be able to successfully and in a timely manner use its current criminal subpoena power to unmask the individuals committing illegal Bitcoin transactions.[173] The government likely cannot meet the specificity requirement because it would have to go through millions of transactions and hundreds of thousands of user accounts in order to pinpoint specific targets.[174] The government might be able to overcome this by using a grand jury subpoena to expedite the process or by targeting websites where the transactions are largely illegal in nature.[175] By focusing on black market transactions on sites similar to the now defunct Silk Road, the government could argue that a subpoena duces tecum requiring the unmasking of each user is relevant and specific; however, courts are not likely to broaden specificity to allow the targeting of thousands, maybe even millions, of user accounts.[176]

[170] *See* FED. R. CRIM. P. 17; Garrie et al., *supra* note 13, at 527 (asserting a need for criminal e-discovery standards); Gruenspecht, *supra* note 118, at 552 (affirming the lack of an e-discovery framework in criminal contexts).

[171] *See* Cheney v. U.S. Dist. Court for D.C., 542 U.S. 367, 387 (2004) (providing a narrow interpretation of the specificity prong); United States v. Nixon, 418 U.S. 683, 700 (1974) (explaining the standard that the government would have to overcome in order to issue a subpoena duces tecum); *see also* Gruenspecht, *supra* note 118, at 552 (listing rejected, overbroad subpoena requests).

[172] *See Nixon*, 418 U.S. at 700; *see also Cheney*, 542 U.S. at 387 (discussing the precision required to meet specificity); United States v. Binday, 908 F. Supp. 2d 485, 492 (S.D.N.Y. 2012) (reiterating that the *Nixon* standard places these three limitations on subpoenas). *But see* Kerr v. U.S. Dist. Court for N. Dist. of Cal., 426 U.S. 394, 399 (1976) (allowing a broad interpretation of relevancy in pretrial contexts).

[173] *See Cheney*, 542 U.S. at 387 (setting a narrow scope on specificity); *Nixon*, 418 U.S. at 700 (explaining the limitations placed upon traditional criminal subpoenas); *see also Binday*, 908 F. Supp. 2d at 492.

[174] *See Cheney*, 542 U.S. at 387; *Nixon*, 418 U.S. at 700; *see also* McIntyre, *supra* note 5, at 344 (describing the government's attempt to identify individual Silk Road users as an "impossible task").

[175] *See* McIntyre, *supra* note 5, at 345 (finding that a majority of Silk Road transactions were illegal). *Contra Cheney*, 542 U.S. at 387 (rejecting prosecution's argument that specificity was met, because the discovery requests "ask[ed] for everything under the sky").

[176] *See Cheney*, 542 U.S. at 387 (setting a very limited scope for specificity); *Nixon*, 418 U.S. at 699 (identifying specific documents to overcome the specificity prong); McIntyre, *supra* note 5, at 344–45 ("The government's allegation that the funds were involved in a money laundering conspiracy was . . . sufficient to justify forfeiture.").

At the same time, if the government uses a grand jury subpoena to sidestep the difficulty of showing specificity, the framework becomes too lenient and open to abuse.[177] Once the Bitcoin marketplace reaches the point where most individuals are engaging in legal transactions, lax subpoena standards become a problem.[178] The U.S. Supreme Court and Congress must be careful when developing a criminal subpoena standard for Bitcoin because it will primarily affect anonymous speech, a crucial First Amendment right that has been highly valued throughout U.S. history.[179] If the government can easily issue subpoenas duces tecum and force marketplace sites to unmask individuals, it might infringe upon Bitcoin users' First Amendment rights to maintain anonymity on the Internet.[180] This creates a

[177] *See* Bourjaily v. United States, 483 U.S. 171, 172 (1987) (concluding that *Nixon* does not apply to subpoena requests arising during a grand jury proceeding); McIntyre, *supra* note 5, at 345 (discussing the government's lack of interest in discerning between legitimate and illicit uses of Bitcoin on Silk Road). An in-depth study of Silk Road found that 3.9% of items listed were books. *See* Christin, *supra* note 72. These were likely legitimate listings and the government seizure of related bitcoins likely intruded upon First Amendment rights. *See* McIntyre, *supra* note 5, at 345 ("[T]he government did not trouble itself with distinguishing users who had purchased books from users who had purchased heroin.").

[178] *See, e.g.*, Trautman, *supra* note 3, at 8 (referencing the idea that early adopters of technological development tend to use it for illegal means); Graham, *supra* note 2 (stating that when PayPal let merchants accept Bitcoin it gave the virtual currency more legitimacy); Rizzo, *supra* note 58 (discussing Microsoft's acceptance of Bitcoin payments for virtual content).

[179] Stavnes, *supra* note 119, at 699; *see* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 314 (2010) (upholding the importance of political speech by extending protection to certain monetary transactions); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (deciding that anonymous speech receives First Amendment protection); *see also* Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005) (providing limited constitutional protection for anonymous online speech). This is especially true when it comes to political speech. *See McIntyre*, 514 U.S. at 341–42 (striking down an Ohio statute that prohibited anonymous leafleting of campaign literature); Stavnes, *supra* note 119, at 699 (discussing the importance of anonymous publications and mentioning the Federalist Papers as an example). The First Amendment likely provides Bitcoin users some protection in maintaining anonymity but thus far, Fourth Amendment claims regarding electronic content have been less successful. *See* Wooster, *supra* note 138, at 319 (summarizing how the expectation of privacy applies to online communication). Although in specific situations courts have allowed a limited expectation of privacy in electronic material such as email messages, in general they have not been open to the idea that Fourth Amendment protections apply to electronic data shared with third parties. *See, e.g.*, United States v. DiTomasso, 56 F. Supp. 3d 584, 594–95 (S.D.N.Y. 2014) (finding that private email correspondence did not affect defendant's expectation of privacy); United States v. Lustig, 3 F. Supp. 3d 808 (S.D. Cal. 2014) (deciding defendant had no reasonable expectation of privacy in advertisements posted on the Internet); United States v. Sawyer, 786 F. Supp. 2d 1352 (N.D. Ohio 2011) (determining that defendant did not have a reasonable expectation of privacy over a "closed" peer-to-peer sharing program); Wilson v. Moreau, 440 F. Supp. 2d 81 (D.R.I. 2006), *aff'd*, 492 F.3d 50 (1st Cir. 2007) (accessing email through a workplace computer did not destroy the user's expectation of privacy). *But see* United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332 (D.P.R. 2007) (holding there is no expectation of privacy in emails that have reached the recipient).

[180] *See* Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005) (acknowledging a First Amendment interest in anonymous online speech); McIntyre, *supra* note 5, at 345 (highlighting the government's disregard of valid listings on Silk Road that were likely protected by the First Amendment

far-reaching effect that would not apply to traditional subpoena duces tecum or grand jury subpoenas because they generally deal with witness production of relevant documents in a criminal case and not identifying anonymous defendants.[181]

The anonymous use of Bitcoin is likely to have some First Amendment protection following the U.S. Supreme Court's decision in 2010, in *Citizens United v. Federal Election Commission*.[182] Even though *Citizens United* only explores the idea of money as political speech, lower courts could apply this holding to virtual currency transactions.[183] Since *Citizens United* tied spending money in the free marketplace to speech, it follows that the same logic would apply to virtual currencies used in online speech.[184] Although these cases may protect money more when it is used in political speech, they still acknowledge some rights in money as speech in general.[185]

B. Creating a Special Subpoena Power

Virtual currencies like Bitcoin will continue to proliferate on the Internet.[186] As the government moves toward regulating various aspects of Bitcoin, it must establish new e-discovery rules targeting users who have taken advantage of Bitcoin's anonymity to commit illegal acts.[187] At the

during their seizure of all user bitcoins); *see also McIntyre*, 514 U.S. at 342 (concluding that the First Amendment protects anonymous speakers).

[181] *See* FED. R. CRIM. P. 17 (discussing witness production of items before trial begins).

[182] *See Citizens United*, 558 U.S. at 314 ("All speakers . . . use money amassed from the economic marketplace to fund their speech, and the First Amendment protects the resulting speech."); Buckley v. Valeo, 424 U.S. 1, 16 (1976) (noting that money is not solely conduct but also has an element of speech). The Court held that money could be considered speech, which gives it some First Amendment protections. *See Citizens United*, 558 U.S. at 314.

[183] *See Citizens United*, 558 U.S. at 314 (describing the way that money should be viewed as speech in situations where corporate funds are used to make a political impact); *Buckley*, 424 U.S. at 16 (indicating that money can be used by individuals as political speech).

[184] *See Citizens United*, 558 U.S. at 314; Jeong, *supra* note 142 (arguing that a Bitcoin as speech analysis is not improbable); *see also Buckley*, 424 U.S. at 16; *Cahill*, 884 A.2d at 546 (acknowledging that *McIntyre* extends limited anonymity rights to online speech).

[185] *See Citizens United*, 558 U.S. at 314 (discussing corporate political speech); *Buckley*, 424 U.S. at 16 (discussing individual political speech). Furthermore, even if this concept is limited to political speech, it will still affect a subset of Bitcoin transactions. *See* Bradbury, *supra* note 147 (emphasizing the importance of Bitcoin in political speech, specifically addressing how Bitcoin aided WikiLeaks when traditional credit card mediums prevented users from donating to the website); *see also Cahill*, 884 A.2d at 546 (discussing the importance of anonymous online political speech).

[186] *See* Graham, *supra* note 2 (referencing Bitcoin's growing legitimacy especially after PayPal's recent deal with Coinbase); Lee, *supra* note 13 (positing that it is too late for regulators to shutdown Bitcoin); *see also* Harper, *supra* note 13 (emphasizing that Bitcoin will remain even if government regulations persist); COINMAP, *supra* note 58 (indicating the growing number of businesses that accept Bitcoin).

[187] *See* I.R.S. Notice 2014-21, *supra* note 13 (discussing virtual currencies and taxation standards); FIN. CRIMES ENF'T NETWORK, *supra* note 13 (describing virtual currencies and FinCEN

same time, potential solutions need to ensure that the government will not be able to overreach and infringe upon the rights of legitimate Bitcoin users who wish to maintain their anonymity.[188] The U.S. Supreme Court and Congress should amend Rule 17 of the Federal Rules of Criminal Procedure to reflect e-discovery, but with respect to Bitcoin, it needs to go one step further and specifically address the issues that would arise with revealing the identities of anonymous users.[189]

When determining the initial threshold for the government to issue a subpoena, the U.S. Supreme Court and Congress should adopt the approach that the Federal Rules of Civil Procedure have taken toward e-discovery in Rules 26 and 45.[190] The proportionality requirement added to Rule 26 is an important limitation that should also exist in a criminal subpoena statute.[191] The cost of e-discovery is less prevalent when it comes to identifying Bitcoin users because it is unlikely that privileged information is involved as opposed to documents available on a corporation's servers.[192] The main upside to implementing this restriction is that it will prevent the government from subpoenaing a website or Bitcoin wallet service to gain information about an unlimited number of transactions.[193] This prevents governmental

regulations); *see also* Brito et al., *supra* note 168, at 144 (discussing how current financial regulation would map onto Bitcoin and how potential regulation of Bitcoin intermediaries would operate). Once Bitcoin exchange and wallet sites are regulated, the government will have a source to subpoena for user information. *See* BRITO & CASTILLO, *supra* note 8, at 9 (describing the resulting decrease in anonymity once Bitcoin intermediaries have to comply with financial regulations).

[188] *See* Rogal, *supra* note 152, at 67 (discussing the First Amendment protection of anonymous online speech); Stavnes, *supra* note 119, at 699 (emphasizing the importance of the right to Internet anonymity); *see also Cahill*, 884 A.2d at 546 (finding limited First Amendment rights in anonymous online speech); Bradbury, *supra* note 147 (reiterating that Bitcoin represents online speech in many situations).

[189] *See* FED. R. CRIM. P. 17; Rogal, *supra* note 152, at 73 (addressing why courts hesitate to unmask online speakers); *see also* McIntyre, *supra* note 5, at 345 (discussing the government overreach that grouped both legitimate and illegal uses of Bitcoin together).

[190] *See* FED. R. CIV. P. 26, 45 (allowing judges general discretion in determining whether an e-discovery request constitutes an undue burden); FED. R. CRIM. P. 17 (containing no specific rules for e-discovery); *see also* Garrie et al., *supra* note 13, at 527 (emphasizing the need for guidance on e-discovery in criminal litigation).

[191] *See* FED. R. CIV. P. 26; Bennett, *supra* note 16, at 437 ("Inherent in the balance between production of information necessary for a fair search for truth, versus the burden and cost of discovery, is a sense of 'proportionality.'"); *see also* Oracle USA, Inc. v. SAP AG, 264 F.R.D. 541, 543 (N.D. Cal. 2009) (highlighting the importance of proportionality when applying Rule 26).

[192] *See* Ward et al., *supra* note 102, at 170–71 (citing the costs of removing privileged information from e-discovery material); *see also* Bennett, *supra* note 16, at 438 (detailing the expensive search costs associated with e-discovery).

[193] *See* Bennett, *supra* note 16, at 437 (describing the need for proportionality in e-discovery presented in Rule 26); Ward et al., *supra* note 102, at 179 (citing proportionality as a limitation on the scope of discovery); *see also* Martin, *supra* note 113, at 190 (stating that courts should carefully consider proportionality when determining the scope of e-discovery).

overstep and potential infringement upon the First Amendment rights of legitimate Bitcoin users.[194]

In addition, before issuing a subpoena to unmask a Bitcoin user, courts and grand juries should consider the same two concerns that courts contemplate when determining whether to quash a subpoena under the Digital Millennium Copyright Act.[195] First, in order for a court or grand jury to approve the subpoena, the government should be required to show some evidence of illegal activity.[196] Second, the government should be required to show that the subpoena is relevant to the claim.[197] When it comes to criminal subpoenas, specificity and relevancy are important to ensure that the government is narrowly tailoring its actions to prevent treading upon First Amendment rights.[198]

The other factors that courts consider when deciding to quash a DMCA subpoena should not explicitly apply to the initial approval of a criminal

[194] *See* Bennett, *supra* note 16, at 437 (putting forth proportionality as a check on e-discovery); Ward et al., *supra* note 102, at 179 (considering proportionality and reasonableness as checks on burdensome e-discovery requests); *see also Citizens United*, 558 U.S. at 314 (providing First Amendment protection for certain monetary transactions).

[195] *See* Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578–79 (N.D. Cal. 1999) (describing the factors a court will consider when assessing a DMCA subpoena); Stavnes, *supra* note 119, at 717 (stating the five criteria that courts consider when deciding whether or not to quash a § 512(h) subpoena); *see also* Digital Millennium Copyright Act, 17 U.S.C. § 512(h) (2012) (detailing the statutory framework for a DMCA subpoena); *Citizens United*, 558 U.S. at 314 (acknowledging the link between monetary transactions and speech rights); *Cheney*, 542 U.S. at 387 (providing a narrow view of specificity within a traditional subpoena framework); *Nixon*, 418 U.S. at 700 (setting forth the three elements that moving parties have to meet for traditional criminal subpoenas); *Cahill*, 884 A.2d at 546 (extending limited First Amendment rights to anonymous online speech).

[196] *See* 17 U.S.C. § 512(h); Stavnes, *supra* note 119, at 717. This requirement prevents the government from randomly gathering a group of transactions or all the transactions on a general Bitcoin website and issuing a subpoena to identify those users. *Cf.* Stavnes, *supra* note 119, at 701 (noting that online anonymity proponents worry about government interference stifling Internet activity). This standard is more lenient than the specificity requirement of Rule 17 of the Federal Rules of Criminal Procedure, which provides more limitations. *See* 17 U.S.C. § 512(h); FED. R. CRIM. P. 17. In the case of Silk Road, the government would have had substantial evidence that most, if not all, of the transactions involved illegal activity. *See* Trautman, *supra* note 3, at 10–20 (detailing various illicit Bitcoin transactions uncovered by the government).

[197] *See* Packwood v. Senate Select Comm. on Ethics, 510 U.S. 1319, 1320–21 (1994) (discussing standards for evaluating a pretrial subpoena duces tecum); *Kerr*, 426 U.S. at 399 (providing a broad scope for pretrial relevancy determinations); *Nixon*, 418 U.S. at 700 (requiring “relevancy” as a necessary element in issuing a criminal subpoena duces tecum). This is a relatively low hurdle for the government to pass and is also one of the elements the U.S. Supreme Court established for Rule 17 of the Federal Rules of Criminal Procedure. *See* 1 ORFIELD, *supra* note 102, § 6:89.

[198] *See supra* notes 165–185 and accompanying text. Courts have generally required specificity when evaluating a DMCA subpoena because it prevents bad faith and frivolous claims. *See* Gleicher, *supra* note 152, at 339–40.

subpoena request because they would be too restrictive.[199] Although these factors should not apply to the initial decision to grant a subpoena, it should be left to the court's discretion to determine whether to consider these other issues when reviewing a recipient's motion to quash a subpoena.[200]

CONCLUSION

In the digital age, there are a growing number of legal and illegal Bitcoin transactions. In order for the government to target criminal use of Bitcoin, the U.S. Supreme Court and Congress must address the gap in e-discovery rules for criminal litigation. When constructing a subpoena power that allows governmental entities to unmask anonymous online Bitcoin users in criminal proceedings, the Court and the legislature need to create a balancing test that fits between the tests for granting subpoenas duces tecum and grand jury subpoenas. Implementing a standard that is more lenient than the direct application of traditional subpoena duces tecum to e-discovery will allow the government to directly target prohibited Bitcoin transactions. Most importantly, ensuring the standard is narrower than a grand jury subpoena will limit the government's ability to infringe upon a Bitcoin user's First Amendment speech rights.

ALICE HUANG

[199] *See* 17 U.S.C. § 512(h); Stavnes, *supra* note 119, at 717 (describing the other elements courts weigh in DMCA cases). If the grand jury considered the existence of prima facie evidence of the crime, it would be too high a standard for simply obtaining a subpoena. *See* Stavnes, *supra* note 119, at 717. This is especially true due to the higher burden of proof in criminal cases. *See id.*

[200] *See* FED. R. CIV. P. 26, 45 (allowing judges discretion when defining limitations on e-discovery); Stavnes, *supra* note 119, at 717; *see also* Margoles v. United States, 402 F.2d 450, 451 (7th Cir. 1968) (giving the lower court discretion to determine the validity of a subpoena duces tecum); Application of Tex. Co., 27 F. Supp. 847, 850–51 (E.D. Ill. 1939) (finding that courts have some discretionary power when evaluating a grand jury subpoena).