DECIPHERING CRYPTOCURRENCY: SHINING A LIGHT ON THE DEEP DARK WEB

CARMINE DIPIERO*

Government agencies have been slow to adapt to evolving technologies and the increasing use of decentralized, digital currencies for illegal acts. Virtual black markets are spawning rapidly, and just as one gets taken down dozens more appear in its place. Current regulations and methods of law enforcement are outdated and must be reformed and recalibrated in order to keep up with the innovative techniques of virtual black-market administrators and anonymous users. Despite the urgency of such reform, it must be accomplished while maintaining fundamental privacy rights and avoiding inhibiting new technologies. This Note explains how users are able to abuse digital currencies, such as bitcoin, for illegal purposes and analyzes the current methods used to catch these users. It then argues for a reformation of law-enforcement and legislative efforts so that resources may be focused efficiently on addressing the issue.

TABLE OF CONTENTS

* J.D. 2017, University of Illinois College of Law.

I. INTRODUCTION

> "Based on my training and experience, Silk Road has emerged as the most sophisticated and extensive criminal marketplace on the Internet today."[1]
>
> —Special Agent Christopher Tarbell, Federal Bureau of Investigation, 2013

The Internet has always been a place for individuals to communicate with others on virtually any topic or issue that sparks their curiosity. Historically, this medium of communication has led to the transfer of goods and services. It has also opened the door for the discussion and purchase of illicit substances or services. In fact, the first thing to be purchased and sold online was marijuana—between students at Stanford and MIT in the early 1970s.[2] Today, more than ever, concerns over privacy and government surveillance have sparked a revolution of individuals committed to the trade and sale of illegal substances through incredibly sophisticated methods.

1. Complaint at ¶ 16, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 14–cr–68 (KPF)).

2. Brian Anderson, *The First Thing to be Bought and Sold on the Internet was Some Weed*, VICE (Oct. 9, 2013, 5:05 PM), http://motherboard.vice.com/blog/the-first-thing-to-be-bought-and-sold-on-the-internet-was-some-weed ("In 1971 or 1972, Stanford students using Arpanet accounts at Stanford University's Artificial Intelligence Laboratory engaged in a commercial transaction with their counterparts at [MIT]. . . . The students used the network to quietly arrange the sale of an undetermined amount of marijuana.").

"Silk Road" was one of the first "Darknet markets" to emerge on the Internet since the invention of the bitcoin. Throughout 2011 and 2013, users of the Silk Road website could buy anything—drugs, child pornography, arranged murders, hacked credit cards, and countless other illicit activities and substances—using a virtual currency known as "bitcoin."[3] The United States government shut down the website in 2013, marking a triumphant victory over cybercriminals.[4] But, just as cutting off the head of a hydra sprouts two more, dozens of new "Silk Roads" arose in its place, making the markets more decentralized and difficult to contain than ever.

This Note addresses the expansion and legal efforts to thwart these so-called Darknet markets directly. As agency efforts and the methods criminals use to conceal their tracks are constantly evolving and reformulating, it takes a narrow approach at addressing certain aspects of the issue. Part II of this Note discusses what a bitcoin is, how individuals access Darknet markets, and the expansion of Darknet markets in the wake of the closure of the Silk Road. Part II also addresses the government agencies and statutes used to combat the expansion. Part III of this Note analyzes the efficiency in these methods and discusses the potential implications of current proposals. Part IV recommends a more specific approach for both legislators and law-enforcement agencies. Part V offers concluding thoughts on the big picture of this technological landscape.

II. BACKGROUND

In order to understand how bitcoin is used to facilitate transactions online while avoiding law enforcement, the technical aspects of how the process works warrants discussion. This Part tackles the complexities behind Bitcoin, Tor, and Darknet markets, as well as the legislative and law-enforcement efforts employed thus far.

A. Bitcoin Basics: A Historic and Technical Overview

In the late 1990s, Julian Assange was involved in a group called the "cyberpunks," who were interested in libertarianism and privacy through cryptography.[5] Around 1998, a member of this group proposed a digital currency called "b-money" that would be anonymous and distributed so

3. *See* Robert Anthony, *The Craziest Things You Could've Bought on Silk Road, the Black Market of the Internet*, ELITE DAILY (Oct. 9, 2013, 11:50 AM), http://elitedaily.com/envision/the-craziest-things-you-couldve-bought-on-silk-road-the-black-market-of-the-internet/.

4. *See* Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014), http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

5. Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 162 (2012).

entities could work together without being traced.[6] The project was left largely ignored until January 2009, about ten years later, when a computer programmer working under the name of "Satoshi Nakamoto"[7] created bitcoin—an open-source, decentralized digital currency.[8] In a publication released with his open-source algorithms for bitcoin, Nakamoto expressed his distrust with financial institutions being third-party intermediaries with virtually every online transaction.[9] The design of bitcoin is largely a reaction to this concern, and Nakamoto ensured many safeguards for the decentralization of this currency.[10]

Nakamoto's design has many intelligent components that follow the theme of his concern for a decentralized currency. The "bitcoin protocol" is how computers communicate in regards to sending, receiving, and managing bitcoin.[11] The "bitcoin network" is an aggregate of every computer that uses the protocol.[12] For someone who wants to become involved in a transaction, they initiate a transaction and the information is sent to the network.[13] After approximately ten minutes (depending on the congestion of the network), the transaction is computationally verified by the network, becoming a permanent addition.[14] Every transaction is public and available to be viewed by any member of the network on what is referred to as the "bitcoin public ledger," or the "blockchain."[15] Because of this method of transaction oversight, every user is essentially involved in every transaction, which makes bitcoin completely decentralized.[16]

bitcoin also has a system in place to provide a sort of pseudo-anonymity. Every user who wants to participate in the network must have a "public key" and a "private key" in order to facilitate a transaction.[17] A private key is a very large randomized number used to generate public keys.[18] A private key is created when a user of the system chooses

6. *Id.*

7. Satoshi Nakamoto's identity has not been released, nor has it been discovered.

8. EDWARD V. MURPHY ET AL., CONG. RES. SERV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 (2015), https://www.fas.org/sgp/crs/misc/R43339.pdf.

9. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN PROJECT, http://bitcoin.org/bitcoin.pdf (last visited Jan. 31, 2017).

10. *See id.* ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.").

11. *See* Nicholas Galunic, *The (Private) Key to Unlocking Bitcoin Legal Issues*, LAW360 (Feb. 19, 2015, 10:38 AM), http://www.law360.com/articles/622698/the-private-key-to-unlocking-bitcoin-legal-issues.

12. *See id.*

13. *See id.*

14. *See id.*

15. *See id.*

16. *See id.*; MURPHY ET AL., *supra* note 8, at 1 ("Each Bitcoin and each user is encrypted with a unique identity, and each transaction is recorded on a decentralized public ledger . . . that is visible to all computers on the network but does not reveal any personal information about the involved parties.").

17. *See* Galunic, *supra* note 11.

18. *See id.*

a bitcoin "wallet" that stores bitcoins and creates public keys.[19] Public keys are then used to create "addresses," which members of the network use to send and receive bitcoins.[20] These addresses are not connected with a person or entity, which is largely what makes the use of bitcoin pseudo-anonymous.[21]

This system also has many safeguards to ensure each transaction is secure. In order to verify each transaction, a very complex mathematical system was put in place to authorize the communications between the networks and to ensure that bitcoins are not "double spent."[22] A bundle of transactions are organized into a "block," which takes very heavy computing power in order to solve and verify that the transactions are genuine.[23] Users who opt to participate in this process—referred to as "mining"—are rewarded with a number of bitcoins for each successful block.[24] For every 210,000 blocks that are solved, this reward is halved until the entire amount of bitcoins[25] have been created.[26] Adding competitors in this mining market does not guarantee blocks will be solved faster, as the difficulty of solving the blocks changes approximately every two weeks (according to the speed in which that previous segment of blocks were solved).[27] This keeps the price of bitcoins relatively stable, as

19. *See id.* For a list of the types of wallets that are used to store Bitcoin and public and private keys, see *Choose Your Bitcoin Wallet*, BITCOIN, https://bitcoin.org/en/choose-your-wallet (last visited Jan. 31, 2017).

20. *See* Galunic, *supra* note 11 ("A bitcoin transaction is a digitally signed message instructing the network to reassign control of some bitcoins from address A to address B.").

21. *See Using Bitcoin Anonymously*, 99BITCOINS, https://99bitcoins.com/know-more-using-bitcoin-anonymously (last visited Jan. 31, 2017). Although, the addresses may give the user's location geographically, depending on which service the user initiated the transaction.

22. Jonathan Lane, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 519 (2014).

23. *Id.* For more information on the amount of energy some Bitcoin mines consume, see Christopher Malmo, *Bitcoin is Unsustainable*, VICE: MOTHERBOARD (June 29, 2015, 12:23 PM), http://motherboard.vice.com/read/bitcoin-is-unsustainable. There are analysts who have calculated the energy cost of each transaction to be over five thousand times that of a regular Visa transaction, with a rapidly rising rate of carbon emissions compared to that of the banking sector. Malmo, *supra* (claiming that the cost of a single transaction could power over one and a half households for a day). Other opponents of Bitcoin have put the energy cost in terms of actual power use. KARL J. O'DWYER & DAVID MALONE, HAMILTON INST., NAT'L UNIV. OF IR. MAYNOOTH, BITCOIN MINING AND ITS ENERGY FOOTPRINT 4 (2014), https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf ("[I]t is plausible that the energy used by Bitcoin mining is comparable to Irish national energy consumption."). There has been debate regarding the validity of these findings. *See* Adam Rothstein, *The Digital Gold Rush: How Much Electricity Does Bitcoin Really Use?*, KERNEL (Jan. 11, 2015), http://kernelmag.dailydot.com/issue-sections/staff-editorials/11336/how-much-electricity-bitcoin-use/#sthash.Hiqn3lC7.dpuf.

24. Lane, *supra* note 22, at 519.

25. The maximum amount of Bitcoin possible is approximately 21 million. *Id.* at 519–20.

26. *Id.*; *see also* MURPHY ET AL., *supra* note 8, at 3 ("[T]he total number of Bitcoins that can be generated is arbitrarily capped at 21 million coins, which is predicted to be reached in 2140."). For a countdown of when the next halving will occur, as well as other statistics regarding bitcoin, see *Bitcoin Block Reward Halving Countdown*, BITCOIN BLOCK HALF, http://www.bitcoinblockhalf.com/ (last visited Jan. 31, 2017).

27. For a look at the difficulty rate history, as well as the current state of adjustment, see *Bitcoin Difficulty*, BITCOIN WISDOM, https://bitcoinwisdom.com/bitcoin/difficulty (last visited Jan. 31, 2017).

it makes it difficult for individuals to steal large amounts of bitcoin, as well as avoids manipulation by banks and governments.

The value of bitcoin is very hard to predict because it is determined by supply and demand.[28] In 2013, the price of bitcoin skyrocketed from around thirteen dollars per Bitcoin in January, to one thousand dollars per coin in November.[29] The value of bitcoin declined to around three to four hundred dollars per coin in 2014,[30] before remaining relatively stable at two hundred and fifty dollars per coin throughout 2015.[31] Bitcoin closed 2015 at around four hundred and thirty dollars.[32] Analysts have many different theories on what could affect the price so much, the most common being a China-driven surge, macro-economic events, and factors relating to specifics in the bitcoin technology and the fast-moving changes in legislation.[33]

Bitcoin can be purchased in several different ways, and additional methods are constantly invented.[34] One of the most common ways is through a bitcoin exchange, such as Coinbase or the former Mt. Gox.[35] The typical way to purchase bitcoins through an exchange is by linking your bank account and scheduling a purchase, although this method typically takes several days to verify (unless the purchaser links another form of credit to his account, such as a credit card).[36] Another popular way is through buying bitcoins in person, either using cash or a credit card.[37] This method is typically completed in the ten minutes a transaction takes to verify.[38]

28. Steven Hay, *What Determines, Affects and Influences Bitcoin's Price?*, BUY BITCOIN WORLDWIDE, https://www.buybitcoinworldwide.com/kb/what-determines-bitcoins-price/ (last visited Jan. 31, 2017).

29. Ben Rooney, *Bitcoin Prices Top $1,000*, CNN MONEY (Nov. 27, 2013, 11:11 AM), http://money.cnn.com/2013/11/27/investing/bitcoin-1000/.

30. To see a chart mapping the change, see BITCOIN CHARTS, http://bitcoincharts.com/charts/bitstampUSD#rg360zczsg2014-01-01zeg2014-12-31ztgSzm1g10zm2g25zv (last visited Jan. 31, 2017).

31. *Id.*

32. *See* Albert Libenzon, *Bitcoin Price Fluctuation in 2015 and a Forecast for 2016*, COIN TELEGRAPH (Jan. 4, 2016, 2:06 PM), http://cointelegraph.com/news/bitcoin-price-fluctuation-in-2015-and-a-forecast-for-2016.

33. *See* Yessi Bello Perez, *Bitcoin's Price Rise Explained by Industry Insiders*, COINDESK (Oct. 31, 2015, 11:50 AM), http://www.coindesk.com/bitcoins-price-rise-explained-by-industry-insiders/.

34. *Darkode*, RADIOLAB (Sept. 21, 2015, 9:16 PM), http://www.radiolab.org/story/darkode/ (discussing the variety of different ways a victim of hacking went through to purchase Bitcoin).

35. *See* COINBASE, https://www.coinbase.com/ (last visited Jan. 31, 2017); *see also* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 03, 2014, 6:30 AM), http://www.wired.com/2014/03/bitcoin-exchange/ (detailing the downfall of the one of the first Bitcoin exchanges).

36. *See* Payment Methods for US Customers, COINBASE, https://support.coinbase.com/customer/en/portal/articles/1148716-how-do-i-buy-and-sell-bitcoin-with-my-us-bank-account- (last visited Jan. 31, 2017).

37. *See* Lauren Orsini, *Here's What Happened When I Bought Bitcoin in Person*, BUSINESS INSIDER (Oct. 23, 2013, 11:34 AM), http://www.businessinsider.com/heres-what-happened-when-i-bought-bitcoin-in-person-2013-10. A common website for Bitcoin users to meet up and trade Bitcoin for money is https://localbitcoins.com/.

38. *Id.*

If an individual wants to use bitcoin for illegal purposes, he or she may be vulnerable by having their IP address or other identifying information linked to the virtual address they sent their bitcoins from.[39] Regardless of the method used to purchase bitcoins, though, users can take their anonymity a step further by using a "tumbler."[40] These tumbling or mixing services receive bitcoins from a user; mix them with many other bitcoins over servers all over the world; then put them back together so the original connection to the individual is untraceable.[41] It can be thought of as throwing three grains of rice in a very large bowl of rice, shaking the bowl for several hours, and then taking out any three of the identical grains. Due to the safeguards put in place by Nakamoto, as well as "tumbling" services provided by others interested in privacy and anonymity, bitcoin is ideal for virtual transactions that require concealment of an individual's identity.

B. Adding Layers of Anonymity: The Onion Router and the Deep Dark Web

There are many other ways individuals can gain more anonymity while using bitcoin. One of which is facilitating transactions and browsing through The Onion Router ("Tor").[42] Tor is a type of Internet browser created to ensure secure government communications for the U.S. Navy.[43] When browsing or transmitting data through the Internet, Tor encrypts and sends the information through layers of randomized relay nodes located all over the world.[44] The path between a user browsing and the website itself is blurred by each randomized node between the user and their final destination.[45] This protects the individual user from having

39. *See* Andy Greenberg, *Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road's Black Market*, FORBES (Sept. 5, 2013, 10:36 AM), http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/.

40. *See* Jon Matonis, *The Politics of Bitcoin Mixing Services*, FORBES (June 5, 2013, 11:39 AM), http://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/; *see also* Andy Greenberg, *An Interview with a Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)*, FORBES (Aug. 14, 2013, 1:45 PM), http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/ ("[W]e employ an internal tumbler for when vendor withdraw their payments, and a more general mix for all deposits and withdrawals. This makes it impossible to link your deposits and withdrawals and makes it really hard to even tell that your withdrawals came from Silk Road.").

41. *See* Matonis, *supra* note 40.

42. Lane, *supra* note 22, at 521–22; *see also* Patrick Lambert, *Everything You Need to Know About Using TOR*, TECHREPUBLIC (June 28, 2013, 4:00AM), http://www.techrepublic.com/blog/it-security/everything-you-need-to-know-about-using-tor/.

43. *See* Abdulmajeed Alhogbani, *Going Dark: Scratching the Surface of Government Surveillance*, 23 COMMLAW CONSPECTUS 469, 483 (2015).

44. *See id.* ("There are over 5,000 nodes all over the world, making it nearly impossible to trace the original destination.").

45. *See id.*

their browsing linked to their IP addresses, making it difficult for government or law-enforcement agencies to identify users.[46]

Tor's ability to make Internet browsing anonymous has clear appeal for users of bitcoin because, when paired, the two create nearly complete anonymity for facilitating transactions online. There are certain websites that can only be viewed through browsers like Tor, which are sometimes referred to as the "Deep Web."[47] The major attractiveness of the Deep Web is that users cannot be traced to their IP address when viewing websites.[48] This makes all websites on the Deep Web, which is accessible through Tor, nearly completely anonymous. The allure of digital anonymity led to the creation of websites that contain illegal substances for sale, of which the network is called the "Dark Web" or "Darknet."[49] The first of these websites was called the Silk Road.

C. The Rise and Fall of the Silk Road

On January 27, 2011, a user on a forum of the website www.shroomery.org[50] unveiled the Darknet website "Silk Road," which the user described as "a Tor hidden service that claims to allow you to buy and sell anything online anonymously."[51] This was not the first online market for illicit substances to exist, but it was the first to combine Tor and bitcoin for this service.[52] The Silk Road's user base and listings grew slowly but steadily until around June 2011, when Adrian Chen, an American journalist, posted an *exposé* revealing the website to the public.[53] It was around this time the user base grew from hundreds of users to over ten thousand.[54] In February 2012, with the Silk Road still rapidly growing, the handler of the Silk Road administrator account publicly announced his role as a leader, as well as a name: the "Dread Pirate Rob-

46. *See id.* at 484 ("The complexity and depth of Tor's software has made it difficult for the NSA to find weaknesses or bugs.").

47. Nyshka Chandran, *From Drugs to Killers: Exploring the Deep Web*, CNBC: TECHNOLOGY (June 23, 2015, 10:07 PM), http://www.cnbc.com/2015/06/23/from-drugs-to-killers-exploring-the-deep-web.html.

48. *Id.*

49. *See* David Kushner, *The Darknet: Is the Government Destroying 'the Wild West of the Internet?'*, ROLLING STONE (Oct. 22, 2015), http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022 ("The Darknet lurks in the Deep Web, because the sites there can't be found by search engines either. But here's the big difference: The Darknet is composed of people and sites that want to remain anonymous and, unless you're using the Tor browser, are nearly impossible to find.").

50. Shroomery.org is a website discussing psychedelic mushroom experiences. Patrick Howell O'Neill, *The Definitive History of Silk Road*, DAILY DOT (Oct. 11, 2013, 9:00 AM), http://www.dailydot.com/crime/silk-road-drug-ross-ulbright-dread-pirate-roberts-history.

51. *Id.*

52. *Id.*

53. *See id.*; *see also* Adrian Chen, *The Underground Website Where You Can Buy any Drug Imaginable*, GAWKER (June 1, 2011, 3:20 PM), http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

54. *See* O'Neill, *supra* note 50.

erts."[55] Throughout the years the Silk Road operated, the Dread Pirate Roberts ("DPR") acted as the administrator and would often communicate with the users of the forum on philosophy and certain changes to the Silk Road.[56]

The Silk Road rapidly expanded throughout 2012 and 2013.[57] Users of the website could buy and sell anything from LSD, Crystal Meth, medical supplies, Steroids, hacked credit cards, tutorials on how to hack credit cards, child pornography, and even an arranged murder of another person (for around $150,000).[58] Vendors would communicate with patrons on the Silk Road primarily through encrypted messages under a system known as "Pretty Good Privacy" or "PGP."[59] Users would meet and purchase illegal goods in a setting similar to Amazon or eBay, with price-fixed listings, search options, and customer feedback.[60] There were only a few arrests during the three-year run of the Silk Road and virtually no known arrests in its first two years of operation.[61] The United States government has estimated that in its short lifespan, the Silk Road generated a total of $214 million in gross income.[62]

The Silk Road was shut down in October, 2013, largely due to a long investigation involving undercover DEA agent Carl Mark Force

55. *See* Joshua Bearman, *The Rise and Fall of Silk Road: Part* I, WIRED, http://www.wired.com/2015/04/silk-road-1/ (last visited Jan. 31, 2017). Specifically, the administrator wrote: "I am Silk Road, the market, the person, the enterprise, everything. But I need a name." The administrator named his persona after a character from the movie *The Princess Bride*, stating: "[m]y new name is: Dread Pirate Roberts." David Kushner, *Dead End on Silk Road: Internet Crime Kingpin Ross Ulbricht's Big Fall*, ROLLING STONE (Feb. 4, 2014), http://www.rollingstone.com/culture/news/dead-end-on-silk-road-internet-crime-kingpin-ross-ulbrichts-big-fall-20140204.

56. *See* Kushner, *supra* note 55.

57. *See* Kyle Soska & Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, USENIX SECURITY SYMP. 33, 40 (2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf ("In early 2013, we only have results for Silk Road, which at that point grossed around $300,000/day, far more than previously estimated for 2012.").

58. Anthony, *supra* note 3.

59. Soska & Christin, *supra* note 57, at 45 ("In the original Silk Road, only approximately 2/3 to 3/4 of vendors had a valid PGP key listed."); *see also* Dylan Love, *Edward Snowden: How to Make Sure the NSA Can't Read Your Email*, BUSINESS INSIDER (June 17, 2013, 4:18 PM), http://www.businessinsider.com/edward-snowden-email-encryption-works-against-the-nsa-2013-6. PGP encryption is a system of encryption that is virtually impossible for authorities to crack. *Id.* Only the sender and recipient of PGP encryption are able to view the messages between each other. *Id.* A third party would only be able to view the message as a series of randomized letters and numbers; the only way to decrypt the message is to own the private key of either the sender or recipient, and that is stored on the users' computers and protected by a user-created password. *Id.* For a brief history of PGP, as well as "government persecution" of its creator and technology, see also History, OPENPGP, http://www.openpgp.org/about_openpgp/history.shtml (last visited Jan. 31, 2017).

60. Soska & Christin, *supra* note 57, at 33 ("Silk Road itself did not sell any product, but provided a feedback system to rate vendors and buyers, as well as escrow services (to ensure that transactions were completed to everybody's satisfaction) and optional hedging services (to buffer fluctuations in the value of the bitcoin).").

61. *See* Olivia Solon, *Police Crack Down on Silk Road Following First Drug Dealer Conviction*, WIRED (Feb. 1, 2013), http://www.wired.co.uk/news/archive/2013-02/01/silk-road-crackdown.

62. Soska & Christin, *supra* note 57, at 40.

IV.[63] Force became involved with the Silk Road in 2012, assuming the username "Nob."[64] After establishing trust with DPR, Nob asked DPR to help arrange a buy of $27,000 worth of cocaine.[65] Federal agents then arrested the buyer that DPR set Nob up with to purchase cocaine.[66] In January of 2013, DPR was concerned the user would divulge incriminating information to the FBI, so DPR allegedly asked Nob to murder the employee.[67] Nob staged a hit of the employee in return for eighty thousand dollars, which led to an attempted murder charge against a man named Ross Ulbricht (which was later dropped).[68]

On or before July 23, 2013, investigators discovered at least one of the Silk Road servers, either in Latvia, Iceland, or Romania.[69] Shortly after, many Silk Road servers were found. This was particularly convenient timing for the investigation because on July 10, 2013, customs on the Canadian border intercepted a package of nine fake ID's that were sent to Ross Ulbricht's home.[70] Then, on July 26, 2013,—days after the Silk Road's first server was found—Homeland Security visited Ulbricht at his home in San Francisco, where he denied all involvement with the IDs.[71] Investigators also linked Ulbricht's Google email account and Google+

63. *See* Complaint, United States v. Carl Mark Force IV, No. 3-15-70370 (N.D. Cal. Mar. 25, 2015).

64. Kate Vinton, *Corrupt DEA Agent Pleads Guilty to Extorting Bitcoin from Silk Road Creator Ross Ulbricht*, FORBES (July 1, 2015, 8:82 PM), http://www.forbes.com/sites/katevinton/2015/07/01/corrupt-dea-agent-pleads-guilty-to-extorting-bitcoin-from-silk-road-creator-ross-ulbricht/. After Force's involvement with the investigation of the Silk Road, he was found guilty of embezzling over $300,000 in Bitcoin that he stole over his involvement with the Silk Road. *Id.* Force exchanged over $100,000 in Bitcoin from Dread Pirate Roberts for fake IDs and information regarding the DEA's investigation into the Silk Road. *Id.* Force also admitted to signing a $240,000 contract deal with 20th Century Fox for information on the Silk Road investigation, without approval from the DEA. *Id. See also* Plea Agreement at 1, United States v. Carl Mark Force IV, No. 46, 15 CR 319-RS (containing Force's admission of guilt). Force was sentenced six-and-a-half years in prison. *See* Sarah Jeong, *DEA Agent Who Faked a Murder and Took Bitcoins from Silk Road Explains Himself*, VICE: MOTHERBOARD (Oct. 20, 2015, 5:17 PM), http://motherboard.vice.com/read/dea-agent-who-faked-a-murder-and-took-bitcoins-from-silk-road-explains-himself.

A second investigator, Shaun Bridges, who is an ex-Secret Service agent, was also found guilty of embezzling over $800,000 in Bitcoin relating to the Silk Road investigation and shut-down. Alex Johnson, *Ex-Secret Service Agent to Plead Guilty to Silk Road Bitcoin Theft*, NBC NEWS (June 21, 2015, 6:25 PM), http://www.nbcnews.com/news/us-news/ex-secret-service-agent-plead-guilty-silk-road-bitcoin-theft-n379416.

65. Leinwand Leger, *supra* note 4.

66. *Id.*

67. *Id.*

68. *Id.* The attempted murder charges against Ulbricht were later dropped or unfounded in the indictment that went to trial. Patrick Howell O'Neill, *The Mystery of the Disappearing Silk Road Murder Charge*, DAILY DOT (Oct. 22, 2014, 2:20 PM), http://www.dailydot.com/crime/silk-road-murder-charges-ross-ulbricht/ ("To date, there have been precisely zero murder charges filed. Instead, the indictment has been changed without explanation, the formal charges omitted, and the broader accusations buried within a lesser drug trafficking charge.").

69. Leinwand Leger, *supra* note 4. It is unclear how investigators actually found the servers that hosted the Silk Road, as the website is run through Tor and virtually untraceable. This has been a large part of the controversy of this case.

70. *Id.* It would later be uncovered that DPR requested IDs with different names from users on the Silk Road in order to further diversify the Silk Road servers for increased security. *Id.*

71. *Id.* Ulbricht suggested that anyone could have used the Silk Road and ordered the IDs to his home. *See id.*

account with the user "altoid," who posted on the www.shroomery.org website first announcing the Silk Road.[72] With enough evidence and information linking Ulbricht to the Silk Road and DPR, Christopher Tarbell was granted an arrest warrant, and federal agents waited for Ulbricht to log onto his computer before arresting him at the San Francisco Public Library on October 1, 2013.[73] The Silk Road was shut down shortly after.

Ulbricht was formally charged with seven offenses for his involvement with the Silk Road, including: "distributing narcotics, distributing narcotics by means of the Internet, conspiring to distribute narcotics, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents, and conspiring to commit money laundering."[74] Ulbricht was convicted on five counts—receiving the maximum sentencing on each charge—resulting in two life sentences without parole plus forty years.[75] In addition, Ulbricht was fined over $183 million.[76] After a four-week jury trial, the judge presiding over the case explained his reasoning for the maximum sentence on each charge:

> There must be no doubt that lawlessness will not be tolerated. There must be no doubt that no one is above the law—no matter one's education or privileges. All stand equal before the law. There must be no doubt that you cannot run a massive criminal enterprise and because it occurred over the Internet minimize the crime committed on that basis.[77]

It appeared that the judge, in using choice language during sentencing, aimed to make a political statement and an example out of this case.

Although all of Ulbricht's crimes are technically nonviolent crimes, one count in particular stands out to many analysts of this case. Regardless of how the judge decided to sentence Ulbricht, the "engaging in a continuing criminal enterprise" charge carries with it a mandatory twenty-year minimum.[78] The charge is referred to as the "kingpin statute,"

72. Complaint at 24–27, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 14–cr–68 (KPF)).

73. *Id.* at 32–33; Leinwand Leger, *supra* note 4 ("The agents found the alleged Dread Pirate Roberts in the science fiction section.").

74. Press Release, FBI, Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison.

75. *Double Life Without Parole*, FREE ROSS ULBRICHT, https://freeross.org/sentencing/?v=7516fd43adaa (last visited Jan. 31, 2017) ("Distribution of Narcotics by Means of the Internet; Continuing Criminal Enterprise; Conspiracy to Commit and Aid and Abet Computer Hacking; Conspiracy to Traffic in Fraudulent Identity Documents; and Money Laundering Conspiracy.").

76. FBI, *supra* note 74.

77. *Id.*

78. Patrick Howell O'Neill, *How Silk Road's Ross Ulbricht Compares to Other Famous Drug Kingpins*, DAILY DOT (May 30, 2015, 1:06 PM), http://www.dailydot.com/crime/ross-ulbricht-kingpin-charges/.

and is normally reserved for gang leaders,[79] violent drug dealers,[80] and prolific mass murderers.[81] Regardless of whether these charges were just—the trial, conviction, and sentencing of Ross Ulbricht set a grave precedent for administrators of the numerous Silk Road-like Darknet markets that followed in its wake.

D. Expansion of Darknet Markets

The closure of the Silk Road was a very short-lived victory for law-enforcement authorities. As early as November, 2013, former administrators and users of Silk Road started the new marketplace "Silk Road 2.0."[82] Months later, even more marketplaces started offering the same services on these Darknet markets.[83] New markets became increasingly common during this time, and, as analysts have noted, the "closure of Silk Road did nothing to slow the growth of the top 11 marketplaces, including Silk Road 2.0, Agora, Pandora, Hydra, BlueSky, the Pirate Marketplace, Andromeda, Cloud 9, Evolution, 1776, among others which are constantly changing, opening and closing."[84] In fact, ten months after the Silk Road was shut down, the drug economy of the Darknet marketplace doubled.[85]

The U.N. World Drug Report of 2014 noted that "the variety [of drugs] available and purchased on the 'dark net' appears to be diverse and growing."[86] As of October, 2015, there are approximately thirty active Darknet marketplaces on the Deep Web.[87] Of these thirty markets, there are approximately 10,000 unique vendors, 80,000 unique listings, and approximately $650,000 worth of sales per day.[88] Although there are numerous vendors and marketplaces, the top 1% of vendors are accountable for over 50% of all trade volume.[89]

79. *Id.* ("Demetrius and Terry Flenory ran the Black Mafia Family from the 1980s to mid-2000s . . . . The Flenory brothers, who were accused of multiple murders throughout the 2000s, pleaded guilty to kingpin charges in 2007 and were sentenced to 30 years in prison.").

80. *Id.* ("The kingpin charge is regularly targeted at young convicts including Bilal Pretlow, who was 21 when a 1991 jury convicted him of running one of New Jersey's most successful and violent cocaine trafficking operations . . . . He's currently serving life in prison.").

81. *Id.* ("Rayful Edmund made his name with crack cocaine during the drug's apex in Washington, D.C. He was convicted of profiting over $300 million per year and committing dozens of murders every year to total over 400 murders, police said.").

82. Soska & Christin, *supra* note 57, at 33–34.

83. *Id.* at 34 ("[T]he anonymous online marketplace ecosystem had evolved significantly compared to the early days when Silk Road was nearly a monopoly.").

84. Mary M. Squyres & Nanette Norton, *The Darknet (the Deep Web)*, 3 TRADEMARK PRAC. THROUGHOUT THE WORLD § 30:43 (Apr. 2015).

85. Alix Culbertson, *Online Drugs Market Exploded After Darknet Silk Road Website Shut Down*, EXPRESS (June 8, 2015, 9:46AM),http://www.express.co.uk/news/world/582956/Online-drugs-market-exploded-after-Silk-Road-shut-down.

86. U.N. OFF. ON DRUGS & CRIME, WORLD DRUG REP. 2014, at 18, U.N. Sales No. E.14.XI.7 (2014).

87. Soska & Christin, *supra* note 57, at 35.

88. *Id.* at 40, 43, 47.

89. *Id.* at 44.

E. Common Characteristics of Darknet Markets

Each market shares a few common characteristics, such as a search engine and categorization of products, and each improves with every security breach, "exit scam,"[90] or law-enforcement shut down of a new Darknet market.[91] The first characteristic that each market shares is risk management for facilitating the primarily illegal transactions. Each market participant must interact anonymously and through the deep web, thereby "reduc[ing] (or indeed, eliminat[ing]) the potential for physical violence during the transaction."[92] Every major Darknet market is only accessible through a ".onion" web address, instead of the typical ".com" or ".net."[93] Some researchers have even claimed that this anonymous purchasing and receiving of drugs has the potential to reduce violence related to drug crimes by 50%.[94] One such reason for this reduction in violence could be that individuals are not meeting in person when they are conducting a drug transaction, which could reduce the chance for violence when a drug deal goes bad; in other words: "[p]eople who don't meet face to face can[no]t hit each other or shoot each other . . . ."[95]

A second characteristic each market shares is the "superior anonymity," which protects users, in most cases, from law enforcement.[96] Because items still need to be delivered to a user's home, though, he or she may not be completely protected from law enforcement.[97] Further, the recent trend has been to focus on suspicious packages coming from the Netherlands, as it is one of the biggest producers of MDMA and ecstasy tablets.[98]

90. An exit scam is when administrators of a Darknet market hold every vendor and buyer's Bitcoin in escrow before withdrawing them to a personal account and shutting down the Darknet market itself. For example, in early 2015, administrators of the Darknet market "Evolution" executed an exit scam, disappearing with over twelve million dollars worth of Bitcoin. Nicky Woolf, *Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear with $12m*, GUARDIAN (Mar. 18, 2015, 12:27 PM), http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars.

91. Soska & Christin, *supra* note 57, at 33.

92. *Id.* at 34.

93. L.M. Brownlee, *Appendix B. The Deep Web and the Dark Web—An Overview for Lawyers*, INTELL. PROP. DUE DILIGENCE IN CORP. TRANSACTIONS (Apr., 2015) (explaining that ".onion" web addresses are only accessible through Tor).

94. Andy Greenberg, *Silk Road Reduced Violence in the Drug Trade, Study Argues*, WIRED (June 2, 2014, 6:30 AM), http://www.wired.com/2014/06/silk-road-study/ ("Aldridge and Decary-Hetu say their data shows a vast portion of the Silk Road's sales were 'business-to-business.' That finding moves the market's role farther up the drug market supply chain than was previously thought . . . [,] placing it closer to the cartel-controlled drug producers behind much of the trade's violence. And since the study argues the traders on both sides of a Silk Road deal were often drug dealers, the researchers claim Silk Road's business-to-business deals mean twice as many opportunities for violence were prevented.").

95. *Id.* (quoting Aldrige) (internal quotations omitted).

96. Soska & Christin, *supra* note 57, at 34.

97. *Id.* at 34 n.2.

98. *See Authorities to Plan a Crackdown on Darknet Markets*, DARKWEBNEWS (Dec. 28, 2015), http://darkwebnews.com/darknet-markets/authorities-to-plan-a-crackdown-on-darknet-markets/ ("Dutch sellers contributed almost 10 percent of the total products sold on Silk Road 2.0, with a turnaround of $34 million.").

A third characteristic Darknet markets share is an escrow system to prevent financial risk in transactions. The system that most Darknet markets share is similar to that of eBay or Amazon. For example:

> Suppose Alice wants to purchase an item from Bob. Instead of directly paying Bob, she pays the marketplace operator, Oscar. Oscar then instructs Bob that he has received the payment, and that the item should be shipped. After Alice confirms receipt of the item, Oscar releases the money held in escrow to Bob. This allows the marketplace to adjudicate any dispute that could arise if Bob claims the item has been shipped, but Alice claims not to have received it. Some marketplaces claim to support Bitcoin's recently standardized "multisig" feature which allows a transaction to be redeemed if, e.g., two out of three parties agree on its validity. For instance, Alice and Bob could agree the funds be transferred without Oscar's explicit blessing, which prevents the escrow funds from being lost if the marketplace is seized or Oscar is incapacitated.[99]

Not all markets share a multisig feature, but almost all use a system of escrow for payment.

A fourth characteristic Darknet markets share—and perhaps the most important one for measuring sales volume—is the vendor-feedback system. After each sale or purchase, most markets provide a mandatory or voluntary feedback system where a user can rate the seller or product, similar to a product or user rating on Amazon.[100] This tells a potential buyer the quality of the goods being sold, the reliability of the vendor, and how much "stealth"[101] the vendor uses when shipping their illicit substance, as well as whatever personal feedback the buyer provides.[102] This system allows potential buyers to shop between vendors based on price and reliability—making the top vendors the easiest to find.

The safeguards and advantages for users engaging in illegal activity are increasing with each update on a Darknet market and each shutdown of a previous market. Users are free to shop amongst the various markets with negligible fear of law-enforcement involvement in their browsing and vending of illegal sales. Section II.F of this Note discusses the visitors of this virtual playing field; that is, the current agencies focused on ending the expansion of Darknet markets.

99. Soska & Christin, *supra* note 57, at 34–35.

100. *Id.* at 35.

101. "Stealth" is a term used to describe the methods that vendors use to conceal the identity of the illicit substance in the mail.

102. Soska & Christin, *supra* note 57, at 35; *see also* Carol Cadwalladr, *How I Bought Drugs from 'Dark Net'–It's Just Like Amazon Run by Cartels*, GUARDIAN (Oct. 5, 2013, 7:06 PM), http://www.theguardian.com/society/2013/oct/06/dark-net-drugs ("I looked on the UK cannabis forum, which had 30,000 postings, and a vendor called JesusOfRave was recommended. He had 100% feedback, promised 'stealth' packaging and boasted excellent customer reviews . . . .").

F. Government Agencies Capable of Addressing Darknet Markets

Numerous government agencies have both successfully and unsuccessfully tried to stop the growth and presence of Darknet markets on the Deep Web. The first public official to bring attention to the Silk Road—and thereby Darknet markets altogether—was Senator Chuck Schumer in 2011.[103] "Schumer said that as technology and cyber crime regarding illegal drug sales grows and develop, it is clear that the federal Department of Justice, FBI and DEA must review their procedures in handling these crimes, and place a greater priority on cracking down on these websites."[104] This Note only addresses the most suitable domestic agencies for discovering servers and identifying administrators and vendors—the Federal Bureau of Investigation ("FBI"), the Drug Enforcement Agency ("DEA"), and the National Security Agency ("NSA").

The FBI is the agency appropriately involved in discovering—and more directly pursuing—criminals involved in the Darknet markets. One of its main priorities is to "[c]ombat transnational/national criminal organizations and enterprises."[105] This portion of the FBI's task force normally focuses on the "33,000 violent street gangs, motorcycle gangs, and prison gangs with about 1.4 million members are criminally active in the U.S. and Puerto Rico today."[106] As stated previously, while Darknet markets have the potential to reduce violent crimes related to drug trade,[107] the FBI has been involved in "sting" operations in order to shut down these markets.[108] Employing undercover operatives is a successful technique the FBI has used many times to bust these extensive criminal enterprises. Most recently, the FBI claimed that the United States is capable of "cracking Tor" and identifying users of Darknet markets.[109] The accuracy of this claim will be addressed in Subsections III.A.1 of this Note.

Because so many drugs are bought and sold domestically and internationally through the dozens of Darknet markets on the Deep Web, the

103. *See* Press Release, Charles E. Schumer (Oct. 27, 2014), https://www.schumer.senate.gov/newsroom/press-releases/schumer-in-response-to-new-investigation-that-finds-illegal-online-drug-market-is-thriving-and-infiltrating-long-island-schumer-calls-for-top-to-bottom-dept-of-justice-review-of-how-dark-web-drug-sales-continue-to-grow_also-vows-increased-funding-to-better-target-cyber-drug-dealers.

104. *Id.*

105. *Mission & Priorities*, FBI, https://www.fbi.gov/about/mission (last visited Jan. 31, 2017).

106. *Gangs*, FBI, https://www.fbi.gov/about-us/investigate/vc_majorthefts/gangs/gangs (last visited Jan. 31, 2017); *see also 2011 National Gang Assessment Report*, FBI, https://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment (last visited Jan. 31, 2017) (noting that "gangs are responsible for an average of 48 percent of violent crime in most jurisdictions, and up to 90 percent in others.").

107. This may be so by reducing the amount of in-person interactions between buyers and sellers. *See supra* text accompanying notes 93–94.

108. *See, e.g.*, Leger, *supra* note 65.

109. Dan Froomkin, *FBI Director Claims Tor and the "Dark Web" Won't Let Criminals Hide From His Agents*, INTERCEPT (Sept. 10, 2015, 4:08 PM), https://theintercept.com/2015/09/10/comey-asserts-tors-dark-web-longer-dark-fbi/.

federal DEA has significant involvement with this field. In fact, the DEA is responsible for approximately 30,000 domestic arrests relating to drug offenses per year.[110] For instance:

a. In 2010, prior to the founding of the Silk Road, the DEA seized roughly: 30,000 kilograms of cocaine; 700 kilograms of heroin; 725,000 kilograms of marijuana; 2,000 kilograms of methamphetamine; and 2,600,000 dosage units of hallucinogens.[111]

b. In comparison, in 2014 (three years after the Silk Road's founding), the DEA seized roughly: 33,000 kilograms of cocaine; 1,000 kilograms of heroin; 25,000 kilograms of marijuana; 2,700 kilograms of methamphetamine; and 50,000 dosage units of hallucinogens.[112]

Whether these findings have any relation to the creation of Darknet markets will be addressed in Part IV of this Note. Notwithstanding, the DEA's involvement in the Silk Road investigation was an extensive investigation involving special agent Carl Mark Force IV, which resulted in Force being charged with, and convicted of, embezzlement and sentenced to six and a half years in prison.[113] The DEA's involvement in Darknet markets are, thus, directly linked to undercover operations and the seizure of drugs processed through these markets.

The NSA "is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes."[114] Its goal is to "[c]ollect, [a]nalyze, and [r]eport intelligence needed to protect national security."[115] Its two main power sources in doing so are through Executive Order 12333 and the Foreign Intelligence Surveillance Act of 1978.[116] Through these powers, the NSA touches over 29,000 terabytes of information processed on the Internet per day.[117] To put this in perspective, one email (text only) is approximately thirty-five kilobytes of data.[118] Additionally, one standard web page is around 180 kilobytes of data.[119] This is the equivalent of 900 trillion emails per day, or the surveillance of 170 trillion websites.[120]

110. *Statistics and Facts*, DEA, http://www.dea.gov/resource-center/statistics.shtml (last visited Jan. 31, 2017).

111. *Id.*

112. *Id.*

113. *See supra* text accompanying note 64.

114. *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, NAT'L SEC. AGENCY (Aug. 9, 2013), https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml.

115. *Id.*

116. *Id.* ("Under Section 702 of the FISA, NSA is authorized to target non-U.S. persons who are reasonably believed to be located outside the United States.").

117. *Id.*

118. *Monthly Data Usage Estimate*, U.S. CELLULAR, http://www.uscellular.com/data/data-estimator.html (last visited Jan. 31, 2017).

119. *Id.*

120. This math is based on the amount of kilobytes in a terabyte. Then, the total kilobytes in NSA processing are divided by thirty-five (text email) and 180 kilobytes (standard web page), respectively. The results are an approximation.

Even though this amount of data surveillance may seem excessive, the NSA has specific internal oversight procedures and regulations in place to ensure that compliance with domestic and international foreign agencies does not subsequently violate other laws.[121] Further, "NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure."[122] Whether these procedures are being followed will be addressed later in this Note.

G. Current Laws Capable of Addressing Darknet Markets

Legislators have called for action over the years to ban or heavily regulate bitcoin, Tor, and, of course, Darknet markets altogether. For example, in 2013, Senator Joe Manchin of West Virginia addressed a letter to federal regulators that "urge[d] the regulators to work together, act quickly, and prohibit this dangerous currency from harming hard-working Americans."[123]

While there does not appear to be any recent legislation looking to ban the use of bitcoin or Tor generally, there are certain laws the government has tried to use—or that have the potential to be used—in the pursuit and prosecution of users of Darknet markets. The relevant acts discussed in Part III.B are the Bank Secrecy Act, the All Writs Act, the Cybersecurity Information Security Act, and the Digital Millennium Copyright Act.

III. ANALYSIS

The legal and criminal arena that has been exposed in Part II of this Note is large and always expanding. It is insurmountable to analyze every aspect of the relevant agencies and applicable laws that could contain the issue of Darknet market use. As such, this Note takes a narrow approach and will examine specific agency claims and the most potentially relevant laws at issue. This Part will address the legitimacy of agency claims, as well as the applicability of current laws and regulations focused on identifying and prosecuting users of Darknet markets. It will discuss the successes or failures of developments in technology related to identifying Darknet-market servers and users. It will also address the efficiency of using undercover federal agents in identifying the top Darknet vendors.

121. *See* NAT'L SEC. AGENCY, *supra* note 114.

122. *Id.* ("If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to constantly improve.").

123. Devin Coldeway, *Senator Calls for Total Ban of 'Dangerous' Bitcoin*, NBC NEWS (Feb. 26, 2014, 9:57 PM), http://www.nbcnews.com/tech/innovation/senator-calls-total-ban-dangerous-bitcoin-n39541 (quoting Joe Manchin) (internal quotations omitted). On February 27, 2014, The Bitcoin Foundation replied to Sen. Manchin, consoling: "[t]here is no need to fear Bitcoin or overreact to the challenges that accompany its huge potential benefits." *Id.* (internal quotations omitted).

A. Legitimacy of Agency Claims Against Darknet Control

A common technique in law enforcement is to bluff in order to scare a potential criminal into either not participating in a crime or giving up an accomplice to save him or herself from jail time. While this may work from time to time, the sophisticated criminals on Darknet markets have the tools and knowledge to evaluate whether these claims are legitimate. Transparency is key in defining an approach to solving the Darknet issue. Accordingly, claims made by law enforcement agencies will be analyzed in this Part before a recommendation can be made on the next appropriate steps to take.

1. Casting Doubt on the FBI's Claim of "Cracking Tor"

FBI director James Comey recently stated that criminals who use Tor "think that if they go to the dark web that they can hide from us. They're kidding themselves, because of the effort that's been put in by all of us in the government over the last five years or so, that they are out of our view."[124] Comey's claim was directed at pedophiles sharing illegal content of children, but the implication extends to any user of Tor, whether they are on the Darknet or the Deep Web.[125] Cryptography expert Bruce Schneier noted that this statement should not be taken at face value. Considering the FBI has lied about being able to crack Tor before, he says, "the truth value is irrelevant."[126] Comey's statements relating to the ability of the FBI to "crack Tor" are more than likely puffery, as he has refused to accept the reality from security and cryptography experts many times before.[127]

A sweeping identification of Tor users at this point is likely impossible, as there are over 5,000 nodes in the world that scramble the pathway between the user and destination of Darknet marketplace.[128] Tor expert Ivan Pustogarov, however, has suggested that if the government can control enough nodes (or "relays"), it would perhaps be possible for an agencies' node to be the exit node connected to the Darknet market's server.[129] Pustogarov's findings indicate that if the FBI invested $12,000 a month in renting "relays" over a twelve-month period, it would have a

124. *Comey: Dark Web Isn't Dark to Him*, C-SPAN (Sept. 10, 2015), http://www.c-span.org/video/?c4550513/comey-dark-web-isnt-dark.

125. Froomkin, *supra* note 109.

126. *Id.*

127. *See, e.g.*, Jenna McLaughlin, *FBI Director Says Scientists Are Wrong, Pitches Imaginary Solution to Encryption Dilemma*, INTERCEPT (July 8, 2015, 4:39 PM), https://theintercept.com/2015/07/08/fbi-director-comey-proposes-imaginary-solution-encryption/ (quoting Comey, stating that "[a] whole lot of good people have said it's too hard . . . [,] maybe that's so. But my reaction to that is: I'm not sure they've really tried.").

128. *See supra* Section II.B.

129. Eric Markowitz, *This Is (Probably) How the FBI Took Down Blake Benthall Last Week*, VOCATIV (Nov. 12, 2014 7:16 AM), http://www.vocativ.com/tech/internet/blake-benthall/.

"99% probability to locate a specific hidden service."[130] This finding suggests that the FBI could have located servers with this method, but that they still would not be able to identify top-level vendors of Darknet markets because the subsequent nodes back to the original user would still be far too many to breach.[131] Therefore, the use of renting relays could be useful for identifying large servers now,[132] but, as the decentralization of Darknet markets grows, it will not be able to keep up.

The FBI has had some success in its claim of "cracking Tor" through the closure of a child pornography deep-web site "Playpen."[133] Playpen was a dark-web site that housed over 200,000 unique users and over 100,000 postings containing "extreme child abuse imagery, as well as providing advice on how potential child sex abusers could avoid detection online."[134] The FBI first seized the server and then ran the site through its own servers for two weeks.[135] When an individual accessed the website, the FBI used a "Network Investigative Technique," or "NIT," to identify users' IP addresses and, subsequently, their identity.[136] Throughout the two weeks the FBI hosted the child-pornography website and how-to guide, it identified approximately 1,300 users—all from a single issued warrant.[137]

The implication of the FBI using this technique is startling. For example, suppose the FBI obtains one warrant to search Susan's—a known drug dealer—house for drugs. After reaching Susan's house and arresting her, the FBI operates the house to catch more drug users. During the two weeks the FBI peddles drugs from Susan's house, they identify 1,500 drug users. The FBI then uses that same warrant to search the drug user's cell phones, personal belongings, and any other private information amassed over years—whether related or not—all from that first initial warrant. This is essentially what happened here. Even if the court allows this search to survive constitutional challenges, the consequences stemming from the FBI using this technique for "cracking Tor" to identify Darknet-market users should not be taken lightly.

130. *Id.*

131. Jason Koebler, *How the NSA (or Anyone Else) Can Crack Tor's Anonymity*, MOTHERBOARD (Nov. 19, 2014, 7:00 AM), http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity.

132. As Tor grows, more nodes and relays will grow as well. The method for the FBI to locate servers is a short-term solution, unless even more money is spent renting relays and identifying servers.

133. *See* Mary-Ann Russon, *FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web*, INT'L BUS. TIMES (Jan. 6, 2016), http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417.

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.* ("The NIT was able to capture the actual IP address of the computer, the type of operating system the user's computer was using, the computer's architecture, the computer's MAC address, the computer's host name, the computer's active operating system username and was even able to issue a unique identifier to the user in order to distinguish all data collected from another user's IP address.").

2. *NSA's Use of Parallel Construction in Finding Darknet Servers*

There is significant concern regarding the NSA's ability to locate the servers related to the shut down of the first Silk Road, as well as the Silk Road 2.0.[138] "Parallel Construction" is a technique from the NSA that uses "considerable technological power to find alleged criminality outside its jurisdiction, without a warrant, and then tips its findings to a relevant law enforcement agency, trusting them to find evidence once they already know their suspect."[139] This was likely not the case in the original Silk Road shut-down where, on September 9, 2014, FBI agent Christopher Tarbell discovered that the method for discovering the Silk Road was through an IP leak in the Silk Road's server's "CAPTCHA" login screen.[140] It is undetermined, however, whether this was the method used to locate the server of Silk Road 2.0.[141] As more evidence from the Ross Ulbricht appeal comes to light, as well as information regarding the shut down of the Silk Road 2.0, claims against the NSA conducting illegal surveillance regarding Tor and Darknet servers will be judged more accurately.

Notwithstanding inconsistencies in discovery from the Silk Road trials, recent evidence has emerged that the NSA will be able to bypass privacy concerns in order to share information with other agencies.[142] Executive Order 12333 is a Reagan-era document issued in 1981 that the NSA has used to justify surveillance of data centers from both Yahoo and Google.[143] As of the writing of this Note, Executive Order 12333 allows the NSA to "incidentally" intercept American private messages as a result of foreign surveillance.[144] This allows the NSA to gather information on a massive scale, but "not share raw 12333 intercepts with other agencies, like the F.B.I. or the C.I.A., to search for their own purposes."[145] Traditionally, the FBI's access to this information came after any identifying information has been removed.[146] But, in light of locating servers and administrators, the new proposal to Executive Order 12333 would allow the FBI to "obtain direct access to raw information from the

138. *See* Kevin Collier, *How the FBI Busted Silk Road 2.0 Before It Even Launched*, DAILY DOT (Nov. 7, 2014, 1:05 PM), http://www.dailydot.com/crime/blake-benthall-fbi-bust/.

139. *Id.*

140. Declaration of Christopher Tarbell at 3, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 1:14-cr-00068-KBF).

141. *See* Collier, *supra* note 138.

142. *See* Charlie Savage, *Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts*, N.Y. TIMES (Feb. 25, 2016), http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html?_r=0.

143. Joel Hruska, *New NSA Rules Allow Agency to Share Data Without Privacy Protections or Terrorism Links*, EXTREMETECH (Mar. 11, 2016, 10:00 AM), http://www.extremetech.com/internet/224565-new-nsa-rules-allow-agency-to-share-data-without-privacy-protections-or-terrorism-links.

144. Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. TIMES (Aug. 13, 2014), http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.

145. *Id.*

146. *See id.*

N.S.A.'s surveillance to evaluate for themselves[,]" under the semblance of "national security."[147] Essentially, this would eliminate some concerns regarding the use of "parallel construction," but it would do so by avoiding traditional Fourth Amendment protections.[148]

B. Applicability of Current Laws

Numerous existing laws and proposed legislation are capable of addressing the issue of identifying, classifying, and prosecuting users and administrators of Darknet markets. Aside from the typical charges that will stick when an administrator or vendor is caught, there are other laws that appear to be useful for identifying and apprehending these individuals before that happens. Specifically, three laws have recently garnered attention for applicability to bitcoin money laundering, tracking and decrypting sophisticated mobile devices, and transferring mass, potentially identifying information regarding threats to cybersecurity. This Section discusses the Bank Secrecy Act, the All Writs Act, the Cybersecurity Information Sharing Act, and the Digital Millennium Copyright Act.

1. Adequacy of the Bank Secrecy Act

One of the main issues with capturing vendors of illegal substances and services on Darknet markets is addressing the issue of money laundering. One method the United States has attempted to use to combat this activity has been through the Bank Secrecy Act of 1970 ("BSA").[149] The United States has attempted to fit bitcoin users and entities into groups capable of being regulated under the BSA by classifying them as money services businesses ("MSBs").[150] Specifically, the category of MSB's government agencies try to categorize users under is the "money transmitters" category, which the Code of Federal Regulations defines as "[a] person that provides . . . the acceptance of currency, funds, or other value that substitutes for currency . . . and the transmission of currency . . . to another location or person by any other means."[151] Transmitting bitcoins to another user for drugs or elicit purposes would not be defined as the "other value that substitutes for currency" definition.[152]

147. Hruska, *supra* note 143.

148. *See id.* ("For now, the government still argues that these rules apply to foreign communication, not domestic—but how long before these rules fall as well? After all, there's no rule that says Americans can't commit terrorism within the United States.").

149. *See* Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529, 543–44 (2014).

150. *Id.* at 536 ("MSBs include: (1) any person doing business, whether or not on a regular basis, as currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders or stored value; (4) sellers or redeemers of traveler's checks, money orders or stored value; (5) money transmitters; and (6) the U.S. Postal Service.").

151. *See id.*; 31 C.F.R. § 1010.100 (2015) ("'Any means' includes, but is not limited to, through a financial agency or institution; . . . an electronic funds transfer network; or an informal value transfer system; or . . . [a]ny other person engaged in the transfer of funds.").

152. Penrose, *supra* note 149, at 540–41.

The BSA was amended by the Money Laundering Control Act of 1986, which defined federal criminalization of money laundering as including criminal and civil forfeiture of BSA violations.[153] While this would be an effective means for capturing large-volume traders of bitcoins, regulators take issue with defining bitcoin as "currency."[154] Accordingly, the Financial Crimes Enforcement Network ("FinCEN") issued guidance in 2013 on how anti-laundering laws can affect virtual currencies such as bitcoin.[155] Specifically, the guidance states:

> A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter. In addition, a person is an exchanger and a money transmitter if the person accepts such decentralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.[156]

This covers "miners" who sell bitcoins to other users for real money as money transmitters and, thus, are punishable under the BSA.[157] It also covers users who receive bitcoins from a miner and then transfers it as part of the same transaction to another user for funds.[158] While this is a step in the right direction for getting to users of bitcoin transmitting services under an anti-laundering scheme, it does not cover users who trade bitcoins for real or virtual goods and services. Therefore, while FinCEN's guidelines may be able to handle heavy bitcoin-to-real-money launderers, it is inadequate to cover users who are not involved in the mining process, which is the majority of Darknet market vendors.

2. *Evolution and Application of the All Writs Act*

There has been growing concern and conversation over the government's ability to use the All Writs Act in order to access an individual's encrypted smart-phone device, which could have broader implica-

153. *Id.* at 537–38.

154. *Id.* at 542; 31 C.F.R. § 1010.100(m) (defining currency as "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance.").

155. *See* MURPHY ET AL., *supra* note 8, at 12–13; U.S. DEP'T TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013).

156. U.S. DEP'T TREASURY, *supra* note 155.

157. *See* MURPHY ET AL., *supra* note 8, at 2.

158. *See* MURPHY ET AL., *supra* note 8, at 1–2.

tions to access laptops and IP addresses of Darknet users.[159] The All Writs Act, enacted in 1789, provides, in relevant part that: "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[160] In 1976, the Supreme Court recognized that the All Writs Act could be used by the judiciary to involve third parties who are not part of the original action, to turn over customer information.[161]

In *United States v. New York Telephone Co.*, the Supreme Court allowed a district court to assist the government in installing a "pen register"—a device used to record dialed phone numbers—to a customer's phone.[162] While the Court allowed the pen register to be installed, it noted that "the power of federal courts to impose duties upon third parties is not without limits; *unreasonable burdens* may not be imposed."[163] Albeit, this case was decided in 1977, and smartphone technology was nowhere near developed yet;[164] however, the implication of using the All Writs Act for current mobile technology raises significant concerns regarding government abuse of privacy.

The Supreme Court has explained that the All Writs Act should only be used to issue writs when another statute does not address the current issue.[165] It "empowers federal courts to fashion extraordinary remedies when the need arises . . . ."[166] District courts have been divided on when to apply the statute to phone manufacturers and when to deny it.[167] In fact, a United States Magistrate judge expressed grave concern in a slip opinion issued in 2005 regarding this very issue:

> Thus, as far as I can tell, the government proposes that I use the All Writs Act in an entirely unprecedented way. To appreciate just how unprecedented the argument is, it is necessary to recognize that the

159. *See, e.g.*, Andrew Crocker, *Sifting Fact from Fiction with All Writs and Encryption: No Backdoors*, EFF (Dec. 3, 2014), https://www.eff.org/deeplinks/2014/12/sifting-fact-fiction-all-writs-and-encryption-no-backdoors.

160. 28 U.S.C. § 1651(a) (2012).

161. United States v. New York Tel. Co., 434 U.S. 159, 174 (1977) ("The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice . . . .").

162. In re XXX, Inc., No. 14 MAG. 2258, 2014 WL 5510865, at *1 (S.D.N.Y. Oct. 31, 2014) (citing *New York tel. Co.*, 434 U.S at 172–75).

163. *New York Tel Co.*, 434 U.S. at 172 (emphasis added).

164. *See id.* at 159.

165. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

166. *Id.* ("[I]t does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate.").

167. *Compare In Re XXX, Inc.*, No. 14 MAG. at *2–3 (granting the government's application for an order under the act that directs the manufacturer to provide "reasonable technical assistance" in unlocking a smartphone, but allowing the manufacturer to delay assistance if compliance with the order would be "unreasonably burdensome") *with* In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 327 (E.D.N.Y. 2005) (refusing to allow the Government to "turn a mobile telephone into a means for contemporaneously tracking the movements of its user").

> government need only run this Hail Mary play if its arguments under the electronic surveillance and disclosure statutes fail. . . . But if, as explained above, those statutes do not authorize the acquisition of cell site information on a showing less exacting than probable cause, there is no way I can plausibly decide that ordering such relief is even consistent with principles of law, let alone in aid of them. . . .
>
> The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.[168]

This opinion was issued in 2005, and since that time the FBI has been more interested in using this controversial piece of legislature.

More recently, the government has tried to compel Apple using the All Writs Act to provide a backdoor for unlocked encrypted mobile devices.[169] Apple has argued that, if iOS 8 is run on a device, it "can't unlock your device for anyone because you hold the key—your unique password."[170] When brought before a federal magistrate judge in Brooklyn, Judge Orenstein refused to require Apple to comply with the order, notingthat it is "a private–sector company that is free to choose to promote its customers' interest in privacy over the competing interest of law enforcement."[171] This statement reiterates that third-party companies are not required to bypass and implement technology in order to assist the government because it would be unreasonably burdensome—unless certain exceptions apply.

One exception that a magistrate judge in California found in allowing the government to use the All Writs Act was concerning a mass shooting in San Bernardino, California. In an order issued on February 16, 2016, Judge Sheri Pym wrote that: "Apple shall assist in enabling the search . . . pursuant to a warrant of this Court by providing reasonable technical assistance to assist law enforcement agents in obtaining access to the data on the SUBJECT DEVICE."[172] Apple CEO Tim Cook responded to this order by urging legislators to keep up with current tech-

168. *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d at 326.

169. *See* Andrew Crocker, *Judge to DOJ: Not All Writs*, EFF (Oct. 12, 2015), https://www.eff.org/deeplinks/2015/10/judge-doj-not-all-writs#footnote1_q8i8unb.

170. *Id.*

171. *Id.* (quoting Judge James Orenstein).

172. *In re* Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016).

nology instead of using outdated and inapplicable statutes.[173] Regardless of how higher courts rule on Apple's appeal of this order, the precedent that may be set will likely be limited to terrorist attacks, as on more than a dozen occasions judges have sided with Apple in denying the government's right to access iPhones.[174]

The disposition and reservation of various federal judges—as well as private companies, such as Apple[175]—to refuse to apply the All Writs Act in enabling the government to decrypt sensitive information on cell phones provides a roadblock in the FBI's pursuit to stopping users of Darknet markets. As the decision to not implement legislation requiring firms to decrypt data in order to assist law enforcement agencies has been echoed by the Obama administration itself,[176] the All Writs Act appeared to be the government's best ability to get around requiring probable cause and other significant constitutional concerns when accessing encrypted data from private companies. This was until the Cybersecurity Information Sharing Act ("CISA") was signed into law on December 18, 2015.[177] Nevertheless, the broad implication that the All Writs Act could be used to access private servers and users hiding behind Tor will be addressed in Section IV.B.

3. Unearthing the Controversial Cybersecurity Information Sharing Act

CISA is a controversial piece of legislation, conveniently inserted into a 2,000 page spending bill, which was signed into law on December 18, 2015.[178] The primary focus of CISA is to gather support from companies and to encourage them to share information between other companies, and with the government, regarding "cybersecurity threats."[179] A significant concern is that privacy will be swept under the rug in order to defend against a perceived threat of cybersecurity. The broader implication would be an exchange such as Coinbase transferring sensitive information to authorities; another is that administrators of Tor will relay

173. Laura Sydell, *Can a 1789 Law Apply to an iPhone?*, NPR (Feb. 19, 2016, 7:18 AM), http://www.npr.org/sections/alltechconsidered/2016/02/19/467299024/can-a-1789-law-apply-to-an-iphone.

174. *See Apple Can't be Forced to Provide iPhone Data in Drug Case, Judge Rules*, CBCNEWS (Feb. 29, 2016, 6:03 PM), http://www.cbc.ca/news/world/apple-iphone-data-judge-drug-case-1.3469938.

175. *See* Oscar Raymundo, *Facebook, Google, Twitter, Woz, Trump, McAfee, Snowden, and More Take Sides on Apple vs. the FBI*, MACWORLD (Feb. 19, 2016, 4:23 AM), http://www.macworld.com/article/3034979/security/facebook-google-twitter-woz-trump-mcafee-snowden-and-more-take-sides-on-apple-vs-the-fbi.html.

176. *See* Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data—For Now*, WASH. POST (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

177. Graeme Caldwell, *Why You Should Be Concerned About the Cybersecurity Information Sharing Act*, TECHCRUNCH (Feb. 7, 2016), http://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/.

178. Hogan Lovells, *Key U.S. Cybersecurity Provisions Signed into Law*, IAPP (Jan. 5, 2016), https://iapp.org/news/a/key-u-s-cybersecurity-provisions-signed-into-law.

179. *See id.*

nodes or Internet service providers themselves will give up IP addresses of users browsing Darknet markets or information regarding Darknet markets.

In response to these privacy interests, Congress inserted several provisions in an attempt to preserve privacy interests and focus on the issue of cybersecurity. First, Section 103 of CISA, regarding cybersecurity threats "ensure[s] the Federal Government has and maintains the capability to share cyber threat indicators *in real time* consistent with the protection of classified information . . . ."[180] This encourages CISA to be used only in real time when the information can best be utilized; in other words, exposing information about past threats or identifying information is discouraged through the use of this act.[181]

Next, and perhaps most important for the purposes of this Note, are provisions requiring the federal government to classify information regarding identifying information. Also, Section 103 of this act demands procedures used in furtherance of this act shall:

> (E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—
>
> (i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and *remove such information*; or
>
> (ii) to implement and utilize a technical capability configured to *remove any personal information or information that identifies a specific person not directly related to a cybersecurity threat* . . . .[182]

These provisions imply that the federal government may even be required to implement a specific procedure or program that removes all personal information before exploring the cybersecurity threat further. In addition, this protection extends to private entities before the sharing of personal information regarding a threat in security.[183]

Third, many Americans hold understandable concerns that the government will not be transparent in the use of CISA, and that government employees will abuse the act to get around privacy blocks at their own discretion.[184] As the Financial Services Roundtable (a financial services lobbying and advocacy organization) has noted, though, "CISA makes sure government employees who misuse shared cyber threat information

180. Cybersecurity Information Sharing Act of 2015, H.R. 753, 114th Cong. § 103(b)(1)(A) (2015) (emphasis added).

181. *Privacy Groups are Spreading CISA Myths: Let's Get the Facts Straight from the Bill*, FSR BITS (last visited Jan. 31, 2017) [hereinafter *CISA Myths*], http://fsroundtable.org/privacy-groups-are-spreading-cisa-myths/ .

182. 6 U.S.C. § 103(b)(1)(E) (2012) (emphasis added).

183. *See CISA Myths*, *supra* note 181 ("It doesn't get a whole lot clearer—CISA requires the removal of personal information. This empowers companies to PROTECT consumer personal information."); *accord* § 104(d)(2).

184. *CISA Myths*, *supra* note 181.

face appropriate sanctions."[185] In addition, "CISA requires the Attorney General to be transparent and to clearly explain to the public the guidelines by which cyber threat indicators and related information will be used."[186] It is apparent, then, that the drafters of CISA provided many safeguards so as not to disintegrate privacy and anonymity on the Internet.

CISA does not *require* any company to share information with the government regarding a threat to cybersecurity. Rather, CISA is a law that allows a company to share information *voluntarily* with other companies or the federal government in order to prevent threats to cybersecurity.[187] The actual use of this law has not yet been determined, as it has just recently passed. Whether this means CISA could apply to Darknet markets, and even Cryptocurrency exchanges, will be addressed in Section IV.B.

4. Usefulness of the Digital Millennium Copyright Act

The Digital Millennium Copyright Act ("DMCA") could provide a potential avenue for law enforcement to identify users of Darknet markets in order to get a better picture of who these individuals are and the next steps to take in order to prosecute them. Plaintiffs have the option to use the DMCA in order to bring a civil suit against anonymous individuals for copyright infringement over the Internet.[188] In order to bring this suit in front of a court, a plaintiff has the option of subpoenaing the target individual's Internet service provider in order to "unmask" the user to reveal personal details.[189]

Section 512(h) of the DMCA provides in relevant part:

> (h) Subpoena to identify infringer.—
> (1) Request.—A copyright owner or a person authorized to act on the owner's behalf 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.
> (2) Contents of request.—The request may be made by filing with the clerk—
> (A) a copy of a notification described in subsection (c)(3)(A);
> (B) a proposed subpoena; and
> (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that *such information will only be used for the purpose of protecting rights under this title*.

185. *Id.*
186. *Id.*
187. *See id.*
188. *See* 17 U.S.C. § 512 (2012); Alice Huang, *Reaching Within Silk Road: The Need for a New Subpoena Power that Targets Illegal Bitcoin Transactions*, 56 B.C. L. Rev. 2093, 2117 (2015).
189. *See* Huang, *supra* note 188, at 2117.

> (3) Contents of subpoena.—The subpoena shall *authorize and order* the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner *or person authorized by the copyright owner* information sufficient to *identify the alleged infringer* of the material described in the notification to the extent such information is available to the service provider.[190]

It is evident from the statute that there are several hurdles a law-enforcement agency would have to clear in order to unmask these users and find other ways to prosecute them. For example, in Section 512(h)(2)(c), the information must be used only for protecting an individual's right to copyright.[191] Even though a "person authorized by the copyright owner" may have the information brought to him,[192] it may be difficult for a court to order a search warrant based on the limitations provided in the DMCA.

A further limitation on using the DMCA to unmask Darknet market administrators and users is how the courts have interpreted the act over time. Courts have recognized the subpoena power of the DMCA only extends to Internet service providers that store information on their servers.[193] This means an individual who is using the Internet to browse information or communicate is not subject to a subpoena requested through the DMCA.[194] Courts tend to uphold a First Amendment interest in securing anonymity through the Internet.[195] This has led to a rejection of DMCA subpoenas unless there is a legitimate, factual reason for the alleged copyright infringement.[196] The practical uses of the DMCA will be addressed in Subsection IV.B.4.

C. Groundwork: Undercover Agents and Tracking Seized Packages

There has not been a clear scientific consensus on admitting expert testimony for analyzing data relating to identification of the two FBI busts of the two Silk Roads.[197] The probability of analysts tracking bitcoins from illegal transactions to specific IP addresses under established standards "should not be admitted due to their lack of general acceptance" in court proceedings.[198] Until new developments are made and the price and amount of bitcoin transactions stabilize, government agen-

190. § 512(h)(3).
191. *See* § 512(h)(2)(c).
192. § 512(h)(3).
193. *See* Huang, *supra* note 188, at 2117.
194. *See id.*
195. *Id.*
196. *See id.* at 2118; *see also* Doe v. Cahill, 884 A.2d 451, 457 (Del. 2005) ("The possibility of losing anonymity in a future lawsuit could intimidate anonymous posters into self-censoring their comments or simply not commenting at all.").
197. *See* Jason Luu & Edward J. Imwinkelried, *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics* (Sch. of Law Univ. Cal., Davis, Legal Studies Res. Paper No. 462), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671921.
198. *Id.* at 50.

cies need to rely on other methods to continue admitting evidence of discovering these servers.

One way this has been accomplished is through undercover agents and tracking seized packages. Currently, the FBI has had success infiltrating the higher ranks of Darknet administrators, but it has run into problems trying to explain to the courts the efforts it has used to locate servers.[199] The reliability of judges in granting motions to compel the government to divulge what techniques it used may not work if the information is under the guise of a "military problem."[200] Undercover agents were used in identifying Ross Ulbricht, and they could be relied upon more to double efforts in locating top vendors and, potentially, website administrators. This could be coupled with U.S. Customs discovery of seized packages, leading to more communication with top vendors in exchange for immunity. A more specific approach will be discussed in Section IV.A.

IV. RECOMMENDATION

Navigating the arena between privacy and crime has always been a significant concern to law enforcement, individuals, and, most importantly, legislators. This is especially challenging in the context of Bitcoin and Darknet markets. This Part suggests making general updates on practices used in the United States Code, as well as a reformulation of law-enforcement efforts related to Darknet transactions. It also addresses the shortcomings of current legislature and government agencies, while attempting to mitigate concerns with preserving anonymity and privacy on the Internet.

A. Get with the Times: Reformulating the Approach to Law-Enforcement Efforts

Current law-enforcement efforts are focused on locating servers and then prosecuting the administrators of the Darknet markets that servers are related to.[201] These agencies are not learning from the expansion of decentralized markets—it is not locating the servers that is the problem, it is locating the top-selling vendors and the vendors of more dangerous substances such as guns, child pornography, hacked credit cards, and arranged murders. The FBI should stop seeking a method to crack Tor[202]

199. *See* Bingo Boingo, *Silk Road 2.0 Case Confirms FBI and CMU Tor Attack Collaboration*, QNTRA (Feb. 24, 2016), http://qntra.net/2016/02/silk-road-2-0-case-confirms-fbi-and-cmu-tor-attack-collaboration/.

200. *Id.*

201. Andy Greenberg, *FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking*, WIRED (Sept. 8, 2014, 3:33 PM), https://www.wired.com/2014/09/fbi-silk-road-hacking-question.

202. Ashley Carman, *Carnegie Mellon Denies It Was Paid to Help the FBI Crack Tor: It Might have Done the FBI's Work for Free, Though*, VERGE (Nov. 18, 2015), http://www.theverge.com/2015/11/18/9757904/Carnegie-Mellon-Tor-Anonymous-Research.

and should instead focus its efforts on undercover agents like Christopher Tarbell targeting top vendors and bringing them down first.

One way this could be achieved would be to establish relationships with top vendors that are successful on Darknet markets. If the FBI wants to curtail the influx of high quantities of drugs and weapons entering the country, it should rely upon methods that are established and successful in order to avoid procedural errors in court proceedings. Creating accounts and leaving feedback with vendors would be a way to establish trust, and, over time, the NSA or FBI could track the specific amount of bitcoins sent to the vendor through the Darknet market itself. Further, if ordering from another country, the FBI could work with U.S. Customs to hold the end address or name the package is sent to. Working backwards, and working with foreign intelligence, the individual who sent the package would not be difficult to identify. As the markets decentralize more, locating servers and administrators will become increasingly irrelevant. The solution to the problem should, therefore, be to increase undercover operations, work with the correct agencies, and find the source of the drugs or weapons.

B. Applicability of Current Legislation

A great deal of legislation has the potential usefulness to aid law-enforcement agencies in identifying and prosecuting Darknet market administrators and users. This Section discusses potential applications to Darknet markets of the laws discussed above. It also cautions implications of using these laws against their intended purposes.

1. Utilize the Bank Secrecy Act in Money Laundering Through Exchanges

On a federal level, the BSA seems capable of addressing large-scale bitcoin launderers to the United States. Without clearly defining bitcoin as a currency and focusing on large creators of the currency rather than individual users who have the ability to accumulate great amounts over Darknet Markets, the BSA is not equipped to deal with the high-ranking vendors of Darknet Markets. One useful application of the BSA under the FinCEN guidelines is tracking exchanges (such as Coinbase or the former Mt. Gox) that notice the suspicious activity of large amounts of bitcoins coming in without good reason. If utilized properly, law enforcement and legislatures can put more effort into pressing the BSA to these exchanges, as they likely receive bitcoin for money from mining companies quite often. As previously stated, sophisticated and experienced vendors already have methods of diversifying and tumbling their bitcoins, so this method would be highly inefficient unless a reclassification of bitcoin traffic could be implemented.

2. *Do Not Expect Judges to Allow the All Writs Act to Bypass Fourth Amendment Concerns*

The All Writs Act should be thought of as a last-ditch effort in order to identify and prosecute illegal uses of bitcoin and Darknet market users. Judges have historically been apprehensive to use such dated legislation in the new technological advances of the twenty-first century.[203] It should not be the first option, or even a viable option, for a law-enforcement agency to use when working to identify questionable traffic from an Internet service provider, or even a bitcoin exchange. Law enforcement agencies should therefore find if there are any other applicable laws because if there are the All Writs Act will be preempted and the discovery will not stand in court. A law enforcement agency thus has a responsibility not to base a case off of an improper warrant because it may be challenged and will likely fail in appellate-court proceedings.[204] A solution to this problem, as Apple CEO Tim Cook requested,[205] would be for legislators to act and either amend the statute or pass a new law specifically relating to this surveillance.

3. *Continue to Use CISA As Intended or Risk Losing Cooperation from Companies*

CISA's purpose is to aid in cybersecurity threats that are occurring on a more frequent basis in recent years.[206] CISA is not an act that should be used to backdoor Fourth Amendment concerns under the guise of a cybersecurity threat. CISA is a voluntary act that does not *force* company adherence[207]—so, if the government wants to foster a good relationship with companies and get them to voluntarily comply with the act, CISA should be used properly and focus only on *threats to cybersecurity*.

If the government can find a creative way to justify Darknet-market use, it may be better able to gain cooperation from companies agreeing to identify users involved in the cybersecurity threat. For example, if a cybersecurity threat is occurring through Tor and there is either a relay node or exit node operating, perhaps the government can gain cooperation from a person or company that is operating the access point and then identify a serious perpetrator of security to the website. This could lead to discovery of servers that would not otherwise have been accessible to the government under the law. It is a fine line that a law-enforcement agency (such as the FBI) must tread in order to avoid jeopardizing an otherwise helpful relationship between companies such as

203. Rebecca J. Rosen, *When Does Technology Change Enough That the Law Should Too?* ATLANTIC (DEC. 27, 2013), http://www.theatlantic.com/technology/archive/2013/12/when-does-technology-change-enough-that-the-law-should-too/282683/.

204. *Id.*

205. *See supra* note 173 and accompanying text.

206. *See supra* note 178.

207. *Id.*

Apple, Comcast, or Coinbase, in solving a breach to the security of their networks.

4. Find Creative Ways to Utilize the DMCA Without Jeopardizing Anonymity

As stated previously, courts are reluctant to use the DMCA unless there is a legitimate reason related to the use of copyright infringement.[208] This may provide some major hurdles if a law-enforcement agency, such as the FBI or DEA, wants to act as an agent for a potential plaintiff. The target of these actions would undeniably be bitcoin users using an exchange, such as Coinbase—which are, in part, committing some type of copyright fraud through illegal means related to Darknet market use.[209]

A potential implication of over-using an act designed for a civil purpose is a concern to bitcoin users. To remedy that, as other analysts have noted, the government should be required to provide evidence of an illegal act outside the realm of copyright in order to get the information from an exchange.[210] If the DMCA is to be used to gain an edge on cryptocurrency users and Darknet administrators, there must be a narrowly tailored, legitimate purpose in order to avoid a court's order denying the subpoena for anonymity concerns.[211]

Further, this strategy could be interpreted similarly to the allegations against the NSA for using "parallel construction" and then tipping off the FBI. Parallel construction is much worse than using the DMCA for discovery, so if that is the purpose of the government's efforts, then it could use this as a more justifiable means. This would only be necessary if Executive Order 12333 is not used for purposes other than terrorism. Nonetheless, the current state of privacy concerns and whistleblowing should only encourage the surveillance of communication through legitimate means.

V. CONCLUSION

There is no simple answer to solving the issue of how to address Darknet markets. This Note aimed to educate legislators and law-enforcement agencies on what they are actually dealing with, with a focus on updating antiquated and failed methods of addressing the actual problem. There is a fine line between maintaining power to control the "drug war" and infringing on privacy and libertarian values. America must be

208. *See supra* Subsection III.B.4.

209. *See* Huang, *supra* note 188.

210. *Id.* at 2118.

211. *See id.* The main issue with encouraging a court to accept the DMCA at face value is manipulation of First Amendment (as well as Fourth Amendment) rights, which could lead to a civil suit against the government. *See id.* The agent using the DMCA would be required to provide more information, as there is a "higher burden of proof" in criminal cases. *Id.*

careful not to jeopardize personal freedoms and the integrity of the Internet. As Edward Snowden put it, "[t]he definition of a security state is any nation that prioritizes security over all other considerations."[212]

Now, more than ever, the government has a responsibility to not force another failed drug war. If this problem is not properly dealt with, there could be significant repercussions and outcry from advocates of personal freedoms and privacy. On the other hand, if it is not dealt with at all, the government could lose control over the trade of drugs and other illicit substances and services. Specificity and transparency are crucial in order to avoid a loss of privacy—both in a virtual and a real sense—which may come if these efforts fail.

212. Matthew Cole et al., *Edward Snowden's Motive Revealed: He Can 'Sleep at Night'*, NBC (May 28, 2014), http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowdens-motive-revealed-he-can-sleep-night-n116851 (quoting Edward Snowden) (internal quotations omitted).