Washington and Lee Journal of Civil Rights and Social Justice

Volume 31 | Issue 2 Article 8

Spring 2025

Life in Limbo: Cryptocurrency and FOSTA as the Pillars of Cyber-Trafficking

Rebecca Liu
Washington and Lee University School of Law, rliu@law.wlu.edu

Follow this and additional works at: https://scholarlycommons.law.wlu.edu/crsj

 Part of the Banking and Finance Law Commons, Civil Rights and Discrimination Commons, Computer Law Commons, Human Rights Law Commons, Legislation Commons, Science and Technology Law Commons, and the Sexuality and the Law Commons

Recommended Citation

Rebecca Liu, *Life in Limbo: Cryptocurrency and FOSTA as the Pillars of Cyber-Trafficking*, 31 Wash. & Lee J. Civ. Rts. & Soc. Just. 329 (2025).
Available at: https://scholarlycommons.law.wlu.edu/crsj/vol31/iss2/8

This Note is brought to you for free and open access by the Washington and Lee Journal of Civil Rights and Social Justice at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Journal of Civil Rights and Social Justice by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

Life in Limbo: Cryptocurrency and FOSTA as the Pillars of Cyber-Trafficking

Rebecca Liu*

Abstract

As the internet continually advances into Web 3.0, human traffickers thrive in using online platforms to prey on their victims, creating a new form of human trafficking: cyber-trafficking. In 2018, Congress passed the Fight Online Sex Trafficking Act ("FOSTA") to dampen the stringent protection that 47 U.S.C. § 230 ("Section 230") offered to internet intermediaries in cyber-trafficking litigation. However, Congress's intended effect in passing FOSTA failed, as courts continue to interpret FOSTA narrowly, upholding the stringent protection that Section 230 offers internet intermediaries. Beyond FOSTA's indifferent impact, governmental bodies struggle adapting to Web 3.0's landscape, neglecting to intervene with traffickers' use of cryptocurrency's de-regulated nature to target victims. Consequently, FOSTA and cryptocurrency act as pillars reinforcing cyber-trafficking. Governmental bodies and courts must swing their ideological pendulums to adjust to the early age of Web 3.0 to protect potential victims from cyber-trafficking.

* J.D. Candidate, May 2025, Washington and Lee University School of Law. This Note arose from my fascination with the intersection of human rights law and Web 3.0 development. First, I would like to thank my faculty advisor Professor Fairfield for his incredible insight. Second, I would like to thank my family, who instilled a love of learning since a young age.

Table of Contents

I. Introduction 332

II. Cryptocurrency as the Bedrock of Cyber-Trafficking .. 341
A. Block chain technology facilitates cryptocurrency transactions through a public ledger 343
B. Traditional "Follow the Money" Techniques Have Been Rendered Useless in Tracking Illicit Activities Funded by Cryptocurrency 348
C. Cryptocurrencies Attempt to Implement Anti-Money Laundering Measures, but Remain Resistant to Traditional Financial Regulations 352

III. The Legislative and Judicial Responses to Human Trafficking Inadvertently Increased Violence Against Vulnerable Groups 357
A. Before FOSTA's passage, Section 230 forbid victims of human trafficking from prosecuting internet intermediaries.. 358
B. The Court of Public Opinion Ignited Congress's Ideological Pendulum Swing, Resulting in FOSTA's Passage 363
C. Despite Congress's Intent in Passing FOSTA, It Failed Its Mission by Displacing the Threat of Trafficking onto Other Vulnerable Populations 365

IV. FOSTA's Judicial Framework Fails to Protect Victims of Cyber-Trafficking 368

V. Courts Should Engage in an Ideological Pendulum Swing to Combat Cyber-Trafficking 372

VI. The Federal Trade Commission Should Require Cryptocurrency Exchanges to Engage in Consumer Transparency 376

VII. Congress Should Consider Passing the Digital Asset Anti-Money Laundering Act 382

VIII. The Department of State Should Consider Block Chain Technology as a Long-Term Solution Towards Government-issued Identification 385

IX. Conclusion 390

I. Introduction

Excited to meet new people, Sarah Cooper first logged on to Facebook when she was twelve or thirteen, where she joined music, Harry Potter, and Twilight fan groups.[1] By the time Sarah got to high school, she wanted to fit in with the "popular" group, and so she wanted more Facebook friends.[2] As Sarah added more Facebook friends, she did not actually know many of these "friends" in real life.[3] One day, Sarah received a Facebook friend request from a boy she did not know who went by "J" in his profile.[4]

Sarah messaged J, and they quickly connected over shared interests, such as music and books.[5] They talked frequently, and Sarah shared her secrets with J.[6] As their relationship grew, Sarah referred to J as her "best friend," and truly felt that he cared for her.[7] Eventually, J asked Sarah to send explicit photos, and Sarah did it because she wanted to strengthen their relationship.[8] They kept in touch for a few years, and eventually spoke on the phone, but never met each other in person.[9]

Shortly after Sarah's eighteenth birthday, they arranged to meet.[10] As J pulled up in his car and Sarah got in, she felt

---

1. *See* Sarah Cooper, *Stories*, EQUALITY NOW (Nov. 15, 2021) ("I joined various Facebook subgroups[.]") [perma.cc/G9ML-C2VA].

2. *See id.* (discussing how Sarah wanted to feel "popular" by getting the "largest number of friends on Facebook").

3. *See id.* ("I had over 1,000 Facebook friends, many of whom were people I didn't know in person.").

4. *See id.* ("His profile picture was of a cartoon character and his username was 'J.'").

5. *See id.* (explaining that Sarah and J connected over music and books, communicating frequently over Facebook Messenger).

6. *See id.* ("I told him all about my life, things in my past, problems I was having.").

7. *See id.* (describing how J emotionally manipulated Sarah).

8. *See id.* ("He asked me to send some explicit photos and I did it because I wanted to be accepted by him.").

9. *See id.* (describing, from Sarah's perspective, how their relationship carried on for a few years, and that they never met in person until she turned eighteen).

10. *See id.* ("[S]hortly after my 18th birthday . . . we finally arranged to meet").

surprised, as he appeared closer to forty, rather than close to Sarah's age.[11] Still, Sarah felt eager for J's acceptance, and she went out with him.[12] J took Sarah to a house party where he forced Sarah to drink alcohol and take cocaine.[13] Continuing to victimize Sarah, J forced her into a motel where he sold her into sex slavery.[14] Sarah found herself stuck in a cruel state of limbo, unsure of when she would reunite with her family again.[15]

Unfortunately, Sarah's harrowing experience in limbo does not constitute an unusual circumstance for victims of human trafficking. Alongside a myriad of other tactics, traffickers heavily use grooming techniques to lure victims, such as Sarah, into forced sexual labor.[16] While Sarah managed to escape her traffickers' grueling limbo, some victims never escape, and they suffer in an indefinite state of abuse under the hand of their trafficker.[17] However, what lurks in the background of how traffickers target their victims goes unaddressed in most narratives that discuss trafficking.[18] Typically, the media portrays traffickers as villains lurking in dark corners, waiting to prey on victims.[19] Although this rings true in some cases, it constitutes a common misconception.[20] As technological advances continue

11. *See id.* (describing Sarah and J's in-person meeting).

12. *See id.* (same).

13. *See id.* (recounting Sarah's kidnapping).

14. *See id.* (describing Sarah's horror as J filed her "audition tape").

15. *See id.* (mentioning that Sarah's traffickers gave her drugs and alcohol to keep her in a daze).

16. *See id.* (explaining how Sarah's trafficker utilized grooming techniques to trap her).

17. *See id.* (emphasizing that Sarah escaped, but other victims are not as "lucky").

18. *See* U.S. DEP'T STATE, OFFICE TO MONITOR & COMBAT TRAFFICKING IN PERS., TRAFFICKING IN PERSONS REPORT (2023) (emphasizing that technology companies have constituted an area of special interest for the Department of State due to increased criminality on all technological platforms) [hereinafter TIP Report].

19. *See Myths, Facts, & Statistics*, POLARIS (2024) (indicating that a common misconception involving human trafficking is that victims are exclusively targeted by strangers) [perma.cc/WKM2-8R8L].

20. *See id.* (same).

to soar, the "dark corner" morphs into the internet, as modern-day technology facilitates a breeding ground for traffickers to groom their victims.[21]

As we reach the early deployment and development of "Web 3.0"[22], human trafficking rarely comes up as an initial thought. Especially since the Covid-19 pandemic, our society learned to praise the benefits of technological innovation, as it allowed instant virtual connection during a time with little in-person connection.[23] However, since the advent of Web 3.0, the internet lurks in the background of stories similar to Sarah's.[24] For instance, the State Department emphatically voiced concerns about Web 3.0's role in trafficking.[25] In fact, the 2023 State Department Trafficking in Persons Report ("TIP Report") highlighted a modern form of trafficking: cyber-trafficking.[26]

As technology constantly advances with the advent of Web 3.0, traffickers continuously adapt by utilizing a novel

---

21. *See* TIP Report, *supra* note 18, at 58–59 (providing an overview of the use of online platforms for recruitment into forced labor).

22. *See* The Investopedia Team, *Web 3.0 Explained, Plus the History of Web 1.0 & 2.0*, INVESTOPEDIA (Oct. 18, 2023) (explaining that Web 3.0 describes the third phase of the internet characterized by decentralization, ubiquity, and artificial intelligence) [perma.cc/W8MU-RDZV].

23. *See generally* Emily Towner et al., *Virtual Social Interaction and Loneliness Among Emerging Adults amid the COVID-19 Pandemic*, 3 CURRENT RSCH. ECOLOGICAL & SOC. PSYCH. 1 (2022) (noting how "[m]any social activities moved online during the global COVID-19 pandemic"); *see also* TIP Report, *supra*, note 18, at 64 (noting that since the pandemic, crime syndicates have adapted and thrived in using online purposes to partake in illicit activities).

24. See UNODC CRIME SECTION, GLOBAL REPORT ON TRAFFICKING IN PERSONS 2022 70 (2023) (explaining that the primary business model for sex traffickers in the United States involved utilizing internet platforms to exploit victims).

25. *See* TIP Report, *supra* note 18, at 64 (outlining how traffickers have thrived in using the internet to facilitate cyber scam operations while exploiting the young and unemployed).

26. *See id.* (same); *see also* Lauren Burke et al., *Cyber Scamming as a New Destination for Human Trafficking Victims*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 17, 2023) (discussing how criminals are using online platforms, cryptocurrency, and other similar scams to commit human trafficking) [perma.cc/QG94-9UA2],

and powerful tool, cryptocurrency, to lure victims into a harrowing state of limbo.[27] Sonith, a survivor of cyber-trafficking, recounted his personal experience in the TIP Report.[28] When Sonith's traffickers offered him a job in Asia, he left his family in the Philippines.[29] Upon his arrival in Thailand for his "job," his traffickers took him to a remote compound, held him hostage, and forced him "to leverage [his] English language skills to run online cryptocurrency scams[.]"[30] Ultimately, Sonith found himself trapped in a cruel state of limbo, unsure of when he would escape this horrendous, newfound reality.[31] Sonith's story illustrates how traffickers adapt to Web 3.0's tools to prey on victims in tandem with perpetuating cryptocurrency scams, as they avoid the strict controls of traditional banking systems.[32]

Given cryptocurrency's fundamentally resistant nature to traditional government regulation, traffickers use this characteristic to their advantage for their criminal pursuits.[33] Since the pandemic, traffickers have utilized

27. *See id.* (outlining cryptocurrency as a topic of "special interest" because traffickers utilize it to run cyber scams).

28. *See* TIP Report, *supra* note 18, at 21 (illustrating Sonith's experience).

29. *See id.* (emphasizing that Sonith believed he left his family for legal work experiences).

30. *Id.*

31. *See id.* (expounding on Sonith's time in captivity, where he worked up to sixteen-hour days and had limited access to food).

32. *See generally id.*; *see also* Gurvais Grigg, *Combatting Trafficking with Blockchain Analysis*, CHAINALYSIS (Apr. 12, 2022) (recognizing how traffickers have utilized cryptocurrencies' speed and cross-border functionality) [perma.cc/V5QK-FTCZ].

33. *See* James McWhinney, *Why Governments Are Wary of Bitcoin*, INVESTOPEDIA (last updated Nov. 3, 2023) (explaining that decentralizing traditional fiat currencies undermines the need for a central bank, leaving governments wary of its ability to act as a conduit by criminals for illegal activities) [perma.cc/DPC5-P4FJ]; *see also* David B. Black, *Cryptocurrency Fuels Growth of Crime*, FORBES (Mar. 11, 2022, 4:15 PM) (emphasizing that cryptocurrency platforms like Bitcoin allow criminals to receive instant payments while remaining anonymous) [perma.cc/YWS5-ZLYY]; *see also* Chainalysis Team, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-time Highs amid Surge in Sanctions Designations and Hacking*, CHAINALYSIS (Jan. 12, 2023)

cryptocurrency extensively to facilitate human trafficking.[34] In fact, the TIP Report emphasized that traffickers thrived in multifaceted ways during the pandemic because of the sudden interruption of migration dynamics, bans on public gatherings, and the cessation of entire industries, allowing traffickers to take advantage of victims' economic hardships.[35] In fact, the Department of Homeland Security reported an annual global profit of $150 billion generated by human trafficking in 2020.[36] As traffickers continually adapt to changes from increased global unemployment and travel restrictions, this effort now constitutes a multi-billion dollar industry: forced criminality in cyber scam operations, which aggravates the human trafficking problem.[37] For instance, traffickers pose as labor brokers and use social media to recruit victims, like Sonith, with English proficiency or technical backgrounds for promising jobs in IT, computer programming, and a myriad of other industries.[38]

Often, when traffickers successfully recruit workers, they initially promise to pay for workers' arrival expenses.[39] However, upon the workers' arrival, traffickers confiscate

(finding that illicit transaction volume rose in 2022, hitting an all-time high of $20.1 billion) [perma.cc/HGZ7-AH9A].

34. *See* TIP Report, *supra* note 18, at 64 (emphasizing that since the Covid-19 pandemic, human trafficking effectuated through cybercrimes surged due to criminals' economic desperation).

35. *See id* (explaining that criminals quickly adapted to the limited in-person opportunities to traffic victims).

36. DHS CTR. FOR COUNTERING HUM. TRAFFICKING, COUNTERING HUMAN TRAFFICKING: YEAR IN REVIEW (OCTOBER 2020 TO SEPTEMBER 2021) ii (2022) ("Human traffickers are in it for the money, with estimated annual global profits of $150 billion.").

37. *See* TIP Report, *supra* note 18, at 64 (emphasizing that traffickers will force victims to work up to fifteen hours a day, ultimately selling victims to other scam operations or forcing victims into sex trafficking if they do not agree to fraudulent recruit additional members).

38. *See id* (explaining that many traffickers pose as job recruiters and post fraudulent employment opportunities on Facebook and other job sites).

39. *See id.* at 42, 54, 59, 85 (discussing the phenomenon of "debt bondage" as a method used by traffickers, where they promise to pay for victims' travel expenses, followed by forcing victims to pay off their expenses through forced labor).

their passports, and demand that the victims defraud individuals in online cryptocurrency schemes.[40] Often accompanied by physical and sexual abuse, traffickers will force victims to serve as models in video chats with prospective scam victims.[41] Millions of exploited individuals across the world live under the coercion and force of their traffickers, ensnared in a life of uncertainty, simply surviving in a cruel state of limbo.[42] As the advent of Web 3.0 continues, traffickers take advantage of its characteristics to participate in cyber-trafficking, targeting potential victims like Sarah and Sonith.[43]

To provide trafficking victims with a means towards justice, U.S. legal protections include the Trafficking Victims Protection Act ("TVPA")[44] and the Fight Online Sex Trafficking Act ("FOSTA").[45] The TVPA, passed in 2000, constitutes the first law in the U.S. that comprehensively addresses human trafficking.[46] It allows prosecution for criminal or civil liability against recruiting, harboring, moving, or obtaining a person through fraud, force, or coercion for the purpose of involuntary servitude, debt bondage, slavery, or sexual exploitation.[47] FOSTA, passed in 2018, acts as an exception to 47 U.S.C. § 230 ("Section 230") of the Communications Decency Act ("CDA").[48] This act

40. *See id.* at 59 (giving examples of these practices from around the world).

41. *See* CTR. FOR STRATEGIC & INT'L STUD., *supra* note 26 (mentioning that traffickers force victims to serve as models on video chats to pay off their travel debts).

42. *See* TIP Report, *supra* note 18, at 4 ("Every year millions of people are exploited within and across borders.").

43. *See generally* TIP Report, *supra* note 18 (emphasizing the frequency of traffickers utilizing the internet to prey on victims).

44. *See generally* 18 U.S.C. § 1595.

45. *See generally* 18 U.S.C. § 1595 (d).

46. *See Federal Law*, NAT'L HUM. TRAFFICKING HOTLINE (2024) (highlighting the importance of the TVPA, as it represents the first federal law to address human trafficking) [perma.cc/29QD-VXNF].

47. *See id.* (outlining that the TVPA addresses prosecution of human trafficking).

48. *See* Lura Chamberlain, *FOSTA: A Hostile Law with a Human Cost*, 87 FORDHAM L. REV. 2171, 2175 (2019) (discussing how FOSTA

deprives online platforms of long-standing legal immunity in connection with illegal actions by users.[49] However, despite Congress's aspirational intentions, FOSTA inadvertently created greater barriers for trafficking victims to seek justice, while increasing the risk of human trafficking onto sex workers.[50]

Beyond TVPA and FOSTA, other regulations imposed upon cryptocurrencies significantly impact the protection of potential victims from trafficking. For instance, the Bank Secrecy Act ("BSA")[51] imposes Anti-Money Laundering ("AML") requirements upon Financial Institutions ("FI") to prevent criminal activities through monetary transactions.[52] Working in tandem with the BSA, the Financial Crimes Enforcement Network ("FinCEN") administers the AML requirements and implements regulatory efforts through its delegated authority by the Department of Treasury.[53]

FinCEN requires cryptocurrency exchanges to comply with AML requirements, such as Know Your Customer ("KYC") checks, to ensure that users do not purchase

---

amended 47 U.S.C. § 230 by preventing internet intermediaries with a route of immunity).

49. *See id.* at 2176 (describing how the law rescinded "the near-categorical immunity that such sites had previously enjoyed from liability").

50. *See What is SESTA/FOSTA?*, DECRIMINALIZE SEX WORK (2023) (discussing the downsides of SESTA/FOSTA despite its intention to protect victims of sex trafficking because it impedes efforts to find and prosecute traffickers) [perma.cc/UJ8B-3X3U]; *see also A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018) (emphasizing that these laws arguably place sex workers into nonconsensual, dangerous situations, putting them at risk for sex trafficking) [perma.cc/MAY8-MZYM].

51. *See generally* Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, 84 Stat. 1118 (codified as amended in scattered sections 12 and 15 U.S.C.).

52. *See* Stan Sater, *Do We Need KYC/AML: The Bank Secrecy Act & Virtual Currency Exchanges*, 73 ARK. L. REV. 397, 397 (2020) (asserting that the BSA acts as the U.S. government's "800-pound gorilla" when regulating financial transactions).

53. *See id.* at 398 (discussing how FinCEN works alongside the Department of Treasury).

cryptocurrency for criminal activities, such as trafficking.[54] Although these regulatory schemes act as necessary safeguards, the nature of cryptocurrency contains informational vulnerabilities that criminals take advantage of. Similar to traffickers' adaptability to Web 3.0, traffickers continually adapt to cryptocurrency's characteristics to circumvent KYC checks.[55]

As traffickers participate in cyber-trafficking within the early age of Web 3.0, this Note will provide a critical analysis of how FOSTA and cryptocurrency represent pillars of this harrowing phenomenon. Moreover, this Note will assert that cryptocurrency's resistance to traditional governmental regulation alongside FOSTA's failures in holding traffickers accountable, act in tandem as pillars of cyber-trafficking.[56] As this Introduction provided an overview of how cyber-trafficking, cryptocurrency, and FOSTA act separately to increase the risks of ensnaring individuals into limbo, the rest of this Note will proceed in five parts.

Part II will explain how cryptocurrencies' characteristics allow traffickers to weaponize it and facilitate cyber-trafficking.[57] Moreover, it will discuss the technological structure of cryptocurrency, cryptocurrency's resistance to traditional forms of financial regulation, and the inconsistencies of its disclosure requirements.[58] Part III will examine the genesis of FOSTA, the inadvertently negative consequences of its passage, and detail the dangerous risks it

54. *See id.* (noting that AML requirements act as surveillance useful for criminal investigations).

55. *See* Micah Kindred, *Gym, Tan, Money Laundering: United States Crypto Anti-Money Laundering Regulations*, UNIV. CIN. L. REV. BLOG (Nov. 29, 2022) (illuminating that the decentralized characteristics of cryptocurrencies have allowed criminals to use it to circumvent anti-money laundering regulations) [perma.cc/ZC2F-3QA7].

56. *See generally infra* Parts II–III.

57. *See infra* Part II (discussing how criminals weaponize cryptocurrency to facilitate trafficking online).

58. *See id.* (demonstrating how characteristics of cryptocurrency allow criminal activity).

imposes against sex workers while neglecting to address general victimization caused by cyber-trafficking.[59]

Part IV will discuss how the current jurisprudence of FOSTA fails to provide cyber-trafficking victims from seeking justice in courts, as courts participate in the wrong debates regarding FOSTA and Section 230.[60] Particularly, courts refuse to "swing" their ideological pendulum towards interpreting statutes according to the early age of Web 3.0.[61] Part V will discuss a judicial solution, suggesting that courts should deputize internet intermediaries, similar to how courts deputized financial intermediaries for the last three decades.[62]

Following judicial solutions, Part VI will assert that consumer transparency could dampen cyber-trafficking, by requiring cryptocurrency exchanges to disclose their efforts towards upholding ethical practices within their exchanges.[63] Then, Part VII will suggest legislative solutions, asserting that Congress should swing its ideological pendulum according to the age of Web 3.0, by enacting the Digital Asset Anti-Money Laundering Act.[64] Lastly, Part VIII will propose a long-term solution, suggesting that the Department of

---

59. *See infra* Part III (discussing FOSTA's history and passage).

60. *See infra* Part IV (analyzing how the lack of current judicial remedies fail to decrease and eliminate cyber-trafficking).

61. *See* Sean J. Shannon, Richard A. Posner: A Study in Judicial Entrepreneurship 17 (Feb. 2016) (Ph.D. dissertation, City University of New York) (on file with the CUNY Graduate Center) (explaining the overall concept of the swinging pendulum, that as one idea dies, another is born, ultimately allowing for innovative new ideas within American jurisprudence); *see also* Lev Menand, *Stilling the Pendulum: Regulatory, Supervisory, and Structural Approaches*, 70 VAND. L. REV. EN BANC 273, 274 (2017) (explaining how the concept of the swinging pendulum applies in the financial regulatory context, emphasizing that Congress will craft reforms in response to a crisis); *see also What Democracy Is Doing with Digital Technology*, COGITO RESEARCH MAGAZINE (May 6, 2019) (pointing out the idea of a pendulum swing in the age of technological advancement, particularly how technology has altered the state of our democratic society) [perma.cc/68HD-ETQW].

62. *See infra* Part V (analyzing how courts deputize intermediaries).

63. *See infra* Part VI (arguing that increased disclosure to online participants can decrease cyber-trafficking).

64. *See infra* Part VII (discussing potential legislative solutions).

Homeland Security should consider maintaining passports on a block chain to prevent traffickers from moving victims out of the U.S., even if the traffickers initially ensnared the victim online.[65] Finally, Part IX will conclude by emphasizing that the early age of Web 3.0 begs for an ideological pendulum swing from Congress, courts, and government agencies to protect potential victims from cyber-trafficking.[66]

II. Cryptocurrency as the Bedrock of Cyber-Trafficking

Initially, a person or group using the pseudonym Satoshi Nakamoto ("Nakamoto") created the first cryptocurrency on the market, otherwise known as "Bitcoin," to facilitate peer-to-peer financial transactions.[67] Bitcoin allowed individuals to send online payments directly to one another, without the involvement of any intermediaries.[68] Nakamoto created cryptocurrency with the intention of seizing financial control back from "elites," giving ordinary people a chance to take part in a decentralized financial system.[69] Following Bitcoin, a variety of cryptocurrencies have emerged, such as Ethereum, Dogecoin, Tether, and more.[70]

---

65. *See generally* Part VIII.

66. *See generally* Part IX.; *see* Lev Menand, *Stilling the Pendulum: Regulatory, Supervisory, and Structural Approaches*, 70 VAND. L. REV. EN BANC 273, 274 (explaining how the concept of the swinging pendulum applies in the financial regulatory context, emphasizing that Congress will craft reforms in response to a crisis); *see also* Lawrence Summers, *The pendulum swings towards regulation*, FIN. TIMES (Oct. 26, 2008) (shedding light on how regulatory schemes analogize themselves with pendulum swings, meaning that following a crisis, the government should swing towards alleviating the harm) [perma.cc/6AWU-HASV].

67. *See Who Is the Mysterious Bitcoin Creator Satoshi Nakamoto?*, COINTELEGRAPH (discussing why Nakamoto created Bitcoin) [perma.cc/W33R-PKT6].

68. *See id.* (describing Nakamoto's desire to create an electronic form of currency, without involvements of intermediaries).

69. *See id.* (mentioning Nakamoto's hope to take financial control back from "financial elites").

70. *See id.* ("Crypto paved the way for various forms of digital currencies . . . ").

Interestingly, Nakamoto's identity remains a mystery.[71] Many critics believe Nakamoto's mystery identity arises out of a desire to avoid law enforcement.[72] Some speculate that Nakamoto understood the potential legal liability that could accompany Bitcoin because they knew of legal issues facing past alternative currencies.[73] For example, in 2011, Bernard von NotHaus was convicted of making, possessing, and selling his own private currency, the "Liberty Dollar."[74] Nakamoto could have potentially faced the same fate, as they surely knew that Bitcoin could garner some enemies, considering that governments do not respond kindly to alternative monetary systems.[75]

Moreover, critics speculate about illicit activities associated with cryptocurrency.[76] Critics assert that Nakamoto likely wanted to avoid legal and regulatory complications borne out of Bitcoin, as criminals made it a prime form of currency within dark markets.[77] For instance, in 2023, the total value of cryptocurrency used in illicit

71. *See* COINTELEGRAPH *supra* note 67 (emphasizing Nakamoto's mysterious nature).

72. *See* Alex Lielacher, *Why Has Satoshi Nakamoto Remained Anonymous?*, BRAVE NEW COIN (June 12, 2023, 9:40 AM) (discussing that while Nakamoto has not disclosed reasons for his anonymity, the article predicts the reasons for his anonymity, such as avoiding the attention of law enforcement) [perma.cc/KMQ6-8MT5].

73. *See* Scott Chipolina, *Why has Bitcoin inventor Satoshi Nakamoto remained anonymous?*, DECRYPT (Sept. 15, 2020) (speculating that Nakamoto potentially remained anonymous because they knew the authorities would come after Bitcoin's creator if identified, given the past treatment of Bernard Van NotHaus, who was convicted of selling his own private currency) [perma.cc/PSP6-7KKS].

74. *See id.* (mentioning that law enforcement convicted Bernard von NotHaus for making the Liberty Dollar).

75. *See id.* (hypothesizing that Bernard von NotHaus's conviction likely encouraged Nakamoto's identity to remain secret, as Nakamoto did not want to deal with a similar "fallout").

76. *See id.* (explaining that many criminals used Bitcoin to launder money and purchase illicit goods).

77. *See* Lielacher, *supra* note 72 (speculating that Nakamoto likely wanted to avoid legal and regulatory complications that could arise from being associated with the creation of a disruptive technology like Bitcoin).

activities totaled to $24.2 billion.[78] Due to cryptocurrency's decentralization, criminals utilize it as a vehicle for cyber-trafficking.[79]

Part II.A will discuss cryptocurrency's technological structure,[80] while Part II.B will detail how cryptocurrency's characteristics make it highly resistant to law enforcement's traditional methods of investigation.[81] Finally, Part II.C will discuss how cryptocurrency's nature makes it highly resistant to traditional forms of financial regulation.[82] Given cryptocurrency's structure and lack of unified regulatory schemes, it fuels a billion-dollar industry of illicit activities, making it the bedrock of cyber-trafficking. Ultimately, cryptocurrency plays a pivotal role in how traffickers ensnare victims, like Sarah and Sonith, in a cruel state of limbo.[83]

A. Block chain technology facilitates cryptocurrency transactions through a public ledger

To understand cryptocurrency's decentralized nature, an overview of block chain technology will provide an understanding as to why traffickers favor this form of currency. In the realm of cryptocurrency, block chains record and confirm cryptocurrency trades, in the form of a digital,

78. *2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth*, CHAINALYSIS (Jan. 18, 2024) (detailing the trends of cryptocurrency values received by illicit addresses) [perma.cc/AF9C-9MD8].

79. *See* TIP Report, *supra* note 18, at 21 (emphasizing that the Department of State has taken special interests in cyber-crimes, as criminals have increasingly used online platforms to conduct illicit activities); *see also* David B. Black, *Cryptocurrency Fuels the Growth of Crime*, FORBES (Mar. 11, 2022) (illuminating the overall trend that cryptocurrency has fueled a new crime wave) [perma.cc/PP68-MZPJ].

80. *See generally* Part II.A.

81. *See generally* Part II.B.

82. *See generally* Part II.C.

83. *See supra* Part I. (discussing how Sarah and Sonith's traffickers ensnared them in horrific states of limbo).

public ledger.[84] Take Bitcoin, for example. When someone purchases a Bitcoin, this transaction adds onto the series of transactions, termed "blocks."[85] Entire series of transactions constitute a "block chain."[86] No single entity maintains this block chain, as instead it relies on a mathematical consensus model.[87]

This consensus model consists of a verification process which every "block" must survive to join the block chain.[88] Overall, the block chain constantly updates the database containing a record of all transactions involving cryptocurrencies.[89] To link these "blocks" together, while ensuring that these "blocks" survive the verification process, cryptography plays a pivotal role.[90] Cryptography links these "blocks" together, and it consists of strings of fixed letters and numbers.[91] Moreover, each "block" in the block chain has a

84. *See Blockchain in Cryptocurrency*, COURSERA (Nov. 29, 2023) (explaining that block chain technology records cryptocurrency trades, similar to a ledger) [perma.cc/32DN-UG7U].

85. *See* Joshua A. T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 814 (2015) (detailing the "Bitcoin protocol," which creates a ledger out of a series of transactions, termed simply as "blocks").

86. *See id.* at 808 (underlying technology of cryptocurrency deemed as "block chain").

87. *See id.* at 814. (describing the block chain as a system relying on a mathematically innovative consensus model).

88. *See What is Blockchain & How Does it Work?*, SYNOPSYS (2024) (explaining the mechanism of the consensus model, such as the prominent verification process) [perma.cc/H83A-SARM]; *see also Making Sense of Bitcoin, Cryptocurrency, and Blockchain*, PWC (2024) (showcasing the verification processes involved in block chain verification) [perma.cc/4MZS-N5R2].

89. *See* SYNOPSYS, *supra* note 88 (explaining that block chain will constantly engage in updating the entirety of the database as more users add onto it).

90. *See* Fairfield, *supra* note 85, at 820 (posing an example of one person, Mary, wanting to convey her interest to Grace, and despite the fact they do not know each other, block chain technology allows them to verify one another's transactions with cryptography).

91. *See id.* at 820–21 (describing how block chain technology would allow Mary to convey her interest to Grace, by verifying strings of letters and numbers).

pair of cryptographically related keys: private and public.[92] With a public key, one can send cryptocurrency in a way that only the person with the private key can access it.[93] Commonly, letterboxes serve as an example of this distinction.[94] The address of the letterbox represents the public key, as anyone can put a letter in it.[95] However, the owner of the letterbox has the key to open it, which represents the private key.[96]

Therefore, if person A wishes to send person B a Bitcoin, A will use B's public key to send it, but B will use B's private key to receive and decrypt it.[97] In turn, cryptography prevents someone from standing in the middle of the transaction, since they cannot decrypt the transaction and therefore access the Bitcoin.[98] This aspect of cryptocurrency displays how blocks add themselves to a transactional chain without relying on central authorities.[99] The term "mining" describes computers that provide computing resources to the network, and in turn, receive processing fees.[100] Miners secure the system to ensure that outsiders cannot falsify transactions onto the block chain.[101]

Mining computers will attempt to guess hash values, and a hash acts as a fixed size number representing an arbitrary

92. *See id.* at 820 (explaining how public and private keys play a role in block chain technology).

93. *See id.* (mentioning that Mary could send her interest to Grace by encrypting it with Grace's public key to send it, and in turn, Grace can decrypt it with her private key to receive it).

94. *See id.* ("A commonly used analogy is that of a letterbox.").

95. *See id.* ("The public key is the address of the letterbox.").

96. *See id.* ("But only the owner of the letterbox has the key to open it and retrieve the contents.").

97. *See id.* (describing how someone can use a private key to receive and decrypt a Bitcoin).

98. *See id.* (explaining that the use of cryptography prevents anyone from standing in the middle of the transaction, since they cannot decrypt or access the transmitted interest).

99. *See id.* at 821. (emphasizing the significant innovation of the block chain, because of how blocks are added to a transactional chain without relying on central authorities).

100. *See id.* (explaining the phenomenon of mining).

101. *See id.* (describing how miners secure the system of verification).

amount of data.[102] An example looks like: DFCD3454BBEA788A751A696C24D97009CA992D17.[103] These hash values have an unpredictable characteristic, as no one can guess what the result will look like.[104] As more computers add onto a network, these hashes increase in difficulty and subsequently adding a new block onto the chain grows in difficulty.[105] Miners purposefully create difficult hashes to ensure that the block chain represents a "proof-of-work" system, ensuring that each block's hash correctly links to the previous block.[106] Because mining must occur with every purchase of cryptocurrency, the retroactive alteration of this decentralized public ledger cannot occur without the alteration of all subsequent blocks and the consensus of the network.[107] All transactions in a cryptocurrency network must "validate identical copies of the ledger so that there exists no central points of failure or fraud."[108]

These mechanics work together to create a distributed public ledger that is difficult to falsify.[109] Beyond the block chain, another key characteristic of cryptocurrency is

102. *See id.* (detailing how mining involves guessing numbers).

103. *See* John Berryhill, *What is a Hash Value?*, BERRYHILL COMPUTER FORENSICS (July 15, 2019) (displaying examples of what hash values look like) [perma.cc/YPD4-HAE7].

104. *See* Fairfield, *supra* note 85, at 822 (emphasizing the complexity of mining, using dice rolling as an example of how miners initially create hash values).

105. See *id.* (emphasizing that as each miner finds a hash that matches the block chain, it increasingly grows in difficulty as more blocks add onto the chain).

106. *See id.* ("[T]he process of securing a block chain is called a 'proof-of-work' system.").

107. *See id.* at 823 (re-stating the fact that each subsequent block is linked to the value of the prior block, creating a consensus).

108. *See Decentralized Ledger*, RIVER LEARN (explaining that each computer system in the larger context of cryptocurrency must validate one another to ensure that no users attempt to engage in fraud) [perma.cc/UG4X-NAYS].

109. *See* Fairfield, *supra* note 85, at 823 (emphasizing that the only way to get a "result" on a block chain involves checking each subsequent block, making it difficult to falsify).

decentralization.[110] Overall, cryptocurrency transactions occur quickly because they do not involve an intermediary, like banks, making this characteristic attractive to criminals.[111] As an example, consider a balance in a bank account. The account itself represents an entry within a private ledger maintained by a bank. The amount of trust one associates to their account depends on their trust in the bank holding the account.[112] Moreover, if a bank cultivates an untrustworthy reputation, the bank account does not carry value, and it is a worthless entry on an untrustworthy ledger.[113]

Paramount resources go towards generating trustworthiness of banks, such as restricting access to entire ledgers, while banks also engage in expensive oversight measures required by the government to ensure their own trustworthiness.[114] In contrast, cryptocurrencies do not engage in these measures, making them outside the scope of governmental oversight, which attracts criminals.[115] Traffickers favor this characteristic, as fifteen out of twenty-seven platforms hosting commercial sex markets accepted cryptocurrency payments as of 2022.[116] Accordingly,

110. *See* Fairfield, *supra* note 85, at 813 (explaining that cryptocurrency involves a system of "trustless ledgers," because of its lack of a central curator).

111. *See* Alisa DiCaprio, *Crime and Decentralization: Preventing Criminal Activity on DeFi*, R3 (July 4, 2023) (emphasizing that the decentralized financial systems arising within the last few years has resulted in a spike in cybercrimes) [perma.cc/83WS-H2ED].

112. *See* Fairfield, *supra* note 85, at 813 (discussing how individuals possess trust towards their banks).

113. *See id.* (summarizing how trust within a bank impacts value).

114. *See id.* at 814 (mentioning aggressive oversight methods utilized by banks).

115. *See Reasons Why Cryptocurrencies Are Interesting for Criminals*, FIN. CRIME ACAD. (Nov. 8, 2023) (illuminating the fact that criminals have high interest in using cryptocurrencies because of its decentralized nature) [perma.cc/B99H-F92B].

116. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105101, TRAFFICKING: USE OF ONLINE MARKETPLACES AND VIRTUAL CURRENCIES IN DRUG & HUMAN TRAFFICKING 15 (2022) ("Illicit actors can conduct some sex trafficking financial transactions entirely online, such as

criminals utilize cryptocurrency to profit off of victims suffering in a state of limbo, such as Sarah and Sonith.

B. Traditional "Follow the Money" Techniques Have Been Rendered Useless in Tracking Illicit Activities Funded by Cryptocurrency

Traffickers recognize cryptocurrencies' decentralization and take advantage of this characteristic.[117] Thus, this section will detail how traditional techniques employed by law enforcement to track criminals' financial transactions do not comport well with cryptocurrency's characteristics. In the age of Web 3.0, traffickers realize that all cryptocurrencies identify users through cryptographic addresses, making it difficult to immediately link transactions to their real identities.[118] Therefore, as traffickers continue their illicit activities via cryptocurrency exchanges, this phenomenon supports money laundering through cryptocurrency, in turn, encouraging cyber-trafficking.[119] As money laundering with cryptocurrency surges, law enforcement agencies face the herculean task of tracing these illicit funds back to the sources, as traditional financial investigation methods do not comport with the unique characteristics of cryptocurrencies.[120]

---

through the acceptance of payment for live virtual sex shows involving trafficked individuals.").

117. *See* Gurvais Grigg, *Combatting Trafficking with Blockchain Analysis*, CHAINALYSIS (Apr. 12, 2022) (emphasizing that cryptocurrencies have provided traffickers with a means of creating massive illicit markets) [perma.cc/V5QK-FTCZ].

118. *See id.* (summarizing the difficulties of linking transactions to real identities).

119. *See Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime*, FIN. CRIME ACAD. (July 3, 2023) (providing an overview of the different methods as to how traffickers utilize cryptocurrency money laundering services, like tumblers, to facilitate human trafficking) [perma.cc/MZD3-P9R5].

120. *See id.* (tracing illicit funds with traditional techniques has imposed difficulties onto law enforcement, as cryptocurrencies' unique decentralized nature creates complexities which oppose these traditional methods of following the money).

When dealing with traditional ("fiat") currencies, traditional "Follow the Money" techniques generally work by first identifying suspicious transactions.[121] To identify these transactions, law enforcement finds large cash deposits, frequent transfers, or unusual patterns within bank accounts.[122] Then law enforcement will collect relevant bank statements for further analysis, which consists of tracing the path of funds from the initial point of entry into the legitimate financial system.[123] In other words, this tracing technique occurs through identifying a series of transactions that create layers of complexity to obscure their origin, which can make them difficult to trace.[124] Ultimately, the end goal is identifying the final destination of the laundered money.[125]

Unlike fiat currencies, cryptocurrencies lack control by any central authority, allowing transactions to take place outside the purview of the government or financial institution oversight.[126] As previously discussed, this

121. *See The "Follow the Money" Method,* SANCTION SCANNER (tracing the movement of illicit funds may comport well with traditional methods, but in the digital age, it is imperative to consider alternative digital tools given the current high complexity of complex money laundering schemes) [perma.cc/MC2U-56PP].

122. *See Law Enforcement Overview,* FIN. CRIMES ENF'T NETWORK (discussing that the Financial Crimes Enforcement Network acts as the central entity, analyzing all money transfers in the U.S. under the Bank Secrecy Act, ultimately requiring reporting schemes from banks to flag any potentially suspicious transfer of funds) [perma.cc/9NT9-XCHN]; *see also 10 Key Tips to Help Law Enforcement and Financial Institutions Work Together More Effectively*, THOMSON REUTERS (Requiring banks to file Suspicious Activities Reports helps law enforcement officials to identify criminal financial activities) [perma.cc/L8YP-S49Y].

123. *See* SANCTION SCANNER, *supra* note 121 (explaining that traditional methods in tracing money trails include following large deposits of funds back to its initial source).

124. *See id.* (clarifying that a complication associated with tracing laundered funds includes criminals' strategies of layering legitimate funds with illegitimate funds).

125. *See id.* ("The ultimate goal is to identify the final destination or integration of layered funds.").

126. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-105346, BLOCKCHAIN IN FINANCE 2 (2023) ("No federal financial regulator has comprehensive authority to regulate the spot market for crypto assets that are not securities.").

decentralization attracts criminals towards purchasing cryptocurrency because their identities remain masked behind a cryptographic address, adding additional layers of complication in tracing illicit funds.[127] By exploiting this feature of cryptocurrency in the age of Web 3.0, criminals can employ a wide array of methods to launder money via cryptocurrency.[128]

An exploration of how criminals use cryptocurrencies will assist in understanding the methodologies employed by traffickers to partake in money laundering. Therefore, common methods used by criminals to launder money via cryptocurrency include tumblers, peer-to-peer ("P2P") networks, over-the-counter ("OTC") brokers, and DeFi platforms.[129] Cryptocurrency tumblers, otherwise known as mixing services, break down large amounts of cryptocurrency into smaller, untraceable amounts, while recombining them after passing through a series of transactions.[130] Take a charity donation, for example.[131] Instead of directly donating to a cause, multiple donors could pool their funds together and designate a third party to complete the actual transaction.[132] For instance, the charity would receive the donation without knowing how the total fund came together.[133] In other words, the remaining set of funds mask the identity of the original source, making it nearly

127. *See* Fairfield, *supra* note 85, at 820 (emphasizing the difficulty of tracking real identities using cryptographic addresses).

128. *See* FIN. CRIME ACAD., *supra* note 119 (outlining the wide variety of money laundering techniques used by criminals to launder funds through cryptocurrency).

129. *See id.* (summarizing different tactics used to launder money).

130. *See id.* (explaining that tumblers and mixers obfuscate the origin of criminals' ill-gotten gains, which creates extra obstacles for law enforcement to trace the movement of funds).

131. *See* Lipsa Das, *What Is a Bitcoin Mixer?*, LEDGER ACAD. (June 29, 2023) (utilizing donation pools as an example to assert that mixers create multiple levels of shields between the bad actor and the illicit transaction) [perma.cc/SB7F-N6Y2].

132. *See id.* (describing how mixers operate).

133. *See id.* (same).

impossible for law enforcement to identify and prosecute those responsible for the criminal activity.[134]

P2P networks and OTC brokers enable users to trade cryptocurrencies without proper identification, providing an environment where criminals have optimal freedom to launder money, outside of the purview of the government.[135] P2P transactions involve the exchange of assets directly between individuals, while OTC transactions involve the help of a broker.[136] OTC exchanges, unlike traditional cryptocurrencies, do not have public ledgers; instead, OTC transactions rely on a broker to find buyers and sellers to facilitate a trade.[137] For example, a criminal could employ a broker to purchase large amounts of Bitcoin to fund trafficking without ever telling the broker the illicit purpose of their purchases.

Ultimately, this complicates law enforcement's role when investigating the identity of a criminal because the criminal has created a shield by utilizing a broker. P2P exchanges offer direct exchanges of cryptocurrencies between individuals.[138] In other words, when a buyer and a seller have matching orders, the exchange software links the buyer and seller immediately, completing the transaction.[139] Lastly, criminals exploit DeFi platforms, due to its broad offering of a wide range of financial products and services.[140] Due to

134. *See id.* (same).

135. *See* Max Korpusov, *Crypto OTC versus P2P Trading: The Full Comparison*, FINCHPAY (outlining the differences between OTC and P2P cryptocurrency exchange methods) [perma.cc/JC2Y-N6NF].

136. *See id.* (mentioning the broker's role).

137. *See id.* (same).

138. *See id.* ("P2P trading involves the exchange of assets directly between individuals.").

139. *See OTC And P2P Trading Explained in Full Detail*, WHALES HEAVEN (Jan. 29, 2022) (asserting that P2P transactions occur directly between individuals without the intervention of central authorities, ultimately connecting individuals through a network of trades, rather than revealing anyone's identity on the platform) [perma.cc/WBZ4-7V4U].

140. *See* FIN. CRIME ACAD., *supra* note 119 (exploiting the anonymity and decentralization in the DeFi sector has allowed criminals to continue laundering money through complex networks of transactions).

numerous methods utilized by criminals to launder money through cryptocurrency, cryptocurrency's characteristics provide a robust breeding ground for traffickers to construct their limbo to ensnare victims like Sarah or Sonith.

C. Cryptocurrencies Attempt to Implement Anti-Money Laundering Measures, but Remain Resistant to Traditional Financial Regulations

Not only do cryptocurrency's characteristics enhance its resistance to traditional "follow the money" techniques, but similar issues arise in the realm of regulation. In the United States, the Financial Crimes Enforcement Network ("FinCEN") requires cryptocurrency exchanges to comply with Anti-Money Laundering ("AML") requirements because FinCEN considers these exchanges as Money Services Businesses ("MSBs").[141] However, these regulations falter in practice because cryptocurrency's decentralized nature makes it highly resistant to traditional forms of financial regulation.[142]

A prime AML requirement includes "Know Your Customer" ("KYC") standards, and FinCEN requires all cryptocurrency exchanges to carry out KYC checks on their users.[143] Generally, to comply with this form of customer due diligence, FinCEN requires MSBs to: (1) identify and verify the identity of customers; identify and verify the identity of the beneficial owners of entities opening accounts; (2)

---

141. Josias N. Dewey & Samir Patel, *Blockchain & Cryptocurrency Laws and Regulations 2024*, GLOBAL LEGAL INSIGHTS (2024) [perma.cc/Q2ZT-6VA8].

142. See *id.* (emphasizing that the decentralized nature of cryptocurrencies make it difficult for government agencies, such as FinCEN, to integrate it within traditional financial regulations).

143. *See* Lightico Marketing Team, *Crypto KYC/AML in the US and Around the Globe*, LIGHTICO (explaining that cryptocurrency exchanges in the U.S. are facing stricter scrutiny by regulators, as these exchanges face AML requirements to combat money laundering) (2024) [perma.cc/5UD4-RXGW]; *see also* Dewey & Patel, *supra* note 141 (clarifying that in 2013, FinCEN issued guidance requiring virtual currency exchanges to follow AML policies) [perma.cc/Q2ZT-6VA8].

understand the nature and purpose of customer relationships to develop customer risk profiles; and (3) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[144] In other words, to satisfy KYC standards, MSBs must require users to provide personal information, which can include their full legal name, date of birth, current residential address, and a social security number or other government-issued identification number.[145] However, while cryptocurrencies attempt to adhere to this standard, its characteristics still include many aspects of decentralization, creating multiple vulnerabilities compared to KYC measures in the context of traditional banks.[146]

Ideally, KYC measures act as onboarding processes for cryptocurrency exchanges to verify their users' identities and conduct due diligence to ensure that users do not participate in illegal activities.[147] However, cryptocurrencies breed vulnerabilities within its KYC measures compared to traditional banks.[148] For instance, while all banks may not

144. *See Information on Complying with the Customer Due Diligence Final Rule*, FIN. CRIMES ENF'T NETWORK (explaining that the Customer Due Diligence Rule aims to improve financial transparency and prevent criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains) [perma.cc/T45W-LQMB].

145. *See Why Know Your Customer (KYC) – for Organizations*, U.S. BANK (Aug. 17, 2023) (gathering KYC information will help limit exposure to risk for banks and their clients) [perma.cc/L6KM-9NXC].

146. *See* Anna Stylianou, *KYC/CDD in Traditional Banking vs. KYC/CDD in Crypto*, LINKEDIN (Apr. 19, 2022) (emphasizing the weaknesses of crypto's current KYC requirements compared to banks) [perma.cc/X9GY-JVPZ]; *see also* FM Contributors, *The KYC and AML Challenges of Cryptocurrency Exchanges: Solutions and Best Practices*, FM (Mar. 31, 2023) ("[T]he anonymous nature of cryptocurrency transactions makes it difficult to successfully execute KYC regulations.") [perma.cc/6TM6-TUXF]; *see also* Gokhan Polat, *KYC Challenges in the Crypto Ecosystem*, MEDIUM (Sept. 28, 2023) (identifying the risk factors involving cryptocurrency service providers, especially in the face of imposing traditional KYC techniques onto crypto) [perma.cc/5P3G-KXQU].

147. *See What is KYC for Crypto and Why Does it Matter?*, TRULIOO (2023) (providing an overview as to how KYC measures aid in tracking criminal activity on cryptocurrency exchanges) [perma.cc/MMH2-NE9J].

148. *See* Richard M., *Crypto KYC: A Growing Need for Industry Regulation*, SHUFTIPRO (last updated Oct. 16, 2023) (calling attention to

share identical KYC policies, banks deal with face-to-face clients, whereas cryptocurrencies do not.[149] Specifically, because cryptocurrency users complete this process online, this makes it more difficult to be entirely sure that the individual is who they purport to be.[150]

With banks, a customer typically visits a bank in person to open an account to obtain full access to its banking services.[151] Therefore, in traditional banking, employees at the bank must obtain real identification documents and proof of address from the client.[152] However, cryptocurrency exchanges places great emphasis on establishing "quick and efficient" KYC procedures.[153] While the average consumer

---

the requirement by the U.S. government for cryptocurrencies to adopt KYC procedures, but, that these procedures may not be required in all jurisdictions internationally) [perma.cc/HSG7-EJ53]; *see also* Anna Stylianou, *KYC/CDD in traditional banking vs. KYC/CDD in crypto*, LINKEDIN (Apr. 19, 2022) (emphasizing the weaknesses of crypto's current KYC requirements compared to banks) [perma.cc/X9GY-JVPZ]; *see also Robust KYC Process: Why Crypto Exchanges Need It & Tips to Strengthen KYC Measures*, LINKEDIN (June 29, 2023) (strengthening KYC measures is crucial for crypto exchanges to prevent criminals from taking advantage of their platforms to conduct illegal activity) [perma.cc/MV3W-9JLM].

149. *See* Stylianou, *supra* note 148 (emphasizing that a weakness of crypto's current KYC processes includes the fact that with banks, customers must go through traditional routes of KYC such as visiting a bank and bringing verifying materials, but with crypto, all clients may access their platforms virtually while completing the KYC process virtually).

150. *See id.* (verifying cryptocurrency users via a non-face-to-face route creates an increased risk of fraud because it is difficult for an entity to be entirely sure that the verification documents match the exact user).

151. *See id.* (utilizing virtual verification creates increased risks of fraud because it is difficult for an entity to be entirely sure that the verification documents match the exact user).

152. *See* Eddie Ponce, *What Does KYC Mean for Crypto?*, MITEK (June 21, 2022) ("John Doe goes in-person to a branch where a teller asks for their ID and login information. The teller can also see, in real-time, that John is who he says he is.") [perma.cc/W5GR-JYCL].

153. *See* Jason Tucker-Feltham, *How Criminals Leverage Non-compliant Crypto Exchanges for Money Laundering*, IDNOW (2024) (emphasizing the "long and bumpy road toward compliance" due to non-compliant crypto exchanges providing an accessible avenue for criminals to launder money) [perma.cc/MMW8-NF5H]; *see also The Rise of Cryptocurrency in Modern Slavery*, VERAFIN (Apr. 19, 2023) (discussing

may appreciate efficient KYC processes compared to the requirement of a face-to-face interaction, this efficiency attracts criminals.[154] For instance, with cryptocurrencies, the verification procedure is entirely virtual.[155] Therefore, cryptocurrencies accept photos of the user's identification and other documentation.[156] Ultimately, cryptocurrencies possess numerous holes in its KYC processes.

For instance, in October of 2019, the U.S. Department of Justice indicted twenty-three-year-old Jong Woo Son, who operated a dark website devoted to Child Sexual Exploitation Materials ("CSEM").[157] The platform, Welcome to Video ("WTV") began operations in 2015 and as of 2018 had over 200,000 unique video files on its server containing CSEM.[158] WTV customers created free accounts on the site and downloaded videos by redeeming points.[159] Specifically, WTV customers could purchase these points with Bitcoin.[160] From the site's inception in 2015 through 2018, WTV received at

---

the ineffectiveness of traditional methods to investigate suspected illicit activities within the context of crypto-related crimes) [perma.cc/K6SC-7JUA].

154. *See* Tucker-Feltham, *supra* note 153 (arguing that KYC processes do not properly abide by KYC requirements).

155. *See What is KYC in Crypto?*, VERIFF (Apr. 6, 2023) (pointing out that every crypto exchange will handle KYC differently, but in most cases customers will be required to provide a photo of a valid government-issued ID card, requiring no in-person component) [perma.cc/BC25-2LPH]; *see also Crypto KYC Requirements*, ONFIDO (2024) (explaining that the dark side to cryptocurrency arises from money laundering, which is why robust KYC requirements are needed) [perma.cc/GME4-5AJU].

156. *See* VERIFF, *supra* note 155 (pointing out that every crypto exchange will handle KYC differently, but in most cases customers will be required to provide a photo of a valid government-issued ID card, requiring no in-person component).

157. *See* THE INT'L CTR. FOR MISSING & EXPLOITED CHILD., CRYPTOCURRENCY AND THE TRADE OF ONLINE CHILD SEXUAL ABUSE MATERIAL 6–7 (2021) (mentioning that the takedown of the Welcome to Video platform constituted one of the largest ever seizure of CSEM by volume).

158. *See id.* at 6 (describing the website's development" . . . around March 2018 had over 200,000 unique video files on its server.").

159. *See id.* (explaining the site's operating model).

160. *See id.* (same).

least 7,300 transactions via Bitcoin.[161] When the site dissolved in March of 2018, it contained over one million Bitcoin addresses hosted on the website's server.[162] Within the realm of KYC efficacy, WTV failed, as the Bitcoin accounts it housed did not have registered names, indicating that customers holding those accounts linked to the WTV site failed to provide sufficient KYC information.[163]

Another case, this one involving the operation of the "DarkScandals" website, also displays the overwhelming failure of KYC methods to solve the issue of anonymous aspects of cryptocurrency exchanges.[164] In this case, DarkScandals sold "packs" of CSEM, and the site received thousands of deposits, totaling about 188.6631 in Bitcoin, which amounted to $1.6 million in U.S. dollars.[165] Tragically, Michael Rahim Mohammad ("Mr. Dark"), the owner and operator of DarkScandals, made almost $2 million in U.S. dollars from selling the CSEM.[166] As a result, the forfeiture complaint revealed that hundreds of accounts held in crypto exchanges associated with DarkScandals had either false or nonexistent KYC documents.[167] Clearly, criminals in the age of Web 3.0 take advantage of the vulnerabilities within

161. *See id.* (discussing that WTV received "at least" 7,300 transactions worth over $370,000 via Bitcoin).

162. *See id.* (" . . . there were over one million Bitcoin addresses hosted on the website's server . . . ").

163. *See id.* at 8 (discussing that many of the Bitcoin accounts indicated a lack of complete KYC information).

164. *See id.* at 9 (emphasizing that large payments were sent to DarkScandals originating from accounts solely used to open and send funds to the site).

165. *See* United States v. Three Hundred Three Virtual Currency Accounts, DarkScandals Domain, and DarkScandals.co Domain, No. 20-cv-712, 2021 U.S. Dist. LEXIS 30718, at *2 (D.D.C. Feb. 19, 2021) ("The Website delivered these illicit materials in 'packs,' each of which 'contained approximately 2,000 videos and images.'").

166. *See* Cunningham, *supra* note 157, at 10 (specifying that Michael Rahim Mohammad made a substantial profit by selling CSEM).

167. *See* Verified Compl. For Forfeiture *In Rem* at ¶ 53, United States v. Three Hundred Three Virtual Currency Accounts, DarkScandals Domain, and DarkScandals.co Domain, No. 20-cv-712, 2021 U.S. Dist. LEXIS 30718 (D.D.C. Feb. 19, 2021) (emphasizing that many of the accounts did not have KYC documents).

cryptocurrency exchanges, including the lack of robust KYC processes.[168] While FinCEN implemented KYC processes with the goal of ensuring a decrease in illicit activities, criminals optimized cryptocurrency's vulnerabilities by taking advantage of its decentralized nature and its inconsistent KYC compliance policies. Ultimately, without a uniform or robust KYC process associated with crypto exchanges, traffickers will continue to force innocent, vulnerable individuals into a terrifying state of limbo.

III. The Legislative and Judicial Responses to Human Trafficking Inadvertently Increased Violence Against Vulnerable Groups

In the United States, TVPA and FOSTA are two statutes that fight against human trafficking through enforcement and prosecution.[169] Although TVPA existed before FOSTA, in the wake of cyber-trafficking, legislators created FOSTA to provide victims with further means to prosecute internet intermediaries that played a role in victimizing individuals on their platforms.[170] While Congress passed FOSTA with the best intentions, this bill exacerbated the risk of human trafficking and failed to provide trafficking survivors with an avenue towards justice within the realm of Web 3.0.[171]

168. *See id.* (pointing out the fact that hundreds of accounts registered to crypto exchanges lacked KYC information, clearly an effort by criminals to conceal their identities).

169. *See generally* Colin Martell, *Customer Transparency Can Dampen the Growing Human Trafficking Problem*, 14 J. BUS. ENTREPRENEURSHIP & L. 35 (2021) (examining the policies passed in the United States to combat human trafficking).

170. *See* Aaron Mackey, *The Fight to Overturn FOSTA, an Unconstitutional Internet Censorship Law, Continues*, ELEC. FRONTIER FOUND. (Sept. 15, 2022) (mentioning that FOSTA has expanded the space to capture internet intermediaries in criminal and civil liability) [perma.cc/UA9J-4ZQS].

171. *See* Romano, *supra* note 50 (passing FOSTA has resulted in websites entirely shutting down chat rooms or pages, ultimately putting sex workers in greater danger); *see also* Liz Tung, *FOSTA-SESTA Was Supposed to Thwart Sex Trafficking. Instead, It's Sparked a Movement*, WHYY (July 10, 2020) (maintaining that FOSTA has put sex workers' lives in danger) [perma.cc/GUZ4-F46Z].

Accordingly, Congress inadvertently exposed vulnerable individuals, like Sarah and Sonith, to a cruel state of limbo. To provide context about these laws and their effects, Part III.A will shed light on Section 230's background and the history of its passage.[172] Following that discussion, Part III.B will discuss FOSTA as Congress's pendulum swing.[173] Finally, Part III.C will discuss how FOSTA fails to hold internet intermediaries accountable for trafficking, while increasing individuals' risk of victimization.[174]

A. Before FOSTA's passage, Section 230 forbid victims of human trafficking from prosecuting internet intermediaries

FOSTA amended Section 230 to allow prosecutors and injured parties the path of least resistance in the process of holding internet intermediaries criminally and civilly liable, particularly when these platforms have facilitated sex trafficking.[175] Before FOSTA, courts generally interpreted Section 230 as an avenue for immunity from civil liability for third-party postings.[176] However, given the pervasive growth of cyber-trafficking, Congress swung its ideological pendulum in response to holding bad actors accountable in the landscape of Web 3.0.[177] In turn, an explanation of Section 230's background must precede the discussion of FOSTA's passage to provide a comprehensive understanding of how they operate together.

---

172. *See generally* Part III.A.

173. *See generally* Part III.B.

174. *See generally* Part III.C.

175. *See* Kendra Albert, et al., *FOSTA in Legal Context*, 52 COLUM. HUMAN RIGHTS L. REV. 1084, 1088 (2021) ("FOSTA materially limits the scope of the Communications Decency Act (CDA) for the first time since the latter's enactment over two decades ago.").

176. *See id.* at 1095 ("Courts have generally interpreted § 230(c) as creating broad immunity from civil liability for third-party postings).

177. *See generally* Part III.B.

Section 230, passed in 1996, safeguarded free speech online in the wake of Web 1.0.[178] Accordingly, courts interpreted it broadly, rarely holding website owners accountable for users' illegal activities.[179] For instance, section 230(c)(1)'s provision provided protection for "Good Samaritan Blocking and Screening of Offensive Material."[180] Specifically, section 230(c)(1) states that "no provider or user of an interactive computer service ('ICS') shall be treated as the publisher or speaker of any information provided by another information content provider ('ICP')."[181] In 47 U.S.C. § 230(f), it defines ICS as any information service that provides or enables computer access by multiple users to a computer server, including a service that provides access to the internet while any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.[182]

Moreover, 47 U.S.C. § 230(f) defines an ICP as any person or entity responsible, in whole or in part, for the creation or development of information provided through the internet or any other interactive computer service.[183] Thus, Section 230 provided immunity to defendants when: (1) the defendant acted as a provider or user of an ICS; (2) the claim

178. *See* 47 U.S.C. § 230(c) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

179. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 317, 328–29 (4th Cir. 1997) (finding America Online protected by Section 230 immunity despite it having notice of defamatory content posted on its site); *see also, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 415 (5th Cir. 2008) (finding MySpace immune under Section 230 despite accusations of a sexual assault of a minor that arose from posts on the MySpace platform); *see also, e.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) (finding Craigslist immune from creating classified services alleged to facilitate prostitution); *see also e.g.*, Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *20 (E.D. Tex. Dec. 27, 2006) (finding that Section 230 grants immunity to websites even when third-party posts contain child pornography).

180. 47 U.S.C. § 230(c).

181. *Id.*

182. *See* 47 U.S.C. § 230(f) (defining "interactive computer service").

183. *See id.* (same).

based itself on information provided by another ICP; and (3) the claim would treat the defendant as the publisher or speaker of that information.[184] Section 230 plays a prominent role in encouraging free speech on the internet, but in the same vein, this statute grants broad immunity to websites involved in trafficking.[185]

Although courts generally interpreted Section 230 broadly,[186] an impactful case, *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,[187] represents a court's pendulum swing by limiting Section 230.[188] Specifically, the Ninth Circuit distinguished between "passively displayed" content on a website and content that a website "creates in whole or in part."[189] The defendant, Roommates.com, matched individuals with potential tenants or roommates.[190] To use the website, users created profiles by answering a series of questions, usually about their gender, sexual orientation, and other relevant biographical information.[191]

Beyond these initial questions, an "Additional Comments" section allowed users to further describe what characteristics they sought in a potential tenant or roommate.[192] Plaintiff, The Fair Housing Council of San

184. *See* Albert, *supra* note 175, at 1093 (providing an explanation of Section 230's protection for internet intermediaries).

185. *See id.* at 1095 (asserting that Section 230 created broad immunity from liability for internet intermediaries).

186. *See generally supra* note 179.

187. 521 F.3d 1157 (9th Cir. 2008).

188. *See* Fair Housing Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1162–63 (9th Cir. 2008) (distinguishing between content a website passively displays and content a website creates in whole or in part).

189. *See id.* at 1165–67 (holding that immunity under Section 230 of the Communications Decency Act did not apply to an interactive online operator whose questionnaire violated the Fair Housing Act, ultimately limiting the broad immunity that Section 230 previously gave to service providers).

190. *See* Roommates.com, 521 F.3d at 1181 (outlining how the website operates).

191. *See id.* at 1161 (detailing how users can use the website).

192. *See id.* at 1175 (describing how the "Additional Comments" section operates).

Fernando Valley, brought an action against defendant, alleging that the website violated the Fair Housing Act by allowing users to discriminate against groups of individuals, via the website's questionnaires.[193] Defendant argued that Section 230 provided the website immunity because it constituted an interactive website, not an ICP.[194] Nevertheless, the Ninth Circuit found that the defendant rose above the level of a "passive transmitter," and did not grant Defendant Section 230 immunity.[195]

After *Roommates.com*,[196] the breadth of Section 230 immunity revolved around whether an ICS engaged in the "creation or development" of material on its site and whether an ICS "contributes materially to the alleged illegality of the conduct."[197] For instance, in *Roommates.com*,[198] the Ninth Circuit emphasized that the defendant created the questions to prompt users, ultimately designing its website registration process around them.[199] Further, the Ninth Circuit found that these questions, made by the defendant, transmitted more than passive information provided by users; it became the developer, at least in part, of the information.[200] While *Roommates.com*[201] strayed from the broad scope of Section 230 immunity, the critical takeaway provided that if an ICS's actions do not rise to the level of "creation or

193. *See id.* at 1163 (alleging that requiring subscribers to disclose their sex, family status, and sexual orientation "indicates" an intent to discriminate against them).

194. *See id.* at 1173 (stating that the defendant argued that the website should benefit from Section 230 immunity).

195. *See* Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1166 (9th Cir. 2008) (concluding that the defendant did not get Section 230 immunity).

196. 521 F.3d 1157 (9th Cir. 2008).

197. *See Roommates.com,* 521 F.3d at 1179 (discussing that the key to Section 230's immunity provision includes the idea of whether the entity took part in the creation or development of the disputed information).

198. 521 F.3d 1157 (9th Cir. 2008).

199. *See* Roommates.com, 521 F.3d at 1165 (creating the questions and choices of answers meant that the defendants took part in the creation and development of the platform).

200. *See id.* (same).

201. 521 F.3d 1157 (9th Cir. 2008).

development," an ICS will maintain Section 230 immunity.[202] Despite this pendulum swing by the Ninth Circuit, the majority of Section 230 jurisprudence provides internet intermediaries with broad opportunities to escape liability from cyber-trafficking.[203] In fact, concerns about courts' broad interpretation of Section 230 when addressing sex trafficking, combined with the disturbing case of *Backpage.com*,[204] would ignite the legislative pendulum swing by Congress: the passage of FOSTA.[205]

In *Backpage.com*, the appellants (three women) brought claims under 18 U.S.C. § 1595, alleging that sex traffickers exploited them on Backpage as minors.[206] The appellants emphasized that Backpage did not represent a passive publisher, and that Backpage created and developed materials on its site to facilitate trafficking.[207] Moreover, the appellants asserted that these advertisements constituted a "participation in a venture" of sex trafficking, which violated the TVPA.[208] However, the First Circuit found in favor of the defendant, concluding that the defendant's website qualified as an ICS, providing the defendant with Section 230

202. *See* Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2008) (laying out the application of Section 230 to the instant case).

203. *See* Albert, *supra* note 175, at 1095 (asserting that Section 230 created broad immunity from liability for internet intermediaries).

204. Jane Doe No. 1 v. Backpage.com, 817 F.3d 12, 19 (1st Cir. 2016).

205. *S*ee Albert, *supra* note 175, at 1098 (explaining how sites like Backpage.com avoided liability due to § 230's immunity despite its use of sex trafficking minors); *see also* Emily J. Born, *Too Far and Not Far Enough: Understanding the Impact of FOSTA*, 94 N.Y.U. L. REV. 1623, 1624–25 (2019) (asserting that prior to Backpage.com's seizure, sex traffickers utilized the website frequently, which prompted President Trump to sign FOSTA).

206. *See* Backpage.com, 817 F.3d at 17 (explaining that the appellants brought claims because Backpage allegedly exploited them).

207. *See id.* at 19 (emphasizing the appellants' arguments regarding passive publishing).

208. *See id.* (detailing the appellants' arguments about the defendant allegedly violating the TVPA).

immunity.[209] This grant of immunity constituted a primary instigator of FOSTA's passage.[210]

B. The Court of Public Opinion Ignited Congress's Ideological Pendulum Swing, Resulting in FOSTA's Passage

In 2018, following an aggressive but necessary outcry from the public, Congress passed FOSTA.[211] This outcry began with Backpage facilitating a platform for traffickers to ensnare innocent women into limbo, which prompted fifty-one of the nation's Attorneys General, on behalf of the National Association of Attorneys General ("the Association"), to write a letter to Backpage expressing concerns regarding sex trafficking on the website.[212] The letter mentioned that the Association tracked over fifty instances in twenty-two states over three years against traffickers lurking on Backpage.[213] Additionally, the Association requested that Backpage provide descriptions of

209. *See id.* at 24 (concluding that the First Circuit granted the defendant with Section 230 immunity).

210. *See* Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018) (emphasizing that courts have taken Section 230 too far, and that it has been used to defend Backpage.com) [perma.cc/G3BQ-96BH].

211. *See id.* (reporting on the outcry caused by the *Backpage* ruling); *see also* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Publ L. No. 1115–164, 132 Stat. 1253 (codified and amended in scattered sections of 18 and 47 U.S.C.) (amending the TVPA to define phrases related to the prohibition of sex trafficking).

212. *See generally* Letter from Rob McKenna, President of Nat'l Ass'n of Att'ys Gen., to Samuel Fifer, Couns. for Backpage.com, LLC (Sept. 16, 2011) [hereinafter McKenna-Fifer Letter] (asserting that chief law enforcement officers across the country have voiced concerns about Backpage acting as a hub for human trafficking).

213. *See* Emily J. Born, *Too Far and Not Far Enough: Understanding the Impact of FOSTA*, 94 N.Y.U. L. REV. 1623, 1629–31 (2019) (detailing the public outcry against Backpage upon the First Circuit's decision against the plaintiff-appellants to hold Backpage accountable for allegedly facilitating sex trafficking of minors); *see also generally* McKenna-Fifer Letter, *supra* note 212 (asking on behalf of fifty-one attorney generals, that Backpage.com should shut down its adult services section, similar to what Craigslist decided to do when there were reported instances of underage sex trafficking).

their understanding of "illegal activities," copies of their oversight policies, and copies of lists of prohibited terms on their site to assist outsiders in better understanding the company's methods in tracking and avoiding illegal activities.[214] While Backpage responded to the letter, detailing their plans to prevent trafficking on the site, law enforcement throughout the U.S. still deemed the site as an "accelerant" of sex trafficking.[215]

Beyond this letter, the Backpage scandal elicited a myriad of other public outcries throughout the next few years.[216] In 2012, protesters gathered in front of the offices of the New York City's Village Voice Media, the owner of Backpage, demanding that they shut down the site due to trafficking.[217] Within a few months, twenty-seven major advertisers, including H&M, AT&T, and Ikea, pulled their ads from Village Voice Media due to the company's alleged links to child sex trafficking.[218] By 2015, the U.S. Senate Permanent Subcommittee on Investigations began its investigation of Backpage.[219] The Subcommittee's report

214. *See* McKenna-Fifer Letter, *supra* note 212, at 4–6 (outlining the requests sent to Backpage.com).

215. *See* Jeff Kappel, *Mayor Updates Public on Efforts to Combat Sexual Exploitation of Children on Backpage.com*, SEATTLE POLICE DEP'T (Sept. 28, 2011) (emphasizing that even after attorneys general sent a letter to Backpage calling for information about the company's efforts to deter sex trafficking, police still believe that Backpage acts as an accelerant for sexual exploitation of minors) [perma.cc/EQ5R-UQYU].

216. *See generally infra* notes 217–222 and accompanying discussion.

217. *See New York's Village Voice Draws Protests Over Classifieds Linked to Child Sex Trafficking*, FOX NEWS (Mar. 30, 2012) ("Nearly 100 protesters gathered in front of the paper's editorial offices . . . to demand that Village Voice Media-owned Backpage.com be shut down because its adult classified section includes ads that have been linked to prostitution involving minors.") [perma.cc/4SJX-G62L].

218. *See Village Voice Not Backing Down After 27 Companies Pull Ads Over Child Sex Trafficking*, BUS. INSIDER (May 3, 2012) (explaining that a Change.org campaign prompted major advertisers to leave the Village Voice Media, but Village Voice Media asserted an aggressive defense of Backpage.com to contest the claim that its classified ads are a source of sex trafficking) [perma.cc/R66C-ZPLS].

219. *See generally* PERMANENT SUBCOMM. ON INVESTIGATIONS, 114TH CONG., BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX

found that Backpage "knowingly" concealed evidence of criminality by systematically editing its adult ads[220] and that Backpage executives knew that their website facilitated illegal activities, such as sex trafficking.[221] In turn, the public outcry came to a crescendo as mainstream media created public service announcements featuring Amy Schumer, Seth Meyers, and other celebrities advocating for an amendment to Section 230, calling it a "stupid loophole."[222] By 2018, Congress responded by amending Section 230 via H.R. 1865,[223] thus creating FOSTA.[224]

C. Despite Congress's Intent in Passing FOSTA, It Failed Its Mission by Displacing the Threat of Trafficking onto Other Vulnerable Populations

Congress amended Section 230 with FOSTA, intending to restrict the scope of Section 230 immunity for website providers that published content promoting or facilitating trafficking.[225] FOSTA provides that internet intermediaries will not receive Section 230 immunity for (1) a federal civil claim brought under § 1595 of the TVPA or (2) a criminal charge for conduct that would constitute a violation of TVPA § 1591.[226] In other words, should an ICS violate any of the

---

TRAFFICKING (2017) (outlining the investigation regarding Backpage.com's participation of trafficking).

220. *See id.* at 5 (emphasizing that Backpage.com "knowingly concealed evidence of criminality").

221. *See id.* (concluding that Backpage.com encouraged trafficking on its site by editing ads to conceal the "true nature" of the transaction).

222. Mary Mazzio, *PSA Featuring Seth Meyers, Amy Schumer, Josh Charles, Tony Shalhoub and Others – SESTA*, VIMEO (Jan. 11, 2018) (showcasing celebrities' complaints about Section 230) [perma.cc/2XHY-DLN8].

223. *See* Allow States and Victims to Right Online Sex Trafficking Act of 2017, Pub. L. No. 1115–164, 132 Stat. 1253 (codified and amended in scattered sections of 18 and 47 U.S.C.).

224. *See id.* (amending the Communications Decency Act).

225. *See* Albert, *supra* note 175, at 1100 (emphasizing that FOSTA restricted the scope of Section 230 immunity).

226. *See* Albert, *supra* note 175, at 1114 (detailing FOSTA's limit on Section 230 immunity).

aforementioned laws, Section 230 will not shield it from liability.[227]

By exposing these internet platforms to liability for third-party content, this amendment represents a significant ideological pendulum swing in the law.[228] While this "swing" intended to protect more users from trafficking in the new age of Web 3.0, it resulted in a chilling effect that Section 230 originally intended to prevent.[229] For instance, websites shut down from a fear of liability.[230] As a result, sex workers lost affordable advertising spaces and access to platforms to share safety information with one another.[231] In turn, this created opportunities for traffickers to ensnare sex workers into limbo because of the loss of online platforms to facilitate vetting processes.[232] Moreover, law enforcement officers can no longer use these sites as a starting point to investigate sex trafficking or locate missing sex trafficking victims.[233]

Because sex workers lost online platforms to advertise and vet their clients, they returned to in-person methods of finding clients, with minimal vetting processes.[234] In fact, in the two years since FOSTA's passage, sex work advocacy groups reported a spike in the number of missing and dead

227. *See id.* (stating that Section 230 will not shield an ICS in certain circumstances).

228. *See id.* ("By exposing ICSs to liability for third-party content, FOSTA represents a significant shift in the law.").

229. *See id.* (noting that these chilling effects include entire sites shutting down certain aspects of their platforms because of a fear of prosecution).

230. *See id.* (same).

231. *See* Caty Simon, *On Backpage*, TITS & SASS (Apr. 25, 2018) (expressing concerns from sex workers about FOSTA, as it has resulted in a substantial cutback on advertising spaces) [perma.cc/VMG6-TVSZ].

232. *See id.* (same).

233. *See* Albert, *supra* note 175, at 1102 (detailing the terrifying consequences FOSTA has placed upon sex workers, specifically that law enforcement has reported a difficulty in investigating trafficking claims because entire platforms have shut down).

234. *See* Chamberlain, *supra* note 48, at 2203 (emphasizing that FOSTA has endangered individuals in the sexual service market by displacing their vetting processes and forcing them back onto the street).

sex workers across the country.[235] Within one month following FOSTA's enactment, thirteen sex workers were reported missing.[236] Additionally, COYOTE, an organization advocating for labor rights of sex workers conducted surveys in 2022, seeking to quantify FOSTA's impact.[237] COYOTE found a sixty-four percent increase in trafficking survivors who were coerced into sex work.[238] Further, the survey indicated a fifty-six percent increase of trafficking survivors who were coerced into the sex work industry as minors.[239]

Beyond these findings, anecdotal evidence substantially supports the idea that sex workers need online platforms to advertise, vet, and choose clients as safeguards.[240] Clearly, FOSTA forces sex workers back onto the streets to find new clients, causing them to lose their vetting processes, and no assurance that they will work in safe conditions upon meeting a client.[241] For instance, Danielle Blunt, a professional dominatrix, confirmed these dangers.[242] Specifically, Blunt confirmed that losing access to internet spaces creates "devastating" effects within the community's ability to take care of themselves, to make money, and to screen clients and stay safe.[243]

---

235. *See id.* (emphasizing that the loss of online platforms has created dangerous circumstances for sex workers to be potential victims of sex trafficking).

236. *See id.* (detailing the harm towards sex workers upon FOSTA's enactment).

237. *See* TARA BURNS & ALLIE BENZ, *FOUR YEARS OF FOSTA: THE SURVEY* 3–4 (2022) (explaining that COYOTE worked with a group of 332 sex workers and sex trafficking survivors to assess the effects of the four years of FOSTA through a series of surveys and interviews).

238. *See id.* at 6 (providing statistics on the effects of FOSTA).

239. *See id.* (same).

240. *See* Romano, *supra* note 50 (explaining that these laws arguably endanger sex workers because it forces them to walk the streets, rather than advertising online and screen clients beforehand).

241. See *id.* (same).

242. *See* Tung, *supra* note 171 (summarizing Danielle Blunt's negative experience with informal vetting processes).

243. *See id.* (same).

FOSTA's passage resulted in an increase of human trafficking victims by 30,000.[244] By 2022, the number of reported human trafficking victims increased to similar levels in 2019, the year following the passage of FOSTA.[245] As FOSTA wreaks havoc on sex workers' livelihood while failing to dampen cyber-trafficking, traffickers will continue to participate in trafficking with Web 3.0's tools, such as online platforms and cryptocurrencies. In fact, forty online sex trafficking platforms widely accept virtual currencies while social media continues to bolster trafficking activity.[246] Between 2019 and 2020, while traditional sites like bus stops and strip clubs declined in trafficking activity, Facebook saw a 125% increase in trafficking recruitment.[247] Due to a lack of governmental presence in these Web 3.0 spaces, traffickers adapted to using these tools to capture victims, like Sarah and Sonith, into horrendous states of limbo. The sad reality remains: cryptocurrency and FOSTA constitute the pillars of cyber-trafficking.

IV. FOSTA's Judicial Framework Fails to Protect Victims of Cyber-Trafficking

The current caselaw interprets FOSTA's restriction on Section 230 narrowly, failing to provide victims of trafficking with a sufficient means towards justice.[248] Although Congress intended to expand the prosecutions under section

244. *See Total Number of Human Trafficking Victims Identified Worldwide from 2008 to 2022*, STATISTICA (last updated Sept. 1, 2023) (detailing the statistics which conclude that human trafficking victims increased since FOSTA's passage) [perma.cc/8BX8-P4HR].

245. *See id.* (outlining data which displays trafficking trends since FOSTA's passage).

246. *See* Ted Knuston, *Crypto Increasingly Used in Human/Drug Trafficking*, FORBES (Jan. 10, 2022) (emphasizing sex trafficking platforms' acceptance of virtual currencies) [https://perma.cc/R3WD-38TX].

247. *See* Matthew Bergman, *Human Trafficking Starts Early and Online*, SOCIAL MEDIA VICTIMS LAW CENTER (Feb. 26, 2024) ("Facebook experienced a 125% increase in trafficking recruitment. The nearly 95% increase only rivals that number in those using Instagram to find victims.") [perma.cc/E7C2-YAP6].

248. *See generally infra* note 251.

1591 of the TVPA's "participation in a venture" requirement, FOSTA's impact on this provision works against Congress's original aims.[249] Accordingly, beyond FOSTA's failure to deter human trafficking, it increased the threat of cyber-trafficking towards sex workers, while preventing victims from seeking appropriate justice in court.[250]

The D.C. Circuit and the Ninth Circuit addressed FOSTA claims.[251] Although the D.C. Circuit discussed FOSTA's constitutionality,[252] the Ninth Circuit issued an opinion specifically regarding FOSTA's restriction on Section 230 in the context of sex trafficking.[253] In *Does v. Reddit, Inc.*,[254] the Ninth Circuit interpreted FOSTA narrowly, even in the face

---

249. *See* Albert, *supra* note 175, at 1127.

> Regardless of which mens rea interpretation is adopted by courts, it is clear that the new definition of "participation in a venture" has added specific conduct ('assisting, supporting, or facilitating') that triggers culpability for third-party defendants. While this new language may or may not be more specific than the previously undefined 'participation,' any degree of potential specificity added does not necessarily make the statute easier to apply. It is instead possible that this specific conduct now constitutes an additional element that must be proved at trial–an outcome the DOJ warned against prior to FOSTA's passage.

250. *See* Elliot Harmon, *Amended Version of FOSTA Would Still Silence Legitimate Speech Online*, ELEC. FRONTIER FOUND. (Dec. 11, 2017) (emphasizing that Section 230 still has a broad coverage of immunity) [perma.cc/NS8Q-4CRA].

251. *See* Woodhull Freedom Found. v. United States, 72 F.4th 1286, 1292 (D.C. Cir. 2023) (finding that FOSTA is not overbroad nor unconstitutionally vague); *see also* Does v. Reddit, Inc., 51 F.4th 1137 (9th Cir. 2022) (addressing liability of an online platform in relation to a trafficking complaint).

252. *See Woodhull Freedom Found.*, 72 F.4th 1286, 1292 (D.C. Cir. 2023) (finding that FOSTA's clarification of Section 230 regarding violations of federal sex trafficking laws comports with the First Amendment).

253. *See Reddit, Inc.*, 51 F.4th at 1145 (holding that the plaintiffs did not allege a connection between the child pornography posted on the website and the revenue the website generated, other than the fact that the website made money from advertising).

254. 51 F.4th 1137 (9th Cir. 2022).

of the disturbing factual allegations.[255] The plaintiffs, the parents of trafficked minors, discovered that traffickers posted their children's sexually explicit images and videos to a Reddit page, otherwise known as a "subreddit."[256] Upon this discovery, the plaintiffs reported the content to Reddit employees and subreddit moderators.[257] Following their initial report, the plaintiffs then discovered that the traffickers posted the explicit images to other subreddits, and they contacted Reddit hundreds of times to report these explicit posts.[258]

The plaintiffs alleged that Reddit engaged in little efforts to remove the unlawful content, as it drove user traffic and increased the site's revenue.[259] For instance, when the plaintiffs filed this suit, Reddit hosted subreddits openly, and these subreddits explicitly marketed themselves as a forums for child pornography, with page titles such as "TeenBeauties."[260] Further, the plaintiffs alleged that Reddit earned substantial advertising revenue from subreddits featuring child pornography because third-party advertising tools listed these subreddits as popular pages, which

255. *See generally* Aaron P. Rubin, et al., *Ninth Circuit Interprets FOSTA Restriction on Section 230 Narrowly*, MORRISON FOERSTER (Oct. 28, 2022) (summarizing how this decision by the Ninth Circuit represents a victory for intermediaries seeking broad protection from Section 230 immunity) [perma.cc/5RM2-JLQW].

256. *See Reddit, Inc.*, 51 F.4th at 1139 (explaining how a subreddit operates).

257. *See id.* (detailing that each plaintiff discovered their child's explicit image on the subreddit page and immediately reported it to Reddit employees).

258. *See id.* (explaining that the vicious cycle of re-posting the plaintiffs' children's explicit photos on subreddits continued, resulting in the plaintiffs contacting Reddit hundreds of times).

259. *See id.* ("The plaintiffs allege that the presence of child pornography on Reddit is blatant, but Reddit has done little to remove the unlawful content or prevent it from being posted, because it drives up user traffic and revenue.").

260. *See id.* (providing examples of subreddit pages, exhibiting titles which imply child pornography).

encouraged advertisers to buy ad space on those pages.[261] Ultimately, the plaintiffs argued that Reddit financially benefitted from hosting pages featuring child pornography.[262] Based on these allegations, the plaintiffs filed a class-action lawsuit against Reddit under 18 U.S.C. § 1595, claiming that Reddit exposed itself to liability as a beneficiary of child sex trafficking.[263]

The Ninth Circuit's analysis focused on whether the plaintiffs could benefit from FOSTA's exception.[264] While the plaintiffs argued that the court should hold Reddit liable as a beneficiary as a user's conduct violated 18 U.S.C. § 1591, Reddit argued that the court should only hold an internet intermediary liable for its "own" criminal conduct.[265] Ultimately, the Ninth Circuit held that for a plaintiff to invoke FOSTA's immunity exception, they must plausibly allege that the website's "own" conduct constituted participation in the "venture" and violated 18 U.S.C. § 1591.[266] While the plaintiffs' complaint confirmed Reddit's role in their case, the court ruled against them.[267] In other words, the defendant-website must "knowingly benefit" from participating in child sex trafficking.[268]

Proponents of Section 230's unfettered protections of internet intermediaries found this ruling as a significant

261. *See id.* at 1139–40 ("Users publicly 'trade' and solicit child pornography on these pages, and advocacy groups and the press have repeatedly reported this activity to Reddit.").

262. *See id.* at 1140 ("[P]laintiffs contend that Reddit financially benefits from openly hosting child pornography.").

263. *See id.* (explaining that the plaintiffs filed a class action lawsuit).

264. *See id.* at 1141 ("At issue in this appeal is the scope of FOSTA's exception to section 230 immunity for civil child sex trafficking claims.").

265. *See id.* (summarizing Reddit's arguments).

266. *See id.* at 1141–42 (emphasizing that a plaintiff must show that a website's own conduct resulted in their participation in a trafficking venture).

267. *See id.* at 1143 (concluding that "the most important component" in a sex trafficking suit against a defendant-website is its own "participation in the venture").

268. *See id.* at 1145 ("[I[t is clear that FOSTA requires that a defendant-website violate the criminal statute . . . with actual knowledge[.]").

win.[269] However, this substantiates a myriad of prior critiques regarding FOSTA's ineffectiveness.[270] FOSTA's current caselaw neglects to address the breadth of cyber-trafficking victimization. As the United States continues to venture into a Web 3.0 landscape, courts must consider Congress's original intention in passing FOSTA, and utilizing its intention to protect victims of cyber-trafficking.[271] By interpreting FOSTA as if it applies in a Web 1.0 landscape, rather than a Web 3.0 landscape, courts continually rubber-stamp cyber-trafficking on internet intermediaries, playing a role in ensnaring innocent individuals, like Sarah and Sonith, into a cruel state of limbo.

V.Courts Should Engage in an Ideological Pendulum Swing to Combat Cyber-Trafficking

Courts should reconsider the statutory interpretation of FOSTA in the new age of Web 3.0. Because courts strictly interpret FOSTA with regards to Section 230's original meaning, they continually insulate their analysis within the world of Web 1.0, failing to acknowledge the current landscape of Web 3.0.[272] Although the advent of Web 3.0 provides society with technological innovation, it brought

269. *See* Rubin, et al., *supra* note 255 (discussing the significance of this ruling, and emphasizing that in the face of disturbing factual allegations, the Ninth Circuit interpreted FOSTA narrowly).

270. *See* Emily J. Born, *Too Far and Not Far Enough*, 94 N.Y.U. L. REV. 1623, 1643–1645 (2019) (applying FOSTA onto the *Backpage* case and predicting that the new law would not capture Backpage's conduct due to the high standards required, such as "participation in a venture").

271. *See* UNODC CRIME SECTION, *supra* note 24, at iii (finding that the COVID-19 pandemic pushed trafficking further underground, while constraining law enforcement capacities to fight trafficking); *see also* January Contreras & Katherine Chon, *Technology's Complicated Relationship with Human Trafficking*, ADMIN. FOR CHILD. & FAMILIES (July 28, 2022) (identifying a twenty-two percent increase in online recruitment into trafficking schemes and emphasizing that the internet has revealed itself as the top recruitment location for all forms of trafficking since the pandemic) [perma.cc/X3BY-MTGN].

272. *See, e.g.*, *supra* note 178 (providing a list of cases demonstrating courts' application of § 230); *see also supra* Part IV (exploring courts' restrictive readings of FOSTA).

with it the phenomenon of cyber-trafficking. As a response, Congress swung its ideological pendulum by passing FOSTA, and courts should respond with a pendulum swing themselves.[273]

When discussing judicial behavior, scholars often invoke the swinging pendulum as a metaphor.[274] In other words, judicial decisions stand upon a body of law, amounting to the importance of *stare decisis*. While judges carefully develop laws to maintain *stare decisis*, sometimes the judges' decision-making must swing in a way which adapts to the circumstances of present-day society.[275] In the current age of Web 3.0, courts continuously fail to swing the pendulum.[276] Due to courts' tendency to frame the FOSTA discussion within the confines of Web 1.0, they fail to provide cyber-trafficking victims with a means towards justice.[277]

To remedy the jurisprudential obstacles preventing trafficking victims with a means towards justice, courts should consider treating FOSTA similarly to the BSA.[278] When Congress passed the BSA, it did so with the intention of creating paper trails to inform law enforcement of suspicious activity while using it as a weapon to prosecute money launderers based on said paper trail.[279] Accordingly, courts honored this intention by heavily enforcing the BSA

273. *See supra* Part III.A. (describing the circumstances that led to Congress's passage of FOSTA).

274. *See generally supra* note 61 and accompanying discussion.

275. *See* Jack G. Day, *Why Judges Must Make Law*, 26 CASE W. RES. L. REV. 563, 565 (1976) (emphasizing that judges should recognize novel gaps in the law and respond to these novelties by considering deviating from the past application of rules to alter the contours of the precedent).

276. *See Understanding Stare Decisis*, AM. BAR ASS'N (Dec. 16, 2022) (explaining that stare decisis means "let the decisions stand" or "to stand by things decided," and that it constitutes a foundational concept in the American legal system considering it holds courts accountable in terms of ensuring consistency in rulings) [perma.cc/MW8C-K5KM].

277. *See generally supra* Part IV.

278. *See Bank Secrecy Act*, OFF. OF THE COMPTROLLER OF CURRENCY (discussing how the U.S. government has utilized financial institutions to assist in detecting and preventing money laundering) [perma.cc/7Z96-SMCC].

279. *See* Sater, *supra* note 52, at 401 (describing the goals of BSA).

requirements on financial institutions, even those committing non-willful violations.[280]

At face value, internet intermediaries like Reddit, Facebook, or Snapchat do not share many characteristics with financial institutions. However, both intermediaries house rich information environments. Financial institutions contain information regarding potentially illicit behaviors, which government agencies fully utilize, treating financial institutions as quasi-law enforcement agents.[281] For example, these financial institutions consistently surveil customers and report information to the government that have high degrees of usefulness in criminal, tax, or regulatory investigations or proceedings.[282] To collect this information, the BSA requires financial institutions to file Suspicious Activity Reports ("SARs") to FinCEN whenever customers engage in cash transactions exceeding $10,000 in the daily aggregate amount.[283]

Similarly, internet intermediaries host information environments rich in blatant, explicit evidence of criminal activities. For instance, in *Does v. Reddit*,[284] the traffickers posted sexually explicit photos of the plaintiffs' children onto Reddit.[285] Additionally, even after Reddit employees initially removed the child pornography, the traffickers continued to repost the content onto other Reddit pages.[286] When the plaintiffs filed their suit, Reddit hosted many pages openly

280. *See* Bittner v. United States, 143 S. Ct. 713, 724 (finding that non-willful violators must pay a penalty).

281. *See* Sater, *supra* note 52, at 398 (emphasizing that every financial institution, as that term is broadly defined in the BSA, has been deputized as a law enforcement agent constantly surveilling its customers and reporting information to the government).

282. *See id.* (same).

283. *See Suspicious Activity Reports*, OFF. OF THE COMPTROLLER OF THE CURRENCY (outlining that the BSA requires financial institutions to submit reports of cash transactions, maintain records of cash purchases, and report suspicious activity that might signal criminal activity) [perma.cc/5H2T-85ZE].

284. 51 F.4th 1137 (9th Cir. 2022).

285. *See id.* at 1139 (detailing how the traffickers posted explicit images of children onto multiple subreddit pages).

286. *See id.* (same).

and explicitly marketing child pornography, allowing users to trade and solicit child porn on these pages.[287] Not only did Reddit benefit in terms of revenue, but more importantly, it contained explicit information regarding child sex trafficking.[288]

Given the illicit activities openly occurring on these sites, these internet platforms host rich information environments that should prove to courts how these intermediaries host and profit from criminal activities. Since the 1970s, the government relied on intermediaries to assist with investigating criminal conduct when Congress enacted the BSA.[289] Given the $150 billion-dollar industry of human trafficking, the most puzzling aspect lays within why courts refuse to treat FOSTA as a method to deputize internet intermediaries.[290] As the original intention of Section 230 worked to preserve free speech online, courts likely gravitate towards broad interpretations of 230 immunity, ultimately adhering to *stare decisis* while garnering narrow interpretations of FOSTA.[291]

Congress originally passed Section 230 with the intent to shield internet intermediaries from liability to encourage free speech online, and this passage occurred alongside the advent of Web 1.0.[292] Almost three decades later, with the arrival of the age of Web 3.0, internet intermediaries continue to expand in size and capabilities, hosting an entire playground for traffickers.[293] Courts should consider

287. *See id.* (emphasizing that Reddit housed multiple subreddit pages which contained explicit images of children).

288. *See id.* (mentioning that the plaintiffs contend that Reddit financially benefits from openly hosting child pornography).

289. *See* Sater, *supra* note 52, at 404 (utilizing financial institutions as law enforcement agents since the BSA's passage).

290. *See* Carmen Niethammer, *Cracking the $150 Billion Business of Human Trafficking*, FORBES (Feb. 2, 2020) (noting the pervasive and lucrative market of human trafficking) [perma.cc/CJR9-MZBZ].

291. *See* Rubin, et al., *supra* note 255 (emphasizing that FOSTA's narrow interpretations result in a win for proponents of unfettered 230 protections).

292. *See generally* Part III.A.

293. *See* The Investopedia Team, *supra* note 22 (describing the reality of Web 3.0).

swinging the pendulum to provide cyber-trafficking victims, such as Sarah and Sonith, with opportunities for justice.

VI. The Federal Trade Commission Should Require Cryptocurrency Exchanges to Engage in Consumer Transparency

Cryptocurrency exchanges should engage in consumer transparency by providing annual, comprehensive reports regarding their efforts toward combatting illicit activities, such as human trafficking, on their platforms. This will foster greater accountability between consumers and cryptocurrency exchanges, as consumers have the most power in the equation of supply and demand.[294] Particularly, in the age of Web 3.0, cryptocurrency exchanges must compete for consumers' attention, which facilitates their revenue.[295] Although Web 3.0 facilitates greater user utility such as allowing consumers to engage in virtual conversations or shop online, it operates on a decentralized structure, which creates legal risks such as cyber-trafficking.[296] Thus, while these legal risks increased with

294. *See* Jason Fernando, *Law of Supply and Demand in Economics: How it Works*, INVESTOPEDIA (Dec. 31, 2023) (noting consumers as a key factor affecting demand because their preferences and willingness to substitute one product for another are among the most important determinants of demand) [perma.cc/FD8X-VLLK].

295. *See* Etienne Mérineau, *The Three Levers of Consumer Power*, FORBES (May 1, 2019) (highlighting the levels of consumer power and pointing out that because of the digital world, which allows for consumers to explore companies at their fingertips, companies must compete for consumers' attention and ensure that they act in response to the interests of consumers) [perma.cc/C352-5XAG]; *see also* The Investopedia Team, *supra* note 22 (discussing the third phase of the evolution of the internet, characterized by decentralization, which has brought with it significant legal and regulatory risks).

296. *See* The Investopedia Team, *supra* note 22 (noting that while Web 3.0 has provided greater user utility, its character includes decentralization, which complicates the use of laws and compliance measures onto it) [perma.cc/W8MU-RDZV]; *see also Online and Technology-facilitated Trafficking in Human Beings*, COUNCIL OF EUR. PORTAL (2024) (utilizing a online analyses to find an increased use of technology for recruiting and controlling victims of trafficking) [perma.cc/H655-4HLZ].

technological advancements, cryptocurrency exchanges' leverage lies in consumers' preferences for ethical practices amongst companies.[297] Requiring annual reports will not only hold cryptocurrency exchanges accountable but also will encourage these exchanges to implement oversight measures to combat cyber-trafficking.

A variety of studies show that consumers prefer engaging with companies exhibiting ethical practices over ones that do not.[298] While each study considers and weighs different factors such as ethical labor practices, ESG initiatives, or sustainability, the consensus suggests that consumers care about buying environmentally and ethically sustainable products.[299] Accordingly, to hold these cryptocurrency exchanges accountable, the Federal Trade Commission ("FTC") should require cryptocurrency exchanges to engage in disclosures by using the Transparency in Supply Chains Act ("the Act") passed by the California State Legislature as a model.[300]

---

297. *See How Much Do Consumers and Companies Care About Ethical Sourcing?*, PROCURIOUS (Jan. 12, 2022) (emphasizing that ethical sourcing is crucial for consumers, citing a recent study regarding consumer intent which found that eighty-eight percent of global consumers surveyed would choose to buy from companies with ethical sourcing structures in place over ones that did not) [perma.cc/DP8R-Y9WK].

298. *See id.* ("The modern shift in consumer buying habits coupled with greater scrutiny of large companies has led to plenty of examples of sourcing policy changes designed to promote a 'greener' image.").

299. See *Consumers Care About Sustainability—and Back It up with Their Wallets*, MCKINSEY & CO. (Feb. 6, 2023) (discussing a joint study from McKinsey and NielsenIQ examining sales growth and its relation to products claiming ESG efforts, ultimately finding that more than 60% of consumers claimed that they would pay more for a product with sustainable packaging and ESG initiatives resulted in an average sales growth of 28%) [perma.cc/T85H-6VC9].

300. *See The California Transparency in Supply Chains Act*, ROB BONTA ATT'Y GEN. (explaining that human trafficking is difficult to uncover, and consumers and businesses inadvertently promote these crimes through purchasing goods tainted in the supply chain, ultimately motivating the Legislature to ensure that large retailers and manufacturers provide consumers with information regarding their efforts to eradicate human trafficking from supply chains) [perma.cc/4J2Y-W3HA].

By enacting the Act, the California State Legislature noticed responded to the fact that businesses and consumers inadvertently facilitated human trafficking through purchasing unethically tainted goods and products in the supply chain.[301] Without publicly available disclosures, consumers lack the information of distinguishing businesses on the merits of their efforts to supply products free from the criminal undertones of human trafficking.[302] Specifically, this Act requires businesses to disclose the extent of their efforts in five areas: verification, audits, certification, internal accountability, and training.[303] A company must disclose to what extent, if any, it engages in verifying product supply chains to evaluate and address risks of human trafficking.[304]

First, the disclosure shall specify whether a third-party conducted the verification.[305] Second, the company shall conduct audits of suppliers to evaluate supplier compliance with company standards for trafficking in supply chains.[306] Third, the company should certify that materials from direct suppliers incorporated into the product must comply with the laws regarding trafficking of the country or countries in which they are doing business.[307] Fourth, the company must maintain internal accountability standards and procedures

301. *See id.* ("The Legislature also found that consumers and businesses are inadvertently promoting and sanctioning these crimes through the purchase of goods and products that have been tainted in the supply chain.").

302. *See id.* (explaining that requiring businesses to partake in disclosures will also allow consumers to make educated decisions about their purchases).

303. *See id.* ("Companies subject to the Transparency in Supply Chains Act must disclose the extent of their efforts in five areas: verification, audits, certification, internal accountability, and training.").

304. *See id.* (emphasizing that businesses must disclose to the public how they verify supply chains to mitigate human trafficking).

305. *See id.* (requiring that the disclosures shall specify if a third party had any involvement).

306. *See id.* (specifying that the disclosure should specify if the verification was not an independent, unannounced audit).

307. *See id.* (ordering direct suppliers to certify that materials were sourced ethically).

for employees or contractors failing to meet company standards regarding slavery and trafficking.[308] Finally, companies must provide employees and management, who have direct responsibility for supply chain management with training on human trafficking and slavery, particularly with respect to mitigating risks within the supply chains of products.[309]

Beyond complying with these provisions, the Act requires companies to post a link disclosing its efforts to eliminate human trafficking from supply chains on its website, unless it does not have a website.[310] Further, the link must appear as conspicuous and easily understood on the company's homepage.[311] For best practices, the state of California suggested that in order to satisfy the conspicuous and easily understood requirements, a company should entitle the link "California Transparency in Supply Chains."[312]

As consumers wield great power in the age of Web 3.0, the FTC should consider implementing parts of California's Act and require cryptocurrency exchanges to create disclosures similar to those required of companies headquartered or doing business in California. Not only will this initiative work towards informing consumers as to which exchanges operate ethically, but market participants can hold cryptocurrency exchanges accountable for illicit activities. Take the Magnuson-Moss Warranty Act[313] as an example. This federal law governs warranties on consumer products, and it essentially requires warrantors to "stand

308. *See id.* (explaining that the company must create internal checkpoints).

309. *See id.* (ensuring that company employees and management must have direct responsibility for the supply chain management).

310. *See* Paul O. Hirose, *The California Transparency in Supply Chains Act: An Overview*, THOMAS REUTERS WESTLAW PRECISION (2025) (discussing the practical implications of the California Transparency in Supply Chains Act and detailing practices that companies must comply with in accordance with the Act) [perma.cc/QP6W-AUMM].

311. *See id.* (requiring the link displayed on the company's homepage, making it obvious and easily accessible to consumers).

312. *See id.* (same).

313. *See generally* 15 U.S.C. § 2302.

behind" their products.[314] Particularly, it proves the integrity of products to consumers throughout sales transactions.[315] Thus, when a consumer purchases an iPhone, the warrantor, or in this case, Apple, agrees to repair or replace the faulty product within a specified time period after its transaction.[316] In turn, consumers can rely on these promises to understand that when they purchase an iPhone, it will not have cracks or scratches.

Therefore, ensuring that cryptocurrency exchanges at least have a consumer transparency report linked to their homepages will act as an "express warranty" to consumers. Requiring these exchanges to comply with a required disclosures will hopefully ensure consumers' trust that the transaction they enter into will not have "cracks" or "scratches," or for the purposes of this Note, connections to human trafficking. Because this disclosure initiative will require cryptocurrency exchanges to engage with analyzing their blockchains while creating employee trainings to further educate regarding the importance of ethical supply chains to track human trafficking, it will hopefully contribute to dampening the cyber-trafficking problem.

Despite the great importance of dampening the phenomena of trafficking facilitated by cryptocurrencies, another critical component of this solution includes a gradual transition period which could potentially ensure a seamless execution by cryptocurrency exchanges. Moreover, a common critique voiced by impacted corporations of the Transparency in Supply Chains Act included a lack of timely guidance necessary to ensure that corporations satisfied all of the legal

314. *See Businessperson's Guide to Federal Warranty Law*, FED. TRADE COMM'N (describing how a warranty works) [perma.cc/A4JD-K6XW].

315. *See* Daniel Liberto, *Express Warranty: Meaning, Overview, and Examples,* INVESTOPEDIA (Sept. 13, 2023) (providing consumers with express warranties allows consumers to know that the item purchased will live up to the promises of the seller) [https://perma.cc/5XTL-TL4J].

316. *See Apple One (1) Year Limited Warranty*, APPLE LEGAL (Mar. 1, 2023) (summarizing how Apple's limited warranty operates) [perma.cc/WV9U-REDN].

expectations.[317] Many companies felt that rather than focusing on actually providing useful content in their disclosures and ensuring streamlined education initiatives to internal employees, companies devoted time and resources to interpreting the language of the Act.[318] As a response to this frustration, the California Department of Justice created a resource guide to detail exact requirements and recommend how companies should move forward to comply with the Act.[319]

In turn, the FTC should consider using this resource guide to draft its policies regarding required disclosures and annual reporting of cryptocurrency exchanges. Lastly, cryptocurrency exchanges should have a transition period to create adequate disclosures while ensuring a direct link to these disclosures on their platforms. Further, the length of this transition period should depend on the annual revenue generated by a cryptocurrency exchange. For example, a cryptocurrency exchange such as Bitcoin, which generates a daily revenue of over $40 million should receive a shorter transition period than smaller cryptocurrency exchanges.[320]

In conclusion, the FTC should encourage cryptocurrencies to engage in consumer transparency while educating their employees on human trafficking prevention to dampen cyber-trafficking occurring on their platforms. By addressing the comprehensive approach of the Act alongside recommendations made by affected corporations and considering the utility of a transition period, this will act as

317. *See* KNOWTHECHAIN, INSIGHTS BRIEF: FIVE YEARS OF THE CALIFORNIA TRANSPARENCY IN SUPPLY CHAINS ACT 6–7 (2015) (outlining a survey conducted on 500 affected companies by the Act and critiques that the companies had in terms of the implementation of the Act).

318. *See id.* at 7 ("Rather than focus on the substance of their statements, corporations have devoted time and resources to forming their own interpretations of the law.").

319. *See* KAMALA D. HARRIS, THE CALIFORNIA TRANSPARENCY IN SUPPLY CHAINS ACT: A RESOURCE GUIDE 7 (2015) (explaining that this resource guide will help covered companies by offering recommendations about model disclosures and best practices for developing such disclosures).

320. *See generally Bitcoin Miners Revenue Per Day*, YCHARTS (Feb. 20, 2024) [perma.cc/8C6Y-4KBF].

a step towards preventing traffickers from perpetuating cryptocurrency as the bedrock of cyber-trafficking.

VII. Congress Should Consider Passing the Digital Asset Anti-Money Laundering Act

Given the billion dollar industry of sex trafficking which occurs on cryptocurrency exchanges related to the failure of KYC measures, cryptocurrencies must work to improve KYC compliance.[321] As the law stands, FinCEN treats cryptocurrencies as Money Service Businesses ("MSBs"), requiring cryptocurrencies to implement KYC measures.[322] However, regardless of the tragic cases such as WTV[323] and DarkScandals,[324] a gap remains within the difference in government regulation of banks and cryptocurrencies. Congress has failed to address this gap as it continually neglects to enact legislation to impose stricter regulatory schemes upon cryptocurrencies in the age of Web 3.0. Ultimately, Congress must swing their pendulum to apply KYC in the context of a modern day MSB: cryptocurrency.

FinCEN released an advisory outlining the danger of unregistered foreign-located MSBs, especially because they rarely comply with U.S. registration and KYC policies, even though they do business in the U.S.[325] Therefore, criminals can take advantage of these cryptocurrency exchanges due to the KYC vulnerabilities.[326] Clearly, Congress should employ stricter measures to hold cryptocurrencies accountable, such

321. *See* Niethammer, *supra* note 290 (emphasizing that the revenue generated by cryptocurrency within human trafficking totals to $150 billion).

322. *See* Dewey & Patel, *supra* note 141 (detailing that FinCEN issued guidance in 2013 stating that they will virtual currency exchanges as Money Service Businesses).

323. *See* Cunningham, *supra* note 157 (outlining the abhorrent case of WTV).

324. See *id.* (detailing the abhorrent case of DarkScandals).

325. *See generally* U.S. TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-2019-A003, ADVISORY ON ILLICIT ACTIVITY INVOLVING CONVERTIBLE VIRTUAL CURRENCY (2019).

326. *See id.* at 6, 8 (warning about illicit activities arising from virtual currencies as they avoid engaging in KYC requirements).

as more robust KYC process in the customer onboarding process.

Congress needs to enact legislation which would deter criminals from cryptocurrencies while mitigating illicit activities. Therefore, Congress should consider enacting the Digital Asset Anti-Money Laundering Act to bolster AML policies upon cryptocurrencies.[327] This bill would require any administrator maintaining a public blockchain infrastructure to register as a financial institution.[328] Therefore, cryptocurrencies must identify and record personal information of each individual using their software or sending transactions over the internet while developing calibrated AML programs to validate, secure, or facilitate digital asset transactions.[329]

Moreover, this bill would require banks and MSBs to verify customer and counterparty identities, keep records, and file reports on certain transactions involving unhosted wallets or wallets hosted in non-BSA compliant jurisdictions.[330] Beyond these measures, BSA rules would extend regarding the reporting of foreign bank accounts to include digital assets. Therefore, this would require U.S. individuals engaged with transactions greater than $10,000 in digital assets through one or more offshore accounts to file a Report of Foreign Bank and Financial Accounts with the Internal Revenue Service.[331]

A foreseeable wrinkle arising out of this bill is the potential confusion amongst cryptocurrency exchanges and

---

327. *See generally* Digital Asset Anti-Money Laundering Act, S.2669, 118th Cong. (2023).

328. *See* Senators Elizabeth Warren & Roger Marshall, THE DIGITAL ASSET ANTI-MONEY LAUNDERING ACT OF 2023 1 (2023) (discussing how cryptocurrencies should register as a financial institution due to high volume of illicit transactions carried out with cryptocurrencies).

329. *See id.* (extending the Bank Secrecy Act responsibilities, like KYC checks, to digital asset providers to ensure validation and security involving digital asset transactions).

330. *See id.* (requiring banks to verify unhosted wallets).

331. *See id.* (requiring U.S. individuals engaged in virtual currency transactions greater than $10,000 in the aggregate to file reports to government agencies).

administrators.[332] However, FinCEN must impose these regulations on to cryptocurrency exchanges to combat criminals' high abuse of cryptocurrency's weak KYC policies. FinCEN could combat this growing pain by considering a phase-out program to allow current exchanges a transition period from their current operational structure to a model which abides by stricter KYC regulations. First, FinCEN should consider a tier system to organize cryptocurrencies into different categories of the phase-out program.[333] For instance, FinCEN should require cryptocurrencies that generate more revenue to convert their current KYC policies and implement the aforementioned suggestions within a year. In contrast, smaller cryptocurrencies which have not generated as much revenue could have more time to convert model to comply with stricter KYC policies, about five years.

Ideally, this phase-out program will remove the burden from cryptocurrency exchanges of smaller sizes to choose between spending copious company resources complying with an entirely new KYC policies and keeping their companies afloat.[334] One last consideration includes encouraging collaboration between FinCEN and cryptocurrencies exchanges.[335] Not only would this collaboration foster innovation within cryptocurrencies towards stronger KYC policies, but it will likely prevent illicit activities such as trafficking. Considering that Congress

---

332. *See* Kindred, *supra* note 55, at 31 (requiring all exchanges and administrators to comply with entirely new regulations will lead to confusion, resulting in cryptocurrency exchanges to decide between keeping their companies afloat and complying with anti-money laundering laws).

333. *See id.* (acknowledging the critical importance of anti-money laundering regulations but mentioning that an improvement is to create a tiered system of regulation for cryptocurrency exchanges to help with the transition towards stricter regulations).

334. *See id.* (mentioning that removing the burden of implementing robust anti-money laundering policies quickly after enactment could disrupt cryptocurrencies' businesses).

335. *See* Warren & Marshall, *supra* note 328 (directing FinCEN to issue guidance to financial institutions on mitigating the risks of transacting with digital assets that have been anonymized using digital asset mixers and other decentralized technologies).

initially created KYC measures to ensure legality within traditional banks, encouraging robust communication between FinCEN and cryptocurrency exchanges will result in better rapport and issuance of the policies, at large.

VIII. The Department of State Should Consider Block Chain Technology as a Long-Term Solution Towards Government-issued Identification

Although block chain maintains cryptocurrency, it possesses a negative public perception.[336] While the public eye focuses on block chain's negative aspects, the discourse may arise from an unsound basis due to the fact that criminals have made cryptocurrency into a prominent form of currency in illicit markets, creating negative associations with the institution of block chain.[337] Over the last few years, numerous U.S. states implemented block chain technology onto various components of infrastructure due to its efficiency and reliability.[338] For example, in 2016, the state of Illinois started an initiative for a "Smart State" vision to heavily incorporate block chain technology.[339] Beyond Illinois's initiative, numerous U.S. companies utilize block chain to combat unethical labor practices, such as trafficking,

336. *See* Rose Jacobs, *The Good and Bad of Blockchain*, CHICAGO BOOTH REV. (Feb. 12, 2018) (discussing that blockchain technology itself will likely endure, but cryptocurrency dramas have resulted in its gaining a bad reputation) [perma.cc/3KVY-EXLC].

337. *See id.* (emphasizing the public's negative perception of virtual currencies).

338. *See* Kevin C. Desouza, et al., *Blockchain and U.S. State Governments: An Initial Assessment*, BROOKINGS (Apr. 17, 2018) (emphasizing that blockchain has versatility, beyond just mining cryptocurrencies) [perma.cc/XJV8-GERT]; *see also* Ben Schreckinger, *The Smallest State Has the Biggest Blockchain Ambitions*, POLITICO (Feb. 9, 2023) (explaining that many states recognize the utility of blockchain technology beyond cryptocurrency, and explaining that New York, Illinois, Vermont, and now Rhode Island have implemented certain aspects of infrastructure on blockchains) [perma.cc/HD2W-GY3K].

339. *See State of Illinois Releases Blockchain Task Force Report*, ILLINOIS.GOV (Jan. 31, 2018) (illuminating different aspects of the state's blockchain initiative, particularly asserting that utilizing blockchain will help spur the state's economy) [perma.cc/68Z7-Y6NQ].

through supply chain analyses.[340] Outside of the U.S., in Estonia, every citizen has a state-issued digital identity maintained on a block chain, which constitutes a national ledger of citizens' identities.[341] These varied methods of block chain implementation throughout industries and territories represent crucial examples of how block chain technology could guide the U.S. towards implementing a long-term solution to combat human trafficking. Therefore, the Department of State should consider implementing a pilot program within the next few years and eventually scale it upwards to implement U.S. passports onto a block chain by 2050 at the earliest.

Estonia started testing their digital identity program in 2008, well before the popularized discussion of block chain.[342] This project, "E-Estonia," began when the Estonian government wanted to digitize all citizens' activities concerning the government.[343] As of 2019, Estonians may access ninety-nine percent of their public services as e-services.[344] Moreover, Estonia's model reportedly saved over 1,400 years of working time and two percent of GDP annually.[345] A prominent feature of Estonia's digital society

340. *See* Mark White, et al., *Blockchain basics for government*, DELOITTE INSIGHTS, 2017 (providing an overview of blockchain, but emphasizing that Estonia has been a leader in implementing it for identity management purposes) [perma.cc/R857-QT7R].

341. *See* MARTINSON & PRIIT, ESTONIA: THE DIGITAL REPUBLIC SECURED BY BLOCKCHAIN 3 (2019) (describing how Estonia has fully implemented blockchain technology into its public sector, through issuing health insurance cards and identification cards with blockchain models, ultimately making it the most advanced digital society in the world).

342. *See* E-ESTONIA, ESTONIAN BLOCKCHAIN TECHNOLOGY 1 (2023) ("Although blockchain has only become hot topic in recent years, Estonia started testing the technology already in 2008–even before the Bitcoin white-paper that first coined the term 'blockchain,' was published.").

343. *See* Silvia Semenzin, et. al, *Blockchain-based Application at a Governmental Level: Disruption or Illusion? The Case of Estonia*, 41 POLICY & SOCIETY 386, 389 (2022) (praising blockchain due to its utility as shown by Estonia).

344. *See* Martinson, *supra* note 341 at 3 ("As of today, 99% of public services are available to citizens as e-services.").

345. *See id.* ("Officials report that Estonia saves over 1400 years of working time and 2% of GDP annually through its digitized public services.").

includes having a digital identity ("ID").[346] Accordingly, the benefits of having a digital ID include having a national health insurance card, having proof of identification when logging into bank accounts, checking medical records, and using it for digital signatures.[347] However, these innovative components of Estonia's infrastructure receive wide varieties of criticism.[348]

The bulk of criticism targets the stability and security of the digital ID.[349] For instance, many critics focus on the cyberattacks on Estonia in 2017.[350] In September of 2017, hackers targeted digital IDs to steal Estonian's identities and access their bank information.[351] Given Estonia's decades of experience in digital ID and digital infrastructures, by early November the government provided citizens with a software update that would fix the security issue.[352] Despite this crisis, Estonians' trust in their nation's digital ID remained strong, as ninety-four percent of citizens renewed their digital IDs the year following the cyberattack.[353]

Digital ID supplies optimal accessibility, as Estonians may vote, access medical records, and access their bank

346. *See id.* at 4 ("Estonia has the most highly-developed national ID card system in the world.").

347. *See id.* (emphasizing that Estonia's system represents a multi-faceted development).

348. *See generally infra* notes 350–353 and accompanying discussion.

349. *See id.*

350. *See* Kalev Aasmae, *Estonia's ID Card Crisis: How E-state's Poster Child Got into and out of Trouble*, ZDNET (Nov. 13, 2017) ("Estonia is built on secure state e-systems, so the world was watching when it hit a huge ID-card problem.") [perma.cc/9AFZ-6M8S].

351. *See id.* (explaining that the e-card gives owners access to bank transactions).

352. *See id.* (emphasizing that the Estonian government immediately investigated the issue and planned on providing a software update to citizens by November).

353. *See What We Learned from the eID Card Security Risk?*, E-ESTONIA May 14, 2018 ("After the suspension of the certificates of the cards with vulnerable chips on November 3, 2017, 94% of the eID cards which are electronically used have been renewed.") [perma.cc/ZT2K-FKNA].

accounts with it.[354] More importantly, digital ID can deter traffickers from robbing innocent individuals, like Sonith or Sarah, of their livelihood and forcing them into a cruel state of limbo. Traffickers often take identifying documents to control their victims' movement while obfuscating their identities.[355] However, with block chain technology as a basis for identity verification, victims can seize their autonomy and verify their identities without the need of a physical ID.[356]

As Estonia has implemented a robust digital ID system, other compelling proposals have asserted the importance of digital ID in human trafficking prevention. In 2018, the World Identity Network ("WIN") engaged in discourse of trafficking prevention in the age of Web 3.0.[357] In the report, WIN emphasized that the key point of victims' vulnerability stems from traffickers stealing their legal identity.[358] Oftentimes, victims lack legal identification, and possession of a functional ID has revealed itself as a key tool in shielding

354. *See* Martinson, *supra* note 341 at 4 (emphasizing that the national eID card allows interdisciplinary use).

355. *See Blockchain Based Solutions to Combat Modern Slavery*, MOODY'S ANALYTICS (Nov. 29, 2022) (emphasizing that traffickers target vulnerable individuals because they know that taking identifying documents will control their victims' movement capabilities while obfuscating their identities, and blockchain identification verification will aid in trafficking prevention) [perma.cc/4XXG-X4PV].

356. *See id.* (same).

357. *See* WORLD IDENTITY NETWORK, BLOCKCHAIN FOR HUMANITY GLOBAL CHALLENGE 5 (2018) (emphasizing that more than a billion people around the world lack the basic human right of personhood, making these individuals targets for traffickers).

358. *See id.* at 8.

> Undocumented children are easy prey for human traffickers, who often use fake identification documents to transport them across borders. Once trafficked, these children and minors are sold to sex brothels, caught in modern slavery rings, and even used for the illegal human organ trade. Lack of identification makes children "invisible" to local authorities and non-governmental organizations willing to help.

potential trafficking victims from preying traffickers.[359] The report asserted that broadening the use of block chain technology to reinforce legal identification systems must take place in order to provide victims an avenue to escape the limbo created by their traffickers.[360] The dire need for digital ID systems to save victims constitutes a large part of the discussion regarding human trafficking prevention. Additionally, Estonia contains about 1.3 million people, while the U.S. contains over 300 million people.[361] Nevertheless, the benefits of a long-term digital ID initiative outweigh these few costs of its implementation.

The Department of Homeland Security must focus on the fact that this digital ID initiative acts as a long-term solution, which could take decades to perfect. In the meantime, the federal government should collaborate with the state of Illinois to better understand its pilot programs for its blockchain initiative as a starting point. In tandem, U.S. government officials should begin communicating with Estonia's government officials to learn more about how the digital ID processes have been implemented. As this project would require copious time and energy from all parties involved, U.S. government employees involved should receive salaries comparable to those working within the private sector in blockchain technology. This would incentivize all parties involved and ensure the success of a digital ID initiative in the future.

Clearly, this solution will likely take decades, as it constitutes a great leap from the U.S.'s current method of identification. Nevertheless, traffickers' greatest tool in trapping victims in a cruel state of limbo involves snatching their government-issued identification, taking away their

359. *See id.* at 18 (specifying that a functional ID acts as a key tool to protect undocumented individuals and improving their autonomy, ultimately acting as a powerful tool to protect themselves from traffickers).

360. *See id.* at 9 (broadening the use of blockchain to identifying and protecting potential victims of trafficking will aid in turning "invisible" individuals into "invincible" ones).

361. *Estonia Population*, WORLDOMETER (2024) [perma.cc/4HW8-6WF7].

possibility of escape.[362] Accordingly, these horrendous crimes cannot outweigh the importance of at least investigating the potential utility in block chain technology towards strengthening verification processes regarding identification documents. To prevent victims like Sonith and Sarah from suffering in limbo, initiating research towards implementing block chain technology onto government-issued identification will act as a prime, but long-term, solution.

IX. Conclusion

The aforementioned solutions represent starting points towards combatting cyber-trafficking and preventing the victimization of innocent individuals, such as Sarah and Sonith. As Web 3.0 continues to develop, traffickers will continue to take advantage of its tools to ensnare individuals into a cruel state of limbo. In tandem, as FOSTA continuously garners narrow interpretations, victims of trafficking will cease to seek justice, while internet intermediaries continue hosting rampant playgrounds for traffickers. Together, cryptocurrency and FOSTA represent the pillars of cyber-trafficking in the age of Web 3.0. Governmental bodies and courts must swing their ideological pendulums to remedy FOSTA's setbacks, while discouraging traffickers' use of Web 3.0's tools.

362. *See supra* note 355 and accompanying text (noting traffickers' use of this strategy to control their victims).