Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 32 *XXXII*
Number 3

Article 1

2022

Speak Out: Verifying and Unmasking Cryptocurrency User Identity

Hadar Y. Jabotinsky

Michal Lavi

Speak Out: Verifying and Unmasking Cryptocurrency User Identity

Cover Page Footnote

* Ph.D. (Law & Economics) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology. **Ph.D. (Law) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology. The Authors thank Roee Sarel, Sarah Scharf, Israel Klein, Emily Cooper, the participants of "New Payment Products and Services, Anti-Money Laundering and Counter Terrorist Financing Risks" workshop (Macquarie University, Sydney Australia (Zoom)) (July 2020), and the participants the U.S. National Business Law Conference (University of Tennessee, U.S.; June 2021). Special thanks are due to Daniel Levin, Laura Rann, Caroline Vermillion, and their colleagues on the Fordham Intellectual Property, Media & Entertainment Law Journal for helpful comments, suggestions, and outstanding editorial work. Finally, we thank Heth Academic Center for Research of Competition and Regulation (College of Management) for granting financial support for this research. This Article is dedicated to the memory of Michal's mother, Aviva Lavi, who died suddenly and unexpectedly. She will always be loved, remembered, and dearly missed.

Speak Out: Verifying and Unmasking Cryptocurrency User Identity

Hadar Y. Jabotinsky[*] & Michal Lavi[**]

Terror attacks pose a serious threat to public safety and national security. New technologies assist these attacks, magnify them, and render them deadlier. The more funding terrorist organizations manage to raise, the greater their capacity to recruit members, organize, and commit terror attacks. Since the September 11, 2001 terror attacks, law enforcement agencies have increased their efforts to develop more anti-terrorism and anti-money laundering regulations, which are designed to block the flow of financing of terrorism and cut off its oxygen. However, at present, most regulatory measures focus on traditional currencies. As these restrictions become more successful, the likelihood that cryptocurrencies will be used as an alternative to fund illicit behaviors grows. Furthermore, the COVID-19 virus and subsequent social distancing guidelines have increased the use of cryptocurrencies for money laundering, material support to terror, and other financial crimes.

---

[*] Ph.D. (Law & Economics) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology.

[**] Ph.D. (Law) Research Fellow at the Hadar Jabotinsky Center for Interdisciplinary Research of Financial Markets, Crises and Technology.

The Authors thank Roee Sarel, Sarah Scharf, Israel Klein, Emily Cooper, the participants of "New Payment Products and Services, Anti-Money Laundering and Counter Terrorist Financing Risks" workshop (Macquarie University, Sydney Australia (Zoom)) (July 2020), and the participants the U.S. National Business Law Conference (University of Tennessee, U.S.; June 2021). Special thanks are due to Daniel Levin, Laura Rann, Caroline Vermillion, and their colleagues on the Fordham Intellectual Property, Media & Entertainment Law Journal for helpful comments, suggestions, and outstanding editorial work. Finally, we thank Heth Academic Center for Research of Competition and Regulation (College of Management) for granting financial support for this research.

This Article is dedicated to the memory of Michal's mother, Aviva Lavi, who died suddenly and unexpectedly. She will always be loved, remembered, and dearly missed.

Cryptocurrencies—electronically generated and stored tokens which can be exchanged via a decentralized payment system—are a game-changer, significantly affecting market functions like never before and making it easier to finance terrorism and other types of criminal activity. These decentralized and (usually) anonymous currencies facilitate a high volume of transactions, allowing terrorists to engage in extensive fundraising, management, transfer, and spending for illegal activities. As cryptocurrencies gain popularity, the issue of regulating them becomes more urgent. This Article proposes to reform cryptocurrency regulation. It advocates for mandatory obligations directed at cryptocurrency issuers, wallet providers, and exchanges to verify the identity of users on the blockchain. Thus, courts could grant warrants obligating cryptocurrency-issuing companies to unmask the identity of cryptocurrency users when there is probable cause that their activities support terrorism or other money laundering schemes. Such reforms would stifle terrorism and other types of criminal activity financed through cryptocurrencies, curbing harmful activities and promoting national security. In recognition of the legal challenges this solution poses, this Article also addresses substantial objections that might be raised regarding the proposed reforms, such as innovation concerns, First Amendment arguments, and Fourth Amendment protections. It concludes by addressing measures to efficiently promote application of the proposed reforms.

INTRODUCTION

"U.S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups."[1]

Recently, the U.S. government seized roughly $2 million in Bitcoin and other types of cryptocurrencies from accounts that sent or received funds in alleged financing schemes for foreign terrorist organizations such as Al Qaeda and the Islamic State of Iraq and Syria ("ISIS").[2] These tokens were fundraised on social media.[3] The affiliated terrorist organizations believed that using cryptocurrencies promised complete anonymity.[4] However, the government has developed tools that can override websites used to solicit terrorist funds and compel information about the accounts involved.[5] Yet, the investigation of donor identities continues.[6] These efforts constituted "the first significant civil forfeiture actions to seize cryptocurrency as part of counterterrorism financing investigations."[7]

On August 28, 2015, "Ali Shukri Amin was sentenced to [eleven] years in prison to be followed by a lifetime of supervised

---

1 Charlie Savage, *U.S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups*, N.Y. TIMES (Aug. 13, 2020), nyti.ms/3aPiDAL [https://perma.cc/M855-6247].

2 *See id.*

3 *See id.* For more information on fundraising campaigns for supporting terrorism, see Andrew Mines & Devorah Margolin, *Cryptocurrency and the Dismantling of Terrorism Financing Campaigns*, LAWFARE (Aug. 26, 2020, 9:02 AM), https://www.lawfareblog.com/cryptocurrency-and-dismantling-terrorism-financing-campaigns [https://perma.cc/7FKF-W3PR].

4 *See* Savage, *supra* note 1.

5 *See id.*

6 *See id.*

7 *Id.*

release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL," commonly known as ISIS.[8] On June 11, 2015, Amin pled guilty.[9] He confessed "to using Twitter to provide advice and encouragement to [ISIS] and its supporters . . . ."[10] Using the Twitter handle @Amreekiwitness, Amin, "provided instructions on how to use Bitcoin, a virtual currency, to mask the provision of funds to [ISIS], as well as facilitation to [ISIS] supporters seeking to travel to Syria to fight with [ISIS]."[11] Amin used this account to conduct Twitter-based conversations regarding ways to develop financial support for ISIS using cryptocurrencies—electronically-generated and stored currencies that enable users to trade objects with one another—and establish a secure funding system for ISIS.[12] For instance, "Amin tweeted a link to an article he had written entitled 'Bitcoin wa' Sadaqat al-Jihad' (Bitcoin and the Charity of Jihad),"[13] which discussed "how to use bitcoins and how jihadists could utilize this currency to fund their efforts," including statements about setting up anonymous donation systems to send Bitcoin money to the mujahedeen.[14]

In January 2015, *Haaretz*, a daily Israeli news outlet, reported on the first instance of an ISIS fundraising for its terror cell using Bitcoin on the dark net.[15] The fundraiser was run by a man identified as Abu-Mustafa, whose Bitcoin account number indicated he raised

---

8 *See* FIN. ACTION TASK FORCE, EMERGING TERRORIST FINANCING RISKS 36 (2015), www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf [https://perma.cc/3ML8-9J9X] [hereinafter FATF REPORT].

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 *Id.*

15 Danna Harman, *U.S.-Based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*, HAARETZ, http://www.haaretz.com/middle-east-news/.premium-1.639542 [https://perma.cc/S3QZ-4ZJ5] (Apr. 10, 2018). The "dark net" is also referred to as the dark web. It is an encrypted network of websites connected to one another. The dark net is part of the greater deep web. The deep web includes all unindexed websites that don't pop up when you do an internet search. *See generally* Gabriel Weimann, *Going Darker? The Challenge of Dark Net Terrorism*, WILSON CTR. (2018), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf [https://perma.cc/LT6H-JVA9].

five Bitcoins (approximately $1,000 USD) before the FBI shut down his account.[16]

The currency used in the abovementioned transactions was Bitcoin—the first and perhaps most well-known cryptocurrency.[17] Cryptocurrencies are electronically generated and stored tokens that individuals can exchange via a decentralized payment system called a blockchain.[18] The blockchain is a peer-to-peer network, which allows users to trade the tokens without relying on banks or other financial institutions, thus cutting out the financial intermediaries and eliminating their fees.[19] Though Bitcoin is the first cryptocurrency,[20] there are new cryptocurrencies tailored for different audiences.[21] Scholars dub this disruptive technology as a "trust machine,"[22] because it eliminates reliance on traditional institutional intermediaries

---

16 *See* Harman, *supra* note 15. For expansion and more examples of the use of cryptocurrencies for terrorism, see Zachary K. Goldman et al., *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, CTR. FOR A NEW AM. SEC. 12–13 (May 2017), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819&focal=none [https://perma.cc/5BJN-55VA].

17 CYNTHIA DION-SCHWARZ ET AL., TERRORISTS USE OF CRYPTOCURRENCIES: TECHNICAL AND ORGANIZATIONAL BARRIERS AND FUTURE THREATS 48 (RAND CORP. 2019) ("Currently, despite an increase in their use, altcoins are not a large part of the total cryptocurrency market, which is still almost completely dominated by Bitcoin."). It should be noted that Bitcoin is not the only cryptocurrency. There are over 5,000 cryptocurrencies in the world right now and this number is rapidly growing. *See* Stephen Wilks, *The Reimagined Schoolyard: Cryptocurrency's Adoption in Tomorrow's International Monetary Order*, 2020 B.C. INTELL. PROP. & TECH. F. 1, 34 (2020) ("More than 5,000 cryptocurrencies exist today, with Bitcoin being the most common, dominating more than sixty percent of the virtual currency market with more than 18 million units valued around $9,000 (U.S.) per coin.").

18 *See* D. Towne Morton, *The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy*, 16 LOY. U. CHI. INT'L L. REV. 129, 130 (2020); Henry S. Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 N.C. L. REV. 395, 402 (2019).

19 *See* Primavera De Filippi, *Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream*, HAL, https://hal.archives-ouvertes.fr/hal-02445179/document [https://perma.cc/2VGA-MHUQ].

20 *See* DION-SCHWARZ ET AL., *supra* note 17, at 57 ("Bitcoin, which was launched by the pseudonymous Satoshi Nakamoto in early 2009, is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system.").

21 *Id.* at 2 (discussing other cryptocurrencies, such as Omni Layer (MasterCoin), BlackCoin, Zcash, Ether, Libra and many more).

22 *The Trust Machine*, ECONOMIST (Oct. 31, 2015), https://www.economist.com/leaders/2015/10/31/the-trust-machine [https://perma.cc/YSE8-Y2RA].

in financial markets and operates within an ecosystem based on self-sovereign identities.[23] As such, cryptocurrencies have potential to revolutionize many sectors of our day-to-day lives.[24] Some believe this revolution could change perceptions of property, expression, and identity.[25]

As coronavirus ("COVID–19") erupted, the use of cryptocurrencies increased.[26] One plausible explanation is the public's growing distrust in institutions and traditional financial intermediaries, increasing demand for alternatives.[27] The decentralized and anonymous cryptocurrency model is a natural candidate, as cryptocurrencies store value and remain borderless.[28] They can be purchased from almost anywhere in the world and subsequently used in most countries without a need for exchange or transfer.[29] From the consumers' perspective, cryptocurrencies are beneficial to circumventing intermediaries, thereby making financial services cheaper and

---

[23] *See* De Filippi, *supra* note 19.

[24] *See generally* Don Tapscott & Alex Tapscott, *How the Tech Behind Bitcoin Will Change Your Life*, TIME (May 6, 2016, 10:22 AM), time.com/4320254/blockchain-tech-behind-bitcoin/ [https://perma.cc/5NV4-953Q].

[25] Timothy C. May, *The Crypto Anarchist Manifesto*, groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html [https://perma.cc/8BBP-NU6A].

[26] *See generally* Hadar Jabotinsky & Roee Sarel, *How Crisis Affects Crypto: Coronavirus as a Test Case* (Mar. 23, 2020) (unpublished manuscript) (on file with authors), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557929 [https://perma.cc/8XAA-VEX9].

[27] *See generally* Jannik Lockl & Jens-Christian Stoetzer, *Trust-Free Banking Missed the Point—the Effect of Distrust in Banks on the Adoption of Decentralized Finance*, EUR. CONF. ON INFO. SYS. (2021), https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1153/wi-1153.pdf [https://perma.cc/A9CM-U6E8]; Dondi Black, *Digital Currencies Skyrocket During Pandemic*, FIS (Jan. 11, 2021), https://www.fisglobal.com/en/insights/what-we-think/2021/january/digital-currencies-skyrocket-during-pandemic [https://perma.cc/J4L2-N6HN].

[28] Tom Sadon, *Why Criminals Use Cryptocurrency*, COGNYTE (Nov. 2, 2021), https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/ [https://perma.cc/E4DP-9RQE] ("Cryptocurrencies can be transferred quickly and easily from one crypto address to another, whether they serve the same person or totally different parties, locals or foreigners, acquaintances, or strangers. They are easily transferred globally, thus enabling international trading, which, in the criminal setting, translates to trafficking.").

[29] *See The Opportunity of Cryptocurrencies for Cross-Border Trade and Marketplaces*, PENTAGON (Nov. 24, 2021), https://wearepentagon.com/2021/11/24/cryptocurrency-to-enable-cross-border-trade/ [https://perma.cc/SW9P-SJZT].

more inclusive.[30] In the case of cryptocurrencies, consumers place trust in technology, rather than in people, institutions, or intermediaries, which improves markets and businesses.

Yet, there is a downside: with great innovation comes social costs. These governance models are especially vulnerable to harmful behaviors due to coin owners' anonymity.[31] They can be abused by illicit actors, such as organized crime syndicates for plotting money laundering schemes,[32] expanding cross-border activities, facilitating and conducting cyberattacks, and demanding ransom, among other acts.[33] Cryptocurrencies can even be exploited for crowd-funding campaigns and aid terrorists in soliciting funding.[34]

Social distancing guidelines that followed the COVID-19 virus outbreak have included mandatory quarantines, air travel limitations, and boarder closings around the world.[35] As a result, cryptocurrencies are increasingly used for illicit activities such as money laundering, material support for acts of terror, and other financial crimes.[36] Much of this increase is caused by the general population

---

30 Daivi Rodima-Taylor & William W. Grimes, *Cryptocurrencies and Digital Payment Rails in Networked Global Governance: Perspectives on Inclusion and Innovation*, *in* BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 109, 110 (Malcolm Campbell-Verduyn ed., 2018) ("Cryptocurrencies can therefore contribute towards more efficient remittance systems and enhance financial inclusion, particularly in economies with inefficient payment systems and underdeveloped infrastructures of traditional finance.")

31 *See id.* at 121.

32 *See, e.g.*, Alex Vet, *Italian Mafia Launders Money Through Crypto*, COINATORY (Apr. 6, 2019), bit.ly/2G0u1P8 [https://perma.cc/ZJ62-JV84].

33 *See* Brian Monroe, *In Pandemic Fraud, Cyber Fusillades, More Criminals Choosing Crypto to Buy Virtual Weapons, Get Paid After Successful Attacks: FinCEN*, CERTIFIED FIN. CRIME SPECIALISTS (May 15, 2020), https://www.acfcs.org/in-pandemic-fraud-cyber-fusillades-more-criminals-choosing-crypto-to-buy-virtual-weapons-get-paid-after-successful-attacks-fincen/ [https://perma.cc/6XS4-PK6H].

34 *See* Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, BELLINGCAT (Aug. 9, 2019), www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/ [https://perma.cc/H57H-XYYN]. This is also the reason behind Canada's Emergency Act which was invoked recently to target crowdfunding platforms and the cryptopayment systems linked to them. *See* Sebastian Sinclair, *Crypto Payments Firms Face New Restrictions Under Canada's Blockade Crackdown*, BLOCKWORKS (Feb. 14, 2022, 8:05 PM), https://blockworks.co/crypto-payments-firms-face-new-restrictions-under-canadas-blockade-crackdown/ [https://perma.cc/TVD7-WZSH].

35 *See* Jabotinsky & Sarel, *supra* note 16, at 3.

36 *See* Monroe, *supra* note 33.

using cash less frequently, making it more difficult to launder money through cash.[37] Further, users' anonymity on the blockchain makes it more difficult for law enforcement agencies to identify and track illegal transactions.[38]

As various regulatory measures are imposed on traditional financial systems to combat terrorism, terrorists' use of cryptocurrencies is likely to increase, affecting how terrorism and related activities are financed.[39] For example, "in the past several years, terrorist groups in Gaza solicited support in Bitcoin," much like ISIS.[40] Cryptocurrencies allow terrorists to fund attacks more easily than fiat currencies,[41] enabling more frequent and extensive attacks.[42] For example:

> [If supporters] are not donating as much to terrorist groups as they did in the past because of an increase in the legal and financial risks involved in doing so, it is plausible that a sufficiently robust, secure, and anonymous cryptocurrency could re-enable donations as a significant source of terrorism financing.[43]

---

[37] For more information on how COVID-19 influences financial crimes, see generally FIN. ACTION TASK FORCE, COVID-19-RELATED MONEY LAUNDERING AND TERRORIST FINANCING: RISKS AND POLICY RESPONSES (2020), bit.ly/2M3MXzm [https://perma.cc/YEJ4-T6EK]. On the abuse of cryptocurrency for buying weapons and supporting crime, see Monroe, *supra* note 33. *See also* U.N. OFF. ON DRUGS & CRIME (UNODC), MONEY LAUNDERING AND COVID19: PROFIT AND LOSS (2020), bit.ly/3rlxmLz [https://perma.cc/QV8R-ZPDQ] ("Traditional cash-courier money laundering has been significantly reduced through ports and airports. It is unclear if Organized Criminals will seek alternative remittance methods for their criminal finances, such as cryptocurrencies or wire transfers, or await the reopening of borders.").

[38] *See* DION-SCHWARZ ET AL., *supra* note 17, at x.

[39] *See id.* at 29 (explaining that cryptocurrencies are likely to increase in acceptance, yet right now there are not enough ATM (*Automated Teller Machine*) kiosks that allow users to purchase crypto currencies by using *cash* or debit card).

[40] *See* Goldman et al., *supra* note 16, at 4.

[41] *See* DION-SCHWARZ ET AL., *supra* note 17, at 7.

[42] *See* Michal Lavi, *Do Platforms Kill?*, 43 HARV. J.L. & PUB. POL'Y 477, 484 (2020) (discussing recent incitement to terrorism on social media and the attacks that followed).

[43] DION-SCHWARZ ET AL., *supra* note 17, at 9.

For that reason, the use of cryptocurrencies by terrorists is a major problem. Curtailing such fundraising is crucial for national security and public safety.[44]

When deciding how to combat money laundering and terrorism financing in traditional financial markets, a consensus emerged (or rather seemed to exist), that going after the money by stifling terrorist financing, thus crippling their operations, is a key instrument in the war against terrorism.[45] This consensus translates into imposing duties and obligations on financial institutions[46] through anti-money laundering laws and anti-terrorism statutes.[47] Counter terrorism financing ("CTF") efforts "often focus on tracking the flow of money through bank accounts and preventing financial transactions that might be used to support attacks and other terrorist activities."[48]

However, terrorists' increased use of cryptocurrencies could undermine CTF's efficacy due to cryptocurrencies' decentralization;[49] regulators cannot rely on a central gatekeeper or intermediary to stop the flow of money for illicit purposes through the blockchain.[50] Moreover, some cryptocurrencies allow anonymous transactions.[51]

---

[44] *See id.* at xi ("We see little current evidence of the adoption of cryptocurrencies by terrorist organizations . . . but that very well might change as countermeasures shut off funding and as the cryptocurrency technology changes.").

[45] *See* Joseph J. Norton & Heba Shams, *Money Laundering Law and Terrorist Financing: Post-September 11 Responses—Let Us Step Back and Take a Deep Breath?*, 36 INT'L LAW. 103, 104 (2002).

[46] *See id.*

[47] *See generally* Olivia G. Chalos, Note, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 FORDHAM L. REV. 303 (2016) (addressing Section 2333 donor liability cases and the requirement for knowledge that the consequences were "substantially certain" to result from the donor's risky conduct, and the donor deliberately disregarded this fact).

[48] *See* DION-SCHWARZ ET AL., *supra* note 17, at ix.

[49] *See id.*

[50] Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code* of *Law and Code* as *Law*, 83 MOD. L. REV. 207, 214 (2019) ("One significant advantage of decentralised computer systems is the absence of any 'single point of failure[.]' Although this enhances the resilience of the network's stability and operation, it may be less desirable from a conventional law perspective because there is no single organisational or individual gatekeeper that it can target in order to intervene in their operation.").

[51] *Id.* at 210–11 ("Blockchain systems record the allocation of these tokens among anonymous accounts, automatically recording all exchanges of these tokens between accounts and automatically updating each copy of the database at each node.").

The only truly public feature of the cryptocurrency ledger is the documentation of ownership and transfers.[52] The names of the individuals performing transfers are not listed on the ledger.[53] Instead, ownership is represented by a set of letters and numbers indicating the user's public cryptocurrency address.[54] Thus, cryptocurrencies provide terrorists with streams of funding without meaningful tools for detection and prevention.[55] The story of Ali Shukri Amin—who provided instructions over Twitter to use Bitcoin to mask the provision of funds to ISIS—is just one of many striking examples demonstrating the risks posed by the anonymity surrounding cryptocurrencies.[56]

An increasing number of regulators are concerned with the use of cryptocurrencies for illegitimate activities such as terrorism financing, money laundering, and tax evasion.[57] In fact, the U.S. Treasury called to create cryptocurrency rules and new reporting requirements.[58] Under the proposed regime:

> Cryptocurrency exchanges and custodians would be required to report more information on the "gross inflows and outflows" of money moving through their accounts. Businesses would also be required to report cryptocurrency transactions above $10,000 [USD] under the new reporting requirements.[59]

---

52 *See* DION-SCHWARZ ET AL., *supra* note 17, at 2.

53 *See id.* at 2–3.

54 *See id.* at 2.

55 *See id.* at 3.

56 *See* FATF REPORT, *supra* note 8, at 36.

57 *See, e.g.*, Council Directive 2018/843, 2018 O.J. (L. 156) (EU); Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6001–6511, 134 Stat. 3388, 4547–633 (2021); Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021). For more information on tax evasion, see Israel Klein, *Contemptuous Tax Reporting*, 2019 WIS. L. REV. 1161, 1169–70 (2019) (defines "tax evasion" as "avoiding the payment of actual tax owed by not complying with the law and by breaching it").

58 *See* U.S. DEP'T OF TREASURY, THE AMERICAN FAMILIES PLAN TAX COMPLIANCE AGENDA 20–21 (2021), https://home.treasury.gov/system/files/136/The-American-Families-Plan-Tax-Compliance-Agenda.pdf [https://perma.cc/WN2E-H2TU].

59 Taylor Hatmaker, *US Treasury Calls for Stricter Cryptocurrency Rules, IRS Reporting for Transfers Over $10K*, TECHCRUNCH (May 20, 2021, 2:00 PM), https://techcrunch.com/2021/05/20/new-cryptocurrency-irs-rules-2023-crypto/ [https://perma.cc/RFQ5-ZQ9J].

Following this call, President Joe Biden signed the Infrastructure Investment and Jobs Act (the "Infrastructure Bill"), on November 15, 2021.[60] Accordingly, cryptocurrency asset exchanges and custodians are required to collect information from their customers, and develop an internal process "to keep track of the holding period and the buy and sell prices of the digital assets in its customer's accounts".[61] Companies that currently receive, or may in the future receive large payments in cryptocurrency need to file an IRS form upon the receipt of more than $10,000 worth of cryptocurrency.[62]

Passed by Congress in early 2021, the Anti-Money Laundering Act of 2020[63] broadens the Bank Secrecy Act's ("BSA") definition of "financial institution" to cover businesses that exchange cryptocurrencies.[64] Accordingly, exchanges must verify the identities of their consumers, develop customer risk profiles, and monitor transactions to submit suspicious activity reports ("SAR") to the Financial Crimes Enforcement Network ("FinCEN").[65]

---

60 Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021).

61 Timothy L. Jacobs et al., *New Cryptocurrency Information Reporting Regime Required on Form 1099 and Form 8300*, NAT'L L. REV. (Dec 13, 2021), https://www.natlawreview.com/article/new-cryptocurrency-information-reporting-regime-required-form-1099-and-form-8300 [https://perma.cc/7MAU-WTXL].

62 *Id*.

63 Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6001–6511, 134 Stat. 3388, 4547–633 (2021).

64 *See, e.g.*, Jodi L. Avergun et al., *The Anti-Money Laundering Act of 2020: New Challenges for Financial Institutions, Their Employees and Customers, and (Nearly) Everyone Else*, NAT'L L. REV. (Jan. 15, 2022), https://www.natlawreview.com/article/anti-money-laundering-act-2020-new-challenges-financial-institutions-their-employees [https://perma.cc/WJE4-M2JC]; Morgan Harrison & Theresa Kananen, *Anti-Money Laundering Act Expands Regulation of Cryptocurrency and Other Digital Assets*, JD SUPRA (May 20, 2021), https://www.jdsupra.com/legalnews/anti-money-laundering-act-expands-8737757/ [https://perma.cc/VN6T-KEWF] ("Section 5312 of the BSA ('Definitions and application') has been amended so that the definition of 'financial institution' includes 'a business in the exchange of currency, funds, or value that substitutes for currency or funds' and 'a licensed sender of money or any other person who engages as a business in the transmission of currency, funds, or value that substitutes for currency.'"); Andres Fernandez & Eddie A. Jauregui, *Key Provisions of the Anti-Money Laundering Act of 2020*, HOLLAND & KNIGHT (Jan. 13, 2021), https://www.hklaw.com/en/insights/publications/2021/01/key-provisions-of-the-anti-money-laundering-act-of-2020 [https://perma.cc/LBF5-2DK8].

65 31 C.F.R. § 1010.230 (2020). *See also* Katherine Kirkpatrick et al., *The Anti-Money Laundering Act and Crypto Collide: Non-Fungible Tokens*, KING & SPALDING (May 18, 2021), kslaw.com/news-and-insights/the-anti-money-laundering-act-and-crypto-collide-

To combat cryptocurrency use for illegal purposes, the European Union recently amended its Anti-Money Laundering Directive. The new Directive mandates cryptocurrency exchanges and custodian crypto-wallet providers to follow the same regulatory requirements as banks and other financial institutions.[66] In contrast to the United States and European Union, which strive to better understand cryptocurrencies in order to establish coherent regulatory policies, other countries, such as China[67] and South Korea, have taken a more extreme approach to mitigate concerns of fraud, money-laundering, and investor deception; they prohibit Initial Coin Offerings ("ICOs") altogether.[68]

This Article proposes that the token holders' identities be registered with corporations issuing the tokens prior to allowing an individual to get hold of the token; doing so will decrease future viability of cryptocurrencies for terrorists and other illicit users, cutting off the oxygen that enables their activities. Furthermore, the user-accessible registry should remain anonymized and court warrants should be required before unmasking the identities of token-holders. This Article is structured as follows:

Part I presents an overview of intermediaries' role as the new gatekeepers of users' illegal activities. It addresses conventional regulations on financial intermediaries to combat transfers of money for illicit purposes. It explains that the twenty-first century has created a pluralistic model—a new school of regulation—with many different actors. This model can be condensed into a triangle of actors: the state, infrastructures that facilitate violations of law, and the violators.[69] Examples of such regulations will be provided. Part I

non-fungible-tokens [https://perma.cc/46QP-CPJT] (discussing reporting obligations under the Anti-Money Laundering Act of 2020); Will Kenton, *Suspicious Activity Report (SAR)*, INVESTOPEDIA, https://www.investopedia.com/terms/s/suspicious-activity-report.asp [https://perma.cc/TG7T-BSZZ] (Jan 25, 2022).

66 *See generally* Council Directive 2018/843, 2018 O.J. (L 156) ¶ 44 (EU).

67 *See China Widens Ban on Crypto Transactions; Bitcoin Tumbles*, BLOOMBERG (Sept. 24, 2021, 5:40 AM), https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown [https://perma.cc/AP6H-3LQK].

68 *See* Hadar Y. Jabotinsky, *The Regulation of Cryptocurrencies: Between a Currency and a Financial Product*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 118, 120 (2020).

69 *See generally* Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011 (2018) (in the related context of regulation of speech).

concludes with a description of anti-money laundering and anti-terrorism regulations that apply to traditional financial gatekeepers.

Part II explores the features of cryptocurrencies and, even more relevantly, the features of the blockchains on which they are registered, focusing on the most commonly used blockchains, namely those of Bitcoin and Ethereum. This Part explains that, due to the blockchain's decentralized structure and the anonymity of token holders, transactions made on the blockchain cannot be regulated. Anonymous blockchain transactions facilitate the use of these tokens by terrorists. Without meaningful regulation of illicit transactions, terrorism can flourish and threaten both national security and public safety.

Part III proposes to mitigate the problem by registering and verifying the identities behind token owners. This is also known as permissioned (private) blockchains, such as the one intended for Facebook's new cryptocurrency, the Diem (previously Libra).[70] On such a blockchain, an access control layer is added to govern who can access the network.[71] Token holder access is then vetted by the network owner.[72] Our suggested regulatory solution would allow unmasking the token owner's identity only where there is probable cause and would be subject to a court warrant. Therefore, such regulatory change would be in line with the Fourth Amendment, even after the Supreme Court's *Carpenter v. United States* opinion narrowing the third-party doctrine.[73] Imposing such obligations on

---

[70] *See* DIEM ASS'N, LIBRA WHITE PAPER v2.0 (2020), https://www.diem.com/en-us/white-paper/#cover-letter [https://perma.cc/GN8S-LKCC].

[71] *See* Anisha Mirchandani, Note, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1201, 1211 (2019); Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1372 (2018); Jake Frankenfield, *Permissioned Blockchain*, INVESTOPEDIA, https://www.investopedia.com/terms/p/permissioned-blockchains.asp [https://perma.cc/X33V-95TK] (Jan. 24, 2022) ("Administrators maintain an access control layer to allow certain actions to be performed only by certain identifiable participants.").

[72] Mirchandani, *supra* note 71, at 1211 ("While a public blockchain requires a majority of all nodes, or participants, to determine whether a transaction or block is verified, a consortium blockchain is a permissioned blockchain that allows only specific, pre-selected nodes to determine whether a block is verified.").

[73] Carpenter v. United States, 138 S. Ct. 2206, 2210–11 (2018). *See also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358, 385 (2019) (explaining

companies issuing cryptocurrencies is just and efficient because the companies benefit commercially from the use of their financial products. The benefits of maintaining a registrar of token holders would exceed the obligated companies' costs and have potential to curb terrorism financing at this crucial juncture.

Part IV addresses objections to the proposed solution. *Inter alia*, this Part addresses First Amendment freedom of expression concerns, as well as considerations such as usability, administrative costs, data security, and enforcement methods. No law reform proposal is free from externalities and vices. While these concerns are duly noted, this Part argues that the costs and risks of verifying and unmasking cryptocurrency identities are justified and consistent with constitutional basics.

I. INTERMEDIARIES AS GATEKEEPERS: TRADITIONAL INTERMEDIARY REGULATION FOR COMBATING VIOLATIONS OF LAW

At a basic level, traditional, or "old-school," regulations impose imprisonment or fines to regulate and decrease violations of law.[74] This type of traditional regulation can be labeled "*dualist*" or "*dyadic.*"[75] In this model, there are essentially two players: the state and the violator.[76] However, in the twenty-first century, there are multiple players, necessitating a pluralist model. Companies at the center of the economy provide infrastructure that facilitates both legal and illegal activities.[77] Policymakers have enlisted entities such as online intermediaries, technology firms, financial intermediaries, and payment processing intermediaries to regulate activities they facilitate.[78] Such regulations can be within the context of

how *Carpenter* alone presents a fundamental change to Fourth Amendment doctrine. *Carpenter* requires a warrant in many situations where none was required before.).

74 *See* Lavi, *supra* note 42, at 505 (quoting Balkin, *supra* note 69, at 2015).

75 *See* Balkin, *supra* note 69, at 2013 (referring to a related context of speech regulation).

76 *See id.*

77 For example, big tech such as internet intermediaries and financial institutions.

78 *See* Balkin, *supra* note 69, at 2016 ("Although nation-states continue to regulate speech directly through old-school methods, they increasingly depend on new-school speech regulation—attempting to coerce or co-opt private owners of digital infrastructure to regulate the speech of private actors.").

administrative law.[79] Yet, in many cases, the obligation to regulate that is imposed on companies providing infrastructure falls within the bounds of civil and criminal law.[80] Professor Balkin dubbed this type of enforcement "the new-school regulation."[81] Balkin focused on the role this model plays in regulating speech through companies that provide infrastructures such as internet service providers ("ISPs"), websites that host content ("content providers"), and even search engines.[82] Yet, the same structure is used to deter and enforce other violations of law. This model includes many different players, but can be condensed into a triangle of actors: the state, the law violator, and the infrastructure, which serves as a gatekeeper.

Violations of law are often committed under a cloak of anonymity and in jurisdictions without effective rules of law.[83] Such violations pose a challenge to law enforcement. In order to cope with this challenge and mitigate harm caused by violators, enforcement relies

---

[79] *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 467–68 (2020) (referring to the rise of the enforcer-firm regulation that gives a prominent role to the administrative state's newest gatekeepers). *See also* Rory Van Loo, *The Revival of Respondeat Superior and Evolution of Gatekeeper Liability*, 109 GEO. L.J. 141, 172 (2020) ("[T]he new gatekeeper governance paradigm is propelling some businesses into higher control relationships, thereby making it more likely courts will see them as principals under the common law."). For a similar argument in the context of privacy law, see ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA AND CORPORATE POWER 106 (2021) (explaining that privacy law tactic changed from self-regulation to public-private partnership in the development of enforcement of law).

[80] Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 958 (2021) (for an example in the context of applying Computer Fraud and Abuse Act ("CFAA") by platform owners); *see also id.* at 954–55 ("Under cyber-trespass laws like the CFAA, some courts have treated platforms as *digital gatekeepers*—as property owners that may permit and restrict access to their websites much like landowners may do with private land in the real world."); WALDMAN, *supra* note 79.

[81] *See* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298–99 (2014) (focusing on this model's role in regulating speech, Balkin explains that states attempt to regulate, coerce, or co-opt key players that shape the internet in order to get their infrastructure to surveil, police, and control speakers).

[82] *See id*. at 2306. For another example of "new-school" speech-regulation methods, see also Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014) (European Union case involving the right to be forgotten). *See also* Michal Lavi, *The Good, the Bad, and the Ugly Behavior*, 40 CARDOZO L. REV. 2597, 2630–35 (2019).

[83] *See* Aniket Kesari et al., *Deterring Cyber Crime: Focus on Intermediaries*, 32 BERKELEY TECH. L.J. 1093, 1130–31 (2017).

heavily on intermediaries that provide the infrastructure for such activities to occur.[84] Accordingly, when an enforcer investigates and intervenes, "legal demands may fall upon third parties, individuals, and businesses that were merely used as conduits by the suspect."[85] Imposing legal obligations and liability on the infrastructures for third-party violations of law is a powerful incentive to mitigate harm, as it ensures the cooperation of companies with law enforcers and incentivizes them to operate safely.[86]

As companies that provide infrastructure are also located at a highly visible choke point for regulatory intervention, it seems natural to obligate them to supervise and regulate their users' activities on the platforms. One prominent example is using online intermediaries to regulate and remedy harmful speech.[87] Although U.S. law allows intermediaries to benefit from overall immunity for content published by others,[88] they are encouraged to mitigate the harm of harmful content voluntarily, or in the shadow of potential regulation.[89] Such cooperation solves structural constraints under constitutional law, as platforms are not state actors and are not constrained by the First Amendment,[90] so government agencies are relatively free to enlist private actors as cooperators which enables them to do things they would otherwise be constitutionally forbidden from

---

84 *See id.* at 1131.

85 *See id.* at 1096.

86 Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, *supra* note 79, at 477 ("[I]f the law imposes vicarious liability on the pharmaceutical company for violations by its ingredient supplier, the pharmaceutical company may be motivated to audit the supplier's production process even though auditing is not required.").

87 *See* Elena Chachko, *National Security by Platform*, 25 STAN. TECH. L. REV. 55, 83 (2021).

88 *See* Communications Decency Act, 47 U.S.C. § 230; *see also* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 246 (2019); Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855, 867–70 (2016). *See generally* Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019).

89 Chachko, *supra* note 87, at 128 (referring to "government threats in nudging platforms to step up their contribution to national security, lest they face unwanted adverse regulation.").

90 *Id*. at 106 (referring specifically to platforms role in removing content that impairs national security and defining this policy as "national security by platforms as privatization").

doing.[91] Moreover, in many countries outside the United States, intermediaries can be held responsible for failing to remove speech inciting terrorism,[92] hate speech,[93] defamation,[94] and even fake news.[95]

---

[91] *See* NEIL RICHARDS, WHY PRIVACY MATTERS 139 (2021).

[92] *See* Lavi, *supra* note 42, at 506–07. *See also* Mark Leiser & Edina Harbinja, *Why the United Kingdom's Proposal for a "Package of Platform Safety Measures" Will Harm Free Speech*, 2020 TECH. & REG. 78, 82 (2020). For criticism, see Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1043–45 (2018). It should be noted that recently, the European Union outlined a regulation regarding terrorist content online that requires platforms to take down terrorist content quickly and "adopt more proactive measures to prevent the spread of terrorist content in the first place." Hannah Bloch-Wehba, *Content Moderation as Surveillance*, 36 BERKELEY TECH. L.J. (forthcoming 2022) (manuscript at 13) (referring to Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online ("TERREG")).

[93] In fall 2017, the German government drafted the Network Enforcement Act ("NetzDG") for accommodating hate speech and fake news. The Act applies to criminally offensive speech as defined in the German Penal Code, including defamation. It stipulates a differential timeframe for intermediaries to remove harmful content. Intermediaries have to make sure that they delete content that appears evidently unlawful within twenty-four hours of filing of a complaint. *See* Gesetz zur Verbesserung der Rechtsdurchsetzung in Sozialen Netzwerken [NetzDG] [Act to Improve Enforcement of the Law in Social Networks], Oct. 1, 2017, BUNDESGESETZBLATT, Teil I [BGBL I], at § 3(2)(4) (Ger.); Wolfgang Schulz, *Regulating Intermediaries to Protect Privacy Online—the Case of the German NetzDG*, *in* PERSONALITY AND DATA PROTECTION RIGHTS ON THE INTERNET 5–6 (forthcoming). *See also* Meg Leta Jones, *Silencing Bad Bots: Global, Legal and Political Questions for Mean Machine Communication*, 23 COMMC'N. L. & POL'Y 159, 177 (2018); Evelyn Mary Aswad, *The Future of Freedom of Expression Online*, 17 DUKE L. & TECH. REV. 26, 45 (2019) (discussing the adoption of codes of conduct against hate speech by major online corporations to meet the standards proposed by the UN).

[94] *See, e.g.*, Delfi AS v. Estonia, App. No. 64569/09, ¶¶ 114–15 (June 16, 2015), https://hudoc.echr.coe.int/eng?i=001-126635 (The European Court of Human Rights held the popular Delfi news website accountable for defamatory statements about a famous Estonian business executive. Following an article about the executive's business ventures, anonymous users posted in the comments section, including personal threats and offensive language. The Court held Delfi responsible even though it removed the comments upon knowledge). *See also* Case C-18/18, Glawischnig-Piesczek v. Facebook Ir. Ltd., ECLI:EU:C:2019:821 (Oct. 3, 2019) (the Court of Justice of the European Union held that law does not preclude intermediaries such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared unlawful).

[95] For example, Singapore allows the government to order intermediaries to remove false statements. Bill No. 10/2019 Protection from Online Falsehoods and Manipulation Bill, bit.ly/30hacIC [https://perma.cc/B9XA-ZHMG]. Part four of the law refers to directions to internet intermediaries and providers of mass media services. *See also* Jason

In a related context, copyright owners turn to online intermediaries to mitigate copyright infringements and to enforce their intellectual property ("IP") rights.[96] In such cases, intermediaries may benefit from a legal safe haven if certain steps are taken, such as responding to takedown requests by IP rights holders.[97] However, a platform's failure to comply may render it vicariously liable for copyright infringements, in case the content is infringing on IP rights.[98]

A third example is payment systems and networks for banks and merchants, such as Visa or Mastercard, which are paid to process consumer purchases.[99] Such payment processing intermediaries attempt to enforce IP rights and mitigate violations of law by "following the money" flowing to online merchants who profit from illegal

---

Luger, *Planetary Illiberalism and the Cybercity-State: In and Beyond Territory*, *in* TERRITORY, POLITICS, GOVERNANCE 1–2 (2019); Niharika Mandhana & Phred Dvorak, *Ordered by Singapore, Facebook Posts a Correction*, WALL ST. J. (Nov. 30, 2019 7:15 AM), on.wsj.com/2L9FU4P [https://perma.cc/P5T9-DDGU]. For further information on anti-fake news laws, see *The Rise of "Fake News" Laws Across South East Asia*, PUB. MEDIA ALL. (Dec. 6, 2019), bit.ly/2Xbl3TO [https://perma.cc/NL4L-UNSR] (providing an overview on fake news laws across Southeast Asia, with a focus on media freedom).

96 JACQUELINE LIPTON, RETHINKING CYBERLAW—A NEW VISION FOR INTERNET LAW 66 (2015).

97 *See, e.g.*, Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512; *see also* Kesari et al., *supra* note 83, at 1095–96; Directive (EU) 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 14(1), 2000 O.J. (L 178). It should be noted that the EU imposes obligations on intermediaries regarding copyright infringement beyond a notice and takedown regime. *See* Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, art. 17, 2019 O.J. (L 130). Moreover, a proposed regulation to amend the Electronic Commerce directive, attempts to impose more obligations on intermediaries to assist enforcement of violations of rights. *See* Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, at 44–45, COM (2020) 825 final (Dec. 15, 2020).

98 *See* Zoe Carpou, Note, *Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users*, 39 COLUM. J.L. & ARTS 551, 565 (2016) ("The ISPs themselves face limited resources and the ever-present risk of losing safe harbor protection if they fail to 'expeditiously' remove content pursuant to takedown requests.").

99 Kesari et al., *supra* note 83, at 1126–27 ("Visa, like MasterCard, is a payment network, an ISP-like entity for banks and merchants that exchange money in order to process consumer purchases.").

activities such as piracy and counterfeiting.[100] Creating a payment blockade seriously threatens the website's continued existence and, thus, is effective in preventing the unwanted behavior.[101] Blocking payment-by-payment processing systems is voluntary.[102] However, these practices are "not in the shadow of existing law, but in the shadow of potential law," such as legislative bills aimed at payment processors.[103] Moreover, litigation costs and potential legal liability can also motivate payment processors to block payments from reaching entities that profit from illegal activities.[104]

Another function of payment intermediaries is monitoring suspicious activities performed by the same merchants across different banks. For example, Visa can search for potential infringements in its payment systems, respond to complaints, investigate or instruct the payment company to investigate the merchant, and create a report within five business days.[105] After reviewing the report, Visa instructs the payment company to send a "comply or terminate" notice to the suspected infringer.[106] Acting as a checkpoint in the marketplace, payment systems can place the flow of revenues and funding of illicit actors under siege and disrupt their activities to avoid potential regulation.

---

100 Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1523 (2016).

101 *See id.* at 1525–27.

102 *Id.* at 1528–29.

103 *Id.* at 1528 (intermediaries tend to coalesce around voluntary enforcement agreements "not in the shadow of existing law, but in the shadow of potential law") (quoting Ronald J. Mann & Seth R. Belzley, *The Promise of Intermediary Liability*, 47 WM. & MARY L. REV. 239, 260 n.59(2005)). For example, the bills COICA, SOPA, and PIPA all aim to prevent services from completing payment transactions involving customers located within the United States, and target the internet site associated with the [targeted] domain name. Such legislative bills influence intermediaries to block entities that profit from illicit activities. Combating Online Infringements and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010); Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011); Protect Intellectual Property Act (PIPA), S. 968, 112th Cong. (2011).

104 *See, e.g.*, Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 798 n.9 (9th Cir. 2007) (dismissing a case in which Perfect 10 sued Visa, MasterCard, and other payment intermediaries (collectively, "Visa") on the theory that they were contributorily and vicariously liable for infringements occurring on so called Stolen Content Websites to which Visa provided payment processing services; Judge Kozinski dissented).

105 Kesari et al., *supra* note 83, at 1127.

106 *Id.* at 1127.

Beyond the context of online speech and IP infringements, intermediaries can suspend or terminate the flow of money.[107] Because of this, traditional financial institutions have aided enforcement of anti-money laundering and anti-terrorism statutes for many years.[108] The Financial Action Task Force ("FATF"), the global organization combating money laundering and terrorist financing, was formed in 1989 by the "G-7"—a group of seven developed countries.[109] The FATF sets international standards aiming to prevent money laundering and terrorism financing. It also works to generate the political will to lead countries toward adopting legislative and regulatory reforms in this area. [110] The FATF's recommendations are then adopted into local legislation by all the jurisdictions complying with the recommendations. Jurisdictions that do not comply are put on a blacklist of non-cooperative states, which flags states that do not comply with it.[111] As a result, financial institutions in compliant states are likelier to refrain from doing business or interacting with financial institutions or individuals from noncompliant states.[112]

---

[107] LUCA BELLI ET AL., PLATFORM REGULATIONS: HOW PLATFORMS ARE REGULATED AND HOW THEY REGULATE US 220 (2017).

[108] *See* Stavros Gadinis & Colby Mangels, *Collaborative Gatekeepers*, 73 WASH. & LEE L. REV. 797, 836, 846 (2016).

[109] *See History of the FATF*, FIN. ACTION TASK FORCE, www.fatf-gafi.org/about/historyofthefatf/ [https://perma.cc/P9PS-ZAFK]. *See also* James Thuo Gathii, *The Financial Action Task Force and Global Administrative Law*, 2010 J. PRO. LAW. 197, 197 (2010).

[110] *See* Gathii, *supra* note 109, at 200 ("To complement this standard-setting role, the FATF seeks to ensure effective compliance of its standards. It does so by recommending its anti-money laundering policies and laws to its members and non-members and by generating the 'political will to bring about national legislative and regulatory reforms.'").

[111] *About the Non-Cooperative Countries and Territories (NCCT) Initiative*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html?hf=10&b=0&s=desc(fatf_releasedate) [https://perma.cc/9VVZ-ETAT].

[112] *See generally* Nizan Geslevich Packin & Hadar Y. Jabotinsky, Sanction Me If You Can—the Law and Economics of Blacklisting (2022) (unpublished manuscript) (on file with authors).

A. The Infrastructure as a Gatekeeper of Illegal Money Transfers for Terrorist Activity

Terrorists need funding for their activities. With greater funding, they can organize and execute more frequent and lethal attacks.[113] As money is usually transferred via a financial intermediary, financial institutions are infrastructures that, unwittingly, facilitate the transfer of money for terrorism.[114] Due to this feature, financial institutions—such as banks and wire services—have the ability to deny services, making it difficult for terrorists to receive and transfer money.[115] If terrorists are prevented from easily receiving donations and funding, the oxygen for their activities is cut off. Financial transfer chokepoints present an opportunity to slow money transfers for terrorist operations, disrupt their activities, and block them from perpetrating illicit acts.[116]

In light of the abovementioned characteristics of financial intermediaries, law enforcement agencies have developed and implemented several successful approaches to prevent the flow of funding to terrorist organizations and other criminals through financial intermediaries.[117] Federal law places responsibilities on financial institutions to prevent donations and payments for terrorism.[118] For example, "when an enforcer investigates and makes interventions," the responsibility to make legal demands may instead fall upon financial intermediaries and businesses "that were merely used as conduits by

---

[113] *See* DION-SCHWARZ ET AL., *supra* note 17, at 1 (citing ARABINDA ACHARYA, TARGETING TERRORIST FINANCING: INTERNATIONAL COOPERATION AND NEW REGIMES (2009)).

[114] Paul Schott Stevens & Thomas C. Bogle, *Patriotic Acts: Financial Institutions, Money Laundering and the War Against Terrorism*, 21 ANN. REV. BANKING L. 261, 283–85 (2002).

[115] Stephen I. Landman, Bank Liability Under the Anti-Terrorism Act: Dispelling the "Routine Banking Services" Defense in Material Support Cases, at 15–16, 24 (Dec. 9, 2008) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1314104 [https://perma.cc/YA5X-8M7M].

[116] *See* Kesari et al., *supra* note 83, at 1106.

[117] *See, e.g.*, DION-SCHWARZ ET AL., *supra* note 17, at ix (discussing Counter Terrorism Financing ("CTF")). For further information on CTF, see *supra* note 48 and accompanying text.

[118] *See* John J. Byrne, *Banks and the USA Patriot Act*, 9 ECON. PERSPS. 18, 18–21 (Sept. 2004).

the suspect."[119] Assigning responsibility to the financial institutions incentivizes these intermediaries to take measures to combat money laundering activities on their platforms (whether the money is transferred through bank accounts or other tools).[120] In addition to impacting terrorist fundraising, "this increased enforcement has significantly reduced the ability of terrorist groups to rely on formal banking," especially money management and transfer services, which is "an expansive category that can include digital transfers, prepaid instruments, and mobile payment systems."[121] The anti-money laundering and anti-terrorism statutes serve as primary examples of gatekeeping obligations and financial institution liability. The following Subsections focus on these existing CTF regulatory solutions and expand upon main gatekeeping obligations.

1. Traditional Financial Intermediaries at the Service of National Security

a) Anti-Money Laundering Statutes

Money laundering is a process in which individuals who obtain money through criminal activity (including terrorism) try to conceal the illegal source of income and make it appear legitimate.[122] Money laundering is a systemic problem that greatly impacts the world's economy.[123] Money laundering activities are typically comprised of three stages: (1) placement—introducing money into the financial system; (2) layering—masking the origin through multiple, separate transactions; and (3) integration—integrating the illegal proceeds from the crime into the legitimate financial system.[124] Anti-money

---

119 *See* Kesari et al., *supra* note 83, at 1096.

120 *See* Amanda Bloch Kernan, *Sustaining the Growth of Mobile Money Services in Developing Nations: Lessons from Overregulation in the United States*, 51 VAND. J. TRANSNAT'L L. 1109, 1141, 1143 (2018).

121 *See* DION-SCHWARZ ET AL., *supra* note 17, at 10 (referencing 31 C.F.R. §§ 1010, 1021, 1022 (2021)).

122 *See generally* Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. INT'L L. & COM. REG. 437 (1994).

123 "[T]he United Nations recently estimated that the criminal proceeds laundered annually between [two] and [five] percent of global GDP, or $1.6 to $4 trillion a year." Rhoda Weeks-Brown, *Straight Talk: Cleaning Up*, INT'L MONETARY FUND, Dec. 2018, at 44.

124 Alford, *supra* note 122, at 439.

laundering regulations try to catch and prevent the latter two steps—layering and integration.

Although anti-money laundering regulation has existed in most developed countries since the 1970s,[125] Western governments have significantly increased the enforcement of these regulations since the September 11, 2001, terrorist attacks ("9/11"). After 9/11, a consensus emerged, "that going after the terrorist money is a key instrument in this war against terrorism."[126] This notion translated into more "duties and obligations on financial institutions around the world."[127] Thus, anti-money laundering has become a core element in combating terrorist activities and related crimes "and a central precept to international banking standards."[128]

The executive branch and Congress took action, and the United States was quick to adopt further measures against money laundering.[129] The result was the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, referred to as the USA PATRIOT Act,[130] ("the Patriot Act"),[131] which calls upon every American patriot to play his or her part in defending against the threat of terrorism.[132] The purpose of the Patriot Act is "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law

---

125 In 1970, Congress passed the Bank Secrecy Act requiring financial institutions to report to the government on cash transactions exceeding USD 10,000. *See* 31 U.S.C. §§ 5311, 5413; 31 C.F.R. § 1010.311 (2021). In 1996, federal regulations began requiring banks to report suspicious activities. *See* 12 C.F.R. §§ 21.11, 163.180 (2021).

126 *See* Norton & Shams, *supra* note 45, at 104. *See also* Goldman et al., *supra* note 16, at 4 (noting that "'following the money' has been a particularly effective component of an overall strategy to degrade the capabilities of terrorist groups.").

127 Norton & Shams, *supra* note 45, at 104.

128 *See id.* at 105.

129 *See id.* at 104. *See also* Chalos, *supra* note 47, at 317 (referencing 18 U.S.C. § 1956(a)(2), which "prohibits the transportation, transmission, or transfer of funds from a place inside the United States to a place outside the United States 'with the intent to promote the carrying on of specified unlawful activity.'" The statue "criminalizes 'reverse' money laundering, or the movement of 'clean' money overseas for an illicit purpose.").

130 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act creates an acronym ("USA PATRIOT"). Norton & Shams, *supra* note 45, at 104.

131 USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). *See* Norton & Shams, *supra* note 45, at 104.

132 Norton & Shams, *supra* note 45, at 104.

enforcement investigatory tools, and for other purposes."[133] The Patriot Act enhances the partnership between the public and private sectors in policing the channels of international financial transfers[134] and applies to foreign financial institutions and foreigners not residing within U.S. jurisdictions.[135] The Patriot Act requires financial institutions—the gateways—to serve as the first line of defense against illicit activity in the financial system.[136] These institutions are charged with blocking any movement of money transmitted through their systems that is generated from crime or designated for terrorism.[137] They are also supposed to "know their clients," by completing a Know Your Client ("KYC") questionnaire that acquaints the institution with a client's account activities; doing so helps avert criminals and terrorists.[138] This should be accomplished by "adopting broader risk management approaches that will make it harder for abuse to [occur] in the first place."[139]

Title III of the Patriot Act—the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001[140]—relates to the global issues of money laundering. Anti-money laundering statutes focus on specific areas of banking obligations.[141] As mentioned above, the provisions obligate financial intermediaries to know their

---

133 *Id.* at 107–08.

134 *See id.* at 116.

135 *See id.* at 108.

136 *See* David A. Andelman, *The Drug Money Maze*, FOREIGN AFFS., July–Aug. 1994, at 94,102–03.

137 *See* Goldman et al., *supra* note 16, at 30 ("These statutes require financial institutions, the gateways, to be the first line of defense against illicit activity moving around the financial system. They are charged with blocking the movement of dirty money that transits their systems and keeping out bad actors, and with adopting broader risk management approaches that will make it harder for abuse to take place in the first place.").

138 *See* 12 U.S.C. § 635(i); 31 C.F.R. § 1020.200 et seq. (2016); Kesari et al., *supra* note 83, at 1096; Bridy, *supra* note 100, at 1565; Norton & Shams, *supra* note 45, at 106, 121 ("[F]inancial institutions are required to consult the list of suspected terrorists and terrorist organizations provided by '*any* government agency' (emphasis added) to determine whether a potential customer appears on the list. This could result in an enormous regulatory burden that is too soon to assess. The financial institutions are already aware of problems imposed by the variations in spelling of Arabic names.").

139 *See* Goldman et al., *supra* note 16, at 30.

140 Pub. L. No. 107-56, tit. III, 115 Stat. 272, 296–342 (2001). *See* Norton & Shams, *supra* note 45, at 104.

141 *See* Norton & Shams, *supra* note 45, at 106.

customers and require that ordinary users provide documentation of their identity.[142] A second area of obligation concerns due diligence, as it relates to private banking activities and supply of credit.[143]Additional obligations relate to reviewing relationships with non-U.S. correspondent banks and shell banks, and monitoring wire transfers for patterns of money laundering activities.[144] Such requirements can create blockades of illegal transfers and thus allow tracking, monitoring, and confiscation of such transfers.[145] Banks are supposed to report unusual activities in their customers' accounts, as well as specific transactions dictated by the laws and regulations.[146] Obviously, complying with anti-money laundering requirements places a heavy regulatory burden on financial institutions—especially since failure to comply can result in liability.[147]

The United States supplements this regulatory framework with three criminal laws: two laws prohibiting money laundering,[148] both relating to the prohibition against financial transfers relating to proceeds from unlawful activities; and one law prohibiting the restructuring of financial transactions to avoid reporting.[149]

i. Money Laundering and Comingled Bank Accounts in Court Rulings

Comingling funds within bank accounts is another issue that perpetuates illegal activities, such as funding terrorism and other financial crimes.[150] Though the Supreme Court has yet to address the issue, lower courts provide a spectrum of opinions on the matter.[151] In

---

142 *See* Robert M. Taylor II, *Anti-Money Laundering and Anti-Terrorist Financing Requirements Applicable to Financial Institutions*, 120 BANKING L.J. 497, 499 (2003).

143 *Id.* at 501.

144 *See* Norton & Shams, *supra* note 45, at 106.

145 *Id.* at 106, 117–21.

146 *Id.* at 109.

147 *See id.* at 122.

148 18 U.S.C. §§ 1956–1957.

149 31 U.S.C. § 5324.

150 *See* Rachel May Zysk & Eddie Suarez, *Proving Money Laundering Beyond a Reasonable Doubt: The Problem of Commingled Property Under 18 USC § 1957*, CHAMPION, May 2017, at 34, 35.

151 *See, e.g.*, United States v. Silver, 864 F.3d 102, 115 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 738 (2018); United States v. Haddad, 462 F.3d 783, 792 (7th Cir. 2006); United States v. Pizano, 421 F.3d 707, 723 (8th Cir. 2005); United States v. Loe, 248 F.3d 449, 467 (5th Cir. 2001); United States v. Davis, 226 F.3d 346, 357 (5th Cir. 2000); United

United States v. Moore, the Fourth Circuit ruled that because legal funds cannot be distinguished from illegal funds in the same bank account, all funds in an account engaged in criminal activity are to be considered proceeds of that criminal activity.[152] A similar approach is taken by other circuit courts,[153] but not by all. For example, the Ninth Circuit demands proof that the funds are the proceeds of criminal activity,[154] and the Fifth Circuit has a presumption that "clean money" is spent before dirty money.[155]

Usually, due to specific clauses in the deposit insurance contract, banks are able to freeze accounts with commingled funds if they detect suspicious activity in the account.[156] Courts may also freeze property that was obtained as a result of money laundering activity.[157] However, in *Luis v. United States*, the Supreme Court held that freezing an account containing comingled funds violated the defendants' Sixth Amendment right to assistance of counsel.[158] Dissenting, Justices Kennedy and Alito opined that it is impossible to tell if a defendant spent the legal funds in the account first or if the illegal funds are fungible.[159] However, as mentioned above, the overarching issue remains unresolved, as the Supreme Court has yet to address it.

States v. Rutgard, 116 F.3d 1270, 1292 (9th Cir. 1997); United States v. Sokolow, 91 F.3d 396, 409 (3d Cir. 1996); United States v. Moore, 27 F.3d 969, 976–77 (4th Cir. 1994); United States v. Johnson, 971 F.2d 562, 570 (10th Cir. 1992); United States v. Jackson, 935 F.2d 832, 840 (7th Cir. 1991); *See also* Sarah Scharf, The Question of Commingled Funds in the Criminal Prosecution of Individuals for Money Laundering (2019) (unpublished manuscript) (on file with author).

152 *Moore*, 27 F.3d at 976–77.

153 Such an approach has been adopted by the Second, Third, Seventh, Eighth, and Tenth Circuits. *See Silver*, 864 F.3d at 115; *Sokolow*, 91 F.3d at 409; *Jackson*, 935 F.2d at 840; *Pizano*, 421 F.3d at 723; *Johnson*, 971 F.2d at 570. *See also* Scharf, *supra* note 151, at 2.

154 *Rutgard*, 116 F.3d at 1292.

155 *Davis*, 226 F.3d at 357 ("[W]hen the aggregate amount withdrawn from an account containing commingled funds exceeds the clean funds, individual withdrawals may be said to be of tainted money, even if a particular withdrawal was less than the amount of clean money in the account."). *See Loe*, 248 F.3d at 467; Scharf, *supra* note 151, at 2.

156 *See, e.g.*, *Deposit Agreement & Disclosures*, COMMERCE BANK (June 15, 2020), www.commercebank.com/personal/bank/deposit-agreement [https://perma.cc/YZ77-AEGN]. *See also* Scharf, *supra* note 151, at 2.

157 18 U.S.C. § 1345(a)(2).

158 136 S. Ct. 1083, 1087 (2016) (plurality opinion).

159 *See id.* at 1109 (Kennedy, J., dissenting). *See also* Scharf, *supra* note 151, at 3.

b) Anti-Terror Statutes: Material Support and the Criminalization of Financing of Terrorism

Financial institutions play an important role in efforts to cut off financial support for terrorist organizations.[160] Anti-terror statutes codify the Patriot Act[161] by prohibiting the provision of material support for terrorism and exposing financial institutions to ex-post civil and criminal liability for facilitating money transfers to terrorist organizations.[162] 18 U.S.C. Section 2339A prohibits providing "material support or resources . . . knowing or intending that they are to be used in preparation for, or in carrying out" a violation of certain offenses, including terror.[163] Section 2339C addresses the collection of funds.[164] It imposes penal sanctions against the provision or collection of funds "with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, in order to carry out" a statutorily enumerated predicate crime.[165]

Unlike Sections 2339A and 2339C, Section 2339B does not require knowledge, intent, or specific intent mens rea[166] to fund

---

[160] The main Anti-Terror Statutes are 18 U.S.C. § 2339A, which "outlaws providing material support for the commission of certain designated offenses that might be committed by terrorists," and 18 U.S.C. § 2339B, which "outlaws providing material support to certain designated terrorist organizations." CHARLES DOYLE, CONG. RSCH. SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. § 2339A AND § 2339B 1 (2016).

[161] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[162] *See* Norman Abrams, *The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code*, 1 J. NAT'L SEC. L. & POL'Y 5, 10 (2005).

[163] 18 U.S.C. § 2339A; *see also* Ronbert H. Schwartz, Comment, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*, 48 LOY. U. CHI. L.J. 1181, 1184–86 (2017); Lavi, *supra* note 42, at 510.

[164] Chalos, *supra* note 47, at 315.

[165] 18 U.S.C. § 2339C(a).

[166] Mens rea is the criminal intent or state of mind of the person committing the crime that must be proven to convict. Francis Bowes Sayre, *Mens Rea*, 45 HARV. L. REV. 974, 1017 (1932); *see also* Chalos, *supra* note 47, at 319–20 ("To violate [Section] 2339A, the defendant must provide material support or resources '*knowing or intending*' that they are used to carry out acts of terrorism. To violate [Section] 2339C, the defendant must have provided or collected funds with *the specific intent or knowledge* that the funds were to be used to 'carry out' enumerated predicate offenses related to terrorism . . . .By contrast, to violate [Section] 2339B, the defendant must only have *knowledge* that the organization is a designated FTO or engages or has engaged in acts of terrorism. The defendant is not required to know or intend that the material support or resources would be used to carry out a violent crime . . . .Courts hold that the knowledge requirement of [Section] 2339B

terrorist activities; rather, it prohibits "knowingly provid[ing] material support or resources to a foreign terrorist organization" ("FTO").[167] Thus, if a provider, such as a bank or other financial institution, knows that an organization has been officially designated as a "terror" organization, or if it knows that an organization engages in terrorism, the financial institution may be found liable, even without knowing that the funds were to be used to "carry out" acts of terrorism.[168]

It is frequently difficult "to separate licit operations and expenses, such as salaries and social services, from clearly illicit spending, such as terrorism recruitment and training."[169] This is due to "lack of information about and the close relationship between these activities."[170] It is especially difficult since legitimate activities help terrorists mask illegal activities.[171] For example, operating costs of terrorism, "such as propaganda, recruitment, salaries, and social services, indirectly contribute to an organization's ability to produce violence."[172] However, Section 2339B applies to any support provided to a terrorist organization.[173] The Supreme Court upheld the constitutionality of Section 2339B in *Holder v. Humanitarian Law Project* ("HLP"), determining that "the federal government [has] the authority to prohibit groups from working with terrorist organizations even when their violent operations [are] interlinked with more benign functions, such as charity work."[174] Considering

---

may be satisfied by evidence that a defendant acted with willful blindness regarding the organization." (internal citations omitted)).

167 18 U.S.C. § 2339B. Chalos, *supra* note 47, at 314; *see also* Lavi, *supra* note 42, at 510–11. FTOs are organizations that the Secretary of State has defined as foreign terrorists. The list of FTOs maintained by the State Department encompasses sixty-one such groups. *See Foreign Terrorist Organizations*, U.S. DEP'T OF STATE, BUREAU OF COUNTERTERRORISM, https://www.state.gov/foreign-terrorist-organizations/ [https://perma.cc/PG55-LPS9].

168 *See* Rachel E. VanLandingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1, 4 (2017).

169 *See* DION-SCHWARZ ET AL., *supra* note 17, at 13.

170 *See id.*

171 *See id.* (citing ELI BERMAN, RADICAL, RELIGIOUS, AND VIOLENT: THE NEW ECONOMICS OF TERRORISM (2009)).

172 *See id.*

173 Chalos, *supra* note 47, at 320–21.

174 Lavi, *supra* note 42, at 510 (discussing Holder v. Humanitarian L. Project, 561 U.S. 1, 7–9 (2010)).

the severe harms that can ensue from terrorist organizations, the Court broadly interpreted "coordination," and determined that "working in coordination with or at the command of FTOs serves to legitimize and further their terrorist means," finding that these actions materially support terrorist organizations.[175]

As previously explored in other research, neither Section 2339A nor 2339B create private, civil causes of action. However, Section 2333 stands in contrast:

> [Section 2333] allows private parties who are nationals of the United States to sue in federal district court and receive treble damages and attorney's fees if they were injured in their "person, property, or business by reason of international terrorism."[176]

This requirement "may be satisfied when an entity recognizes it is supporting a terrorist organization; it needs not be aware that its aid is going to advance a specific terrorist conspiracy."[177]

In the wake of terrorist attacks, victims and their families are left with a troubling reality: they have little chance of bringing those directly responsible to justice in court.[178] Holding those who provide material support to terrorist groups civilly liable may serve a few purposes: "(1) it allows victims and their families to hold anyone in the chain of causation directly accountable, (2) it allows for potentially significant financial recourse, and (3) it encourages banks to think twice about their role in terrorism's causal chain."[179] There is a growing trend to press civil claims against banks.[180] However, even though liability can be imposed on banks for material support,[181] courts are deeply divided over whether Section 2333 allows

---

175 *Id.* at 510–11 (citing *Holder*, 561 U.S. at 30–31).

176 *See id.* at 511; *see also* Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53, 85 (2017); Alexander Tsesis, *Social Media Accountability for Terrorist Propaganda*, 86 FORDHAM L. REV. 605, 621 (2017).

177 Tsesis, *supra* note 176, at 620.

178 *See* Chalos, *supra* note 47, at 307.

179 *Id.* at 305–06 (internal quotations omitted).

180 *See id.* at 305.

181 *See generally* Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287 (E.D.N.Y. 2015), *vacated and remanded*, 882 F.3d 314 (2d Cir. 2018) (for a case where the court imposed liability on a bank for material support. The bank provided funding to Hamas, which used the

for secondary liability based on the theory that a bank aided or abetted an act of terrorism.[182] Courts also disagree on the required degree of fault necessary to assert civil liability under Section 2333(a).[183] Thus, despite the potential benefits of Section 2333 claims, the current framework creates inconsistent civil judgments.[184]

In summary, laws impose obligations and liability on intermediaries to improve the efficiency of policing illegal activities, including terrorist activities. However, such enforcement methods are only as effective as the way in which courts impose them. The war against money laundering is ongoing and can only be won if it becomes difficult to circumvent the laws and regulations relating to anti-money laundering and financing of terrorism. Circumventing traditional intermediaries makes it possible to avoid enforcement for illegal transfers and use funds for terrorist activities. As this Article demonstrates, cryptocurrencies circumvent traditional intermediaries and means of enforcement, and enable the flow of money to support and manage terrorist activities.

II. WHAT ARE CRYPTOCURRENCIES, HOW DO THEY WORK, AND WHAT BENEFITS DO THEY PROVIDE FOR TERRORISTS?

A. Cryptocurrencies

Cryptocurrencies are electronically generated and stored currencies that enable users to trade objects with one another.[185] In 2008, the first and perhaps most well-known cryptocurrency, Bitcoin, was introduced to the world by a "white paper."[186] This first white paper,

---

money for terror attacks between 2000 and 2004. The bank funded several other FTOs in addition to Hamas). *See also* Linde v. Arab Bank, PLC, 384 F. Supp. 2d 571, 571–72 (E.D.N.Y. 2005). It should be noted that in *Linde*, the bank was more than a financial institution and actually cooperated with the FTO. *Linde*, 384 F. Supp. 2d at 584–85.

182 Chalos, *supra* note 47, at 306–07.

183 *Id.* at 307.

184 *Id*. at 308.

185 *See* Jabotinsky, *supra* note 68, at 118.

186 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, SATOSHI NAKAMOTO INST. (Oct. 31, 2008), https://git.dhimmel.com/bitcoin-whitepaper/v/a5f36b332cb6a5fa9e701886f376ac1ac2946d07/ [https://perma.cc/ZF3H-JVED]; *see also* Armin Krishnan, *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations*, 13 J. STRATEGIC SEC. 41, 42 (2020); Saman

entitled "Bitcoin: A Peer-to-Peer Electronic Cash System," was posted online by an unknown author under the pseudonymous name, "Satoshi Nakamoto."[187] As the white paper revealed, the Bitcoin network is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the system's unit of value.[188] It further explained that Bitcoin is an encrypted digital token that can be transferred from one user to the other without requiring a centralized entity to register the transactions.[189] Instead, transactions are recorded in distributed ledger technology ("DLT"), which allows all users to keep track of the registered transactions.[190] As the technology is made out of blocks connecting to each other via an encrypted digital signature, it is called a "blockchain."[191]

The Bitcoin blockchain allows users to transfer Bitcoin tokens and follow the transfers by providing an open ledger.[192] The blockchain is maintained by an online peer-to-peer network—a DLT—"that tracks transactions and maintains a complete history of verified

---

Adhami et al., *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings*, 100 J. ECON. & BUS. 64, 65 (2018); Roee Sarel, *Property Rights in Cryptocurrencies: A Law and Economics Perspective*, 22 N.C. J.L. & TECH. 389, 397–98 (2021).

187 *See* Nakamoto, *supra* note 186.

188 *See* DION-SCHWARZ ET AL., *supra* note 17, at 57 ("Bitcoin, which was launched by the pseudonymous Satoshi Nakamoto in early 2009, is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system.").

189 *See* Sarel, *supra* note 186.

190 *See id.*

191 It should be noted that the original Bitcoin White Paper does not use the specific term blockchain and this term was developed later. *See generally* Nakamoto, *supra* note 186. The White Paper refers to a chain. *Id.* ("The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work."). For overviews and further details on the blockchain technology, and for a detailed explanation of how it works, see DYLAN YAGA ET AL., U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NISTIR 8202: BLOCKCHAIN TECHNOLOGY OVERVIEW (2018), https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf [https://perma.cc/JUR7-M4A9]; Lin William Cong & Zhiguo He, *Blockchain Disruption and Smart Contracts*, 32 REV. FIN. STUD. 1754 (2019). For an overview of Bitcoin in particular, see generally Christian Rueckert, *Cryptocurrencies and Fundamental Rights*, 5 J. CYBERSECURITY, 2019, at 1.

192 *See* Yan Chen, *Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation*, 61 BUS. HORIZONS 567, 569 (2018) ("The Bitcoin blockchain allows users to store and transfer Bitcoins on a peer-to-peer network.").

transactions."[193] Accordingly, and true to the nature of a public blockchain, "[a]ny user of the system can participate in all aspects of its operations, including all transactions, [but] no single participant has control."[194] To maintain anonymity, "Bitcoin transaction participants are identified by a unique string of random numbers rather than by a name or other personal information."[195] The same is true for Ether tokens, another widely-used cryptocurrency that runs on the Etheruem blockchain.[196] The Etheruem blockchain allows users to make use of "smart contracts."[197] Such contracts are basically computer orders which follow the logic of "if x occurs, do y."[198] Other firms use this blockchain as a template to develop and issue their own tokens in a process called an Initial Coin Offering

---

193 *See* DION-SCHWARZ ET AL., *supra* note 17, at ix; ROBBY HOUBEN & ALEXANDER SNYERS, CRYPTOCURRENCIES AND BLOCKCHAIN: LEGAL CONTEXT AND IMPLICATIONS FOR FINANCIAL CRIME, MONEY LAUNDERING AND TAX EVASION 15–16 (2018).

194 *See* DION-SCHWARZ ET AL., *supra* note 17, at 2.

195 *See id.* It should be noted that Bitcoin provides pseudo-anonymity and not overall anonymity. *See* Dmitry Ermilov et al., *Automatic Bitcoin Address Clustering*, 16TH IEEE INT'L. CONF. ON MACH. LEARNING & APPLICATIONS 461, 461 (2017) ("Bitcoins owning and transferring (addresses and transactions) is available as a public ledger called blockchain. But real-world owners of addresses are not known in general. That's why Bitcoin is called pseudo-anonymous. However, some addresses can be grouped by their ownership using behavior patterns and publicly available information from off-chain sources.").

196 *See* Shaanan Cohney & David A. Hoffman, *Transactional Scripts in Contract Stacks*, 105 MINN. L. REV. 319, 335–36 (2020) ("[A] programmer named Vitalik Buterin proposed and developed Ethereum, a blockchain based computing platform, with an associated cryptocurrency, Ether. . . . The protocol's explicit goal was to permit enhanced scripting—more complicated logical operations than recording ownership—on a blockchain."); *see generally* Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger (EIP-150 Revision)*, GAVIN WOOD, http://gavwood.com/Paper.pdf [https://perma.cc/NFX9-5PJB].

197 *Smart Contracts: 10 Use Cases for Business*, AMBISAFE, https://ambisafe.com/blog/smart-contracts-10-use-cases-business/ [https://perma.cc/2LBT-9SMB] ("Smart contracts do not require any intermediaries. Hence, you pay no fees. As there's no bureaucracy involved, transactions become fast and cheap. Moreover, the transparency guaranteed by the blockchain reduces the possible risks of fraud."); *see also* Alexander Savelyev, *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law* 16 (Nat'l Rsch. Univ. Higher Sch. of Econ., Working Paper No. BRP 71/LAW/2016, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 [https://perma.cc/3H7Z-JCWD]; *Ethereum Smart Contract Best Practices*, GITHUB, bit.ly/3oL4KJW [https://perma.cc/G9B6-KZZA]; Cohney & Hoffman, *supra* note 196, at 321 n.9 ("[S]mart contracts are actually meant to replace legal contracts.").

198 *See* Jabotinsky, *supra* note 68, at 138–39.

("ICO"). Anonymity is also maintained for Etheruem blockchain users.[199]

The most recently popularized cryptocurrency was Facebook's initiative: the Diem (previously Libra).[200] The Diem project was meant to launch in 2020, but following regulatory concerns was abandoned in January 2022.[201] Diem—which was supposed to be a global coin designed to replace some fiat currencies—would have allowed users to send money or make purchases with almost zero fees.[202] According to plans, to use Diem, users should have downloaded a wallet application such as Novi, the application Facebook designed for its new currency.[203] This application was meant to be incorporated into WhatsApp and Facebook Messenger,[204] and users of these apps should have formed Diem's user base.[205] This intended token aimed to allow users to exchange fiat currencies (such as USD, EUR, etc.) in return for Diem and exchange the tokens back to fiat currencies when they please.[206] The Diem token was

---

199 *See generally* Sergio Martins & Yang Yang, *Introduction to Bitcoins: A Pseudo-anonymous Electronic Currency System*, *in* PROCEEDINGS OF THE 2011 CONFERENCE OF THE CENTER FOR ADVANCED STUDIES ON COLLABORATIVE RESEARCH 350 (2011).

200 *See* LIBRA WHITE PAPER, *supra* note 70; *see also* Ivan Pupolizio, *From Libra to Diem. The Pursuit of a Global Private Currency*, *in* GLOBAL JURIST (Oct. 8, 2021), https://www.degruyter.com/document/doi/10.1515/gj-2021-0055/html [https://perma.cc/QL8J-U6BT].

201 *See* Romain Dillet, *Facebook Ditches Diem Stablecoin with Asset Sale to Silvergate*, TECHCRUNCH (Jan. 27, 2022, 1:49 PM), https://techcrunch.com/2022/01/27/facebook-reportedly-ditches-diem-stablecoin-with-asset-sale/ [https://perma.cc/8VW9-23HA].

202 *See* Jabotinsky, *supra* note 68, at 146.

203 *See* Pupolizio, *supra* note 200, at 11 ("The proposed governance arrangements of the Libra/Diem project are further complicated by the existence of Novi (formerly known as Calibra), a Facebook subsidiary company designed for creating the digital wallets necessary to use Libra.").

204 *See* Josh Constine, *Facebook Announces Libra Cryptocurrency: All You Need to Know*, TECHCRUNCH (June 18, 2019), techcrunch.com/2019/06/18/facebook-libra/ [https://perma.cc/KQ9W-3ZAX].

205 *See* John Taskinsoy, *This Time Is Different: Facebook's Libra Can Improve Both Financial Inclusion and Global Financial Stability as a Viable Alternative Currency to the U.S. Dollar*, 5 J. ACCT., FIN. & AUDITING STUD., no. 5, 2019, at 67, 71 ("With a user base of close to 3 billion (i.e. Messenger, WhatsApp, Instagram, and Facebook), Facebook's Libra is forecasted to dominate daily transactions for goods/services and money transfers online.").

206 *See* Jahja Rrustemi & Nils S. Tuchschmid, *Facebook's Digital Currency Venture "Diem": The New Frontier . . . or a Galaxy Far, Far Away?*, 10 TECH. INNOVATION MGMT.

supposed to be pegged to a basket of short-term government securities and bank deposits to mitigate the fluctuation usually associated with cryptocurrencies.[207]

Unlike other cryptocurrencies, such as Bitcoin, Ether, and most tokens built on the Ethereum blockchain, Diem was supposed to run on what is known as a "private blockchain," which screens participants upon entrance.[208] The blockchain designed for Diem was intended to be run by the Diem Association members.[209] This means that the ledger of transactions should have been accessible only to them and that they would have had control over who enters the system.[210] Since Diem was supposed to control the entry point to the system, this currency initiative was arguably less decentralized relative to other cryptocurrencies.[211]

ICOs are attractive to entrepreneurs for different reasons, some more legitimate than others. Legitimate reasons might include the fact that issuing tokens, as opposed to stocks, enables entrepreneurs to maintain all of their rights in the corporation without dilution while still raising money, allowing them to reach more investors worldwide, and avoiding costly regulatory demands.[212] For these reasons, the market for ICOs bloomed between 2016 and 2019,[213] raising over $35 billion (USD) from investors worldwide.[214] During

---

REV., Dec. 2020, at 19, 25 ("Facebook will have to set up some sort of system where people in those countries can exchange their national fiat currency from and to Diem.").

[207] *See* Jabotinsky, *supra* note 68, at 146. Cryptocurrencies which are pegged to other assets are also known as "stable coins."

[208] *See* Michele Benedetto Neitz, *The Influencers: Facebook's Libra, Public Blockchains, and the Ethical Considerations of Centralization*, 21 N.C. J.L. & TECH. 41, 44 (2019) ("Private blockchains, also known as permissioned blockchains, limit participation to specific individuals selected by a particular enterprise.").

[209] The Libra Association (now Diem) is an independent membership organization responsible for the governance of the Libra network and the development of the Libra project. *See About Us*, DIEM ASS'N, libra.org/en-US/association/ [https://perma.cc/9K7S-273S].

[210] *See* Neitz, *supra* note 208, at 44.

[211] *See* Jabotinsky & Sarel, *supra* note 26, at 24.

[212] *See* Sarel, *supra* note 186, at 399–400.

[213] *See id.* at 400.

[214] Oksana A. Karpenko et al., *The Initial Coin Offering (ICO) Process: Regulation and Risks*, 14 J. RISK & FIN. MGMT., 2021, at 5 ("In recent years, a new form of funding—ICOs has become widespread. ICOs allow an enterprise to raise funding in exchange for cryptographically secure tokens, which are a means of paying for future projects or

this time, exchanges designated solely for cryptocurrencies and supplying the market with liquidity began to pop up.[215] These exchanges form the marketplace where buyers and sellers of tokens can conduct exchanges.[216]

However, alongside legitimate reasons for issuing tokens, there are illegitimate reasons, including using tokens' anonymity for money-laundering,[217] fraud, tax evasion,[218] Ponzi schemes, and[219] terrorist organization funding.[220]

B. Why and How Are Cryptocurrencies Used by Terrorist Organizations?

Terrorists require significant funding for their operations, propaganda, recruitment, training, salaries, and management.[221] For example, ISIS approved a $2 billion (USD) budget for 2015.[222] Costs of specific attacks range from an estimated $10,000 USD for the 2015 Paris attacks, to $400,000–500,000 USD for the 9/11 attacks.[223] Money fuels terrorist activities; the more funding organizations have, the more they can recruit members, organize schemes, and commit terror attacks. Terrorist groups' sources of revenue and fundraising activities combine traditional and non-traditional methods.[224] These organizations depend on numerous sources of income derived from both criminal activities and legitimate activities that are abused to generate funds.[225] Examples of criminal activities

services. In 2016–2019, over 7400 businesses attempted ICOs, raising a staggering USD 35 billion.").

215 *See* Sarel, *supra* note 186, at 399–400.

216 *See id.* at 400.

217 *See generally* Rolf Van Wegberg et al., *Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin*, 25 J. FIN. CRIME 419 (2018).

218 *See generally* Thomas Slattery, *Taking a Bit Out of Crime: Bitcoin and Cross-Border Tax Evasion*, 39 BROOK. J. INT'L L. 829 (2014).

219 SECS. & EXCH. COMM'N, OFF. INV. EDUC. & ADVOCACY, INVESTOR ALERT: PONZI SCHEMES USING VIRTUAL CURRENCIES, PUB. NO. 153 (July 1, 2013), https://www.sec.gov/files/ia_virtualcurrencies.pdf [https://perma.cc/JB9K-VMQV].

220 *See* Sarel, *supra* note 186, at 400–01.

221 *See* FATF REPORT, *supra* note 8, at 9–10.

222 *See* Goldman et al., *supra* note 16, at 10.

223 *Id.*

224 *Id.*

225 *Id.*

include arms and drug trafficking, kidnapping for ransom, extortion, and racketeering.[226] In addition, terrorist organizations and their associates divert funds from charities, donations, sponsorships, and legal sources such as businesses and personal credit loans to terror.[227]

After generating funds, terrorist organizations must manage their money.[228] If the money received is not yet under the direct control of the terrorist organization, or if it cannot be transferred because of operational security concerns, terrorists may use money laundering and other transfer mechanisms to support the cash needs of their members and associates.[229] Terrorist groups and organizations *spend* the money they generate on salaries, services, and their operations.[230]

1. The Anonymity of Some Cryptocurrencies and Its Importance to Terrorist Activities

Cryptocurrencies are attractive to terrorists, as using anonymous tokens can promote their activities, aid organizational transactions, allow the collection and management of funds, and ultimately the use of the funds collected. Such tokens make it possible to transfer money instantly around the world without using intermediaries, such as banks, as those facilitate greater transparency and are obligated to report suspicious activity in depositors' accounts.[231] Anonymous cryptocurrencies make it possible to hide and protect the identity of the user; "[w]hile the original purchase of the currency may be visible (e.g., through the banking system), all following transfers . . . are difficult to detect."[232]

---

226 *Id.*

227 *Id.*

228 DION-SCHWARZ ET AL., *supra* note 17, at 10.

229 *Id.*

230 *Id.* at 13.

231 On the duty of financial institutions to report suspicious activities, see Matthew R. Hall, Note, *An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report*, 84 KY. L.J. 643, 653 (1995).

232 FATF REPORT, *supra* note 8, at 35.

Admittedly, the anonymity on the blockchain is incomplete[233] and perhaps insufficient for some users,[234] as the degree of anonymity depends on operational and technical factors, allowing transactions to be de-anonymized through a variety of methods.[235] However, such methods of de-anonymization have costs and revealing identities takes time.[236] Moreover, dark wallets, which seek to render de-anonymizing cryptocurrency transactions impossible, disrupt potentially identifying characteristics on the blockchain, enabling illicit financial transactions.[237]

Anonymity in financial transactions is an important aspect of every terrorist's financial activities. First, anonymity is important for *fundraising*.[238] Since it is illegal to provide material support to known terrorist organizations, lack of anonymity serves as a deterrent to donors.[239] Likewise, recipients of funds meant for terrorist operations require anonymity, as being actively involved with raising funds for terrorist organizations or operations is illegal and would, if unmasked, be blocked by authorities.[240] Thus, when cryptocurrencies remain anonymous, it is possible to circumvent the Western banking system, which limits donations for jihad through restrictions on the financial system.[241] Second, anonymity of financial transactions is critical for *illegal drug and arms trafficking.*[242]

---

233 *See* Paul Carroll & James Windle, *Cyber as an Enabler of Terrorism Financing, Now and in the Future*, 13 J. POLICING, INTEL. & COUNTER TERRORISM 285, 288 (2018).

234 *See* Stephan Breu & Theodor G. Seitz, *Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on Economy and Society*, *in* LEGAL IMPACT ON THE ECONOMY: METHODS, RESULTS, PERSPECTIVES (2018).

235 *See* DION-SCHWARZ ET AL., *supra* note 17, at 25; Smith, *supra* note 34; Carroll & Windle, *supra* note 233, at 288 ("Cryptocurrencies provide increased, rather than complete, anonymity as they are added to blockchains which can be used to trace the originating electronic wallet from which the cryptocurrency was sent.").

236 *Cf.* Woodrow Hartzog & Ira Rubinstein, *The Anonymization Debate Should Be About Risk, Not Perfection*, 60 COMMC'N. ACM, no. 5, May 2017, at 22, 24 ("By focusing on process instead of output, data release policy can aim to raise the cost of re-identification and sensitive attribute disclosure to acceptable levels without having to ensure perfect anonymization.").

237 *See* Goldman et al., *supra* note 16, at 15.

238 DION-SCHWARZ ET AL., *supra* note 17, at 32.

239 *Id.* For expansion on the Material Support Statutes, see *supra* part I.A.1.b.

240 DION-SCHWARZ ET AL., *supra* note 17, at 32.

241 *See supra* part I.A.1.

242 DION-SCHWARZ ET AL., *supra* note 17, at 32.

Terrorist organizations require anonymity to avoid detection by the authorities during and after these illegal transactions.[243] Finally, anonymity is highly important for *funding terrorist attacks*.[244] In particular, it is crucial for terrorist organizations that the attacker receiving the money is not detected prior to the operation.[245]

Terrorists can conceal their identities and reduce the risk that their communications and financial activities will be detected. While terrorists have been active on various online platforms for more than two decades, the surface web has turned out to be too risky for anonymity-seeking terrorists, as they can be monitored, traced, and found.[246] However, "the majority of the internet lies below the metaphorical waterline, unsearchable and inaccessible to the general public."[247] The deepest layers of the internet, commonly known as the dark net, "contai[n] content that has been intentionally concealed including illegal and anti-social information."[248] It also allows hidden transfers of funds, using cryptocurrencies that fulfill terrorists' needs for anonymous and secure streams of funding.[249] This trend "is one of the most alarming combinations of organized terrorism and [d]ark [n]et capabilities."[250] Because some cryptocurrencies provide the same form of anonymity in the financial setting as the dark net does for communication systems, cryptocurrencies are susceptible to abuse by terrorists who can utilize them and generate great benefits.[251]

Unlike regular bank transfers and accounts, law enforcement agencies and counterterrorist professionals find it difficult to stop transactions, track cryptocurrency assets, and freeze such assets to disrupt illicit funding.[252] Individuals can store infinite amounts of

---

243 *See id.* at 32–33.

244 *Id.* at 33.

245 *Id.*

246 *See* Weimann, *supra* note 15.

247 The dark web can be accessed by any internet user by using special software such as Tor (short for "The Onion Router") or I2P ("Invisible Internet Project"), tools for anonymously communicating online. *Id.*

248 *Id.*

249 *See id.*

250 *Id.*

251 *See id*.

252 *See* Krishnan, *supra* note 186, at 44–45.

information in their heads simply by memorizing a private key that gives access to funds on the blockchain, or by just writing this sequence on a piece of paper and keeping it.[253] This makes it difficult to enforce capital controls over cryptocurrencies. Terrorists can raise funds through cryptocurrency donations from anyone and anywhere in the world by publishing their public cryptocurrency key on a website, thereby avoiding relying on third-party intermediaries.[254] For example, this makes it possible to exploit the Bitcoin system for crowdfunding campaigns that enable terrorist activities.[255] Such illicit funding networks are hard to disrupt.[256] Technology makes it easier to use and access cryptocurrencies and the dark web and provides terrorists with more opportunities to fundraise, operate, and commit illicit operations, all while evading detection by authorities.[257] Consequently, national security threats grow.[258]

a) The Problem of Counter Terrorism Financing in Cryptocurrencies

Public blockchains use peer-to-peer networks that are autonomously managed.[259] Information on the blockchain is secured and decentralized, without encountering the compliance regulations of the established financial system.[260] As a result, it is difficult for law enforcement and security organizations to identify users on the blockchain.[261] Various regulators and legislators have identified cryptocurrencies' tremendous risks and their potential to undermine the successes of counter terrorism financing ("CTF").[262] Accordingly, "since May 2017, a U.S. congressional subcommittee has been developing a bill to study the use of digital currencies by

253 *See id.* at 45.
254 *See id.* at 45 (giving an example of ISIS, which reportedly solicited donations by posting a Bitcoin address).
255 *See generally* Smith, *supra* note 34.
256 *See* Carroll & Windle, *supra* note 233, at 293.
257 *See* Weimann, *supra* note 15.
258 *See* Carroll & Windle, *supra* note 233, at 296–97.
259 *See* Breu & Seitz, *supra* note 234.
260 *See id.*
261 *See* Carroll & Windle, *supra* note 233, at 300–01.
262 *See* DION-SCHWARZ ET AL., *supra* note 17, at 3.

[t]errorists."[263] In January 2018, a Financial Technology Innovation and Defense bill was introduced in Congress, aiming to establish an Independent Financial Technology Task Force.[264] Section 2 provides that Congress seeks to "prioritize the investigation of terrorist and illicit use of new financial technology, including digital currencies," among other provisions.[265] Other bills also aim to promote the analysis of the use of virtual currencies by terrorists.[266]

In addition, the Financial Crimes Enforcement Network ("FinCEN") declared that it "regards developers as well as exchanges of [virtual currency] as 'money transmitters' for the purposes of the US Bank Secrecy Act."[267] FinCEN is the authority in charge of combating money laundering and terrorism financing through the financial system.[268] It does so through laws such as the Bank Secrecy Act, which it supplements with instructions regarding registration with FinCEN and the management of accounts.[269] Among others, it

---

263 *See* Breu & Seitz, *supra* note 234, n.6 ("[At the] 115th Congress 1st Session Miss Kathleen Rice from New York introduced the following bill to direct the Under Secretary of Homeland Security for Intelligence and Analysis to develop and disseminate a threat assessment regarding terrorist use of virtual currency: "Homeland Security Assessment of Terrorists Use of Virtual Currencies Act.").

264 *See* DION-SCHWARZ ET AL., *supra* note 17, at 3–4 n.9; *see also* Financial Technology Innovation and Defense Act, H.R. 4752, 115th Cong. (2018) ("To establish an Independent Financial Technology Task Force, to provide rewards for information leading to convictions related to terrorist use of digital currencies, to establish a FinTech Leadership in Innovation Fund to encourage the development of tools and programs to combat terrorist and illicit use of digital currencies, and for other purposes.").

265 *See* DION-SCHWARZ ET AL., *supra* note 17, at 3–4 (referring to the Financial Technology Innovation and Defense Act, H.R. 4752, 115th Cong. (2018)). It should be noted that there are other regulatory issues relating to cryptocurrencies such as investor protection and prevention of fraud. These issues have also taken time to be resolved and are still in an ongoing process. For example, in April 2019 the SEC finally issued its long-awaited framework for "investors contract" analysis of digital assets. *Framework for "Investment Contract" Analysis of Digital Assets*, SECS. & EXCH. COMM'N (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets [https://perma.cc/9LXK-W7T5].

266 *See, e.g.*, Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act, H.R. 428, 116th Cong. (2019); *see also* JAY B. SYKES & NICOLE VANATKO, CONG. RSCH. SERV., R45664, VIRTUAL CURRENCIES AND MONEY LAUNDERING: LEGAL BACKGROUND, ENFORCEMENT ACTIONS, AND LEGISLATIVE PROPOSALS 12 (2019).

267 Blake Hamil, Note, *EU Cryptocurrency Regulation: Creating a Haven for Businesses or Criminals?*, 48 GA. J. INT'L. & COMPAR. L. 833, 837–38 (2020).

268 *Id.* at 838.

269 *Id.*

requires money transmitters to have risk-based KYCs and anti-money laundering programs, in addition to reporting suspicious transactions.[270] In a 2018 letter, FinCEN made clear that virtual currency exchanges and administrators are considered "money services businesses" and are therefore subject to the same requirements.[271] The European Banking Authority also classified terrorists' use of cryptocurrencies as a high priority risk.[272]

During 2017 and 2019, regulators around the world began imposing regulations on ICOs in an attempt to protect investors and prevent illegal use of tokens.[273] Some countries, such as South Korea and China, went as far as banning ICOs altogether.[274] South Korea banned all forms of cryptocurrency-based fundraising activities and announced steps to marginalize cryptocurrency trading.[275] China deemed ICOs entirely illegal.[276] In September 2017, the most important cryptocurrency exchanges in China announced they would "voluntarily halt trading until further reports of government interventions are publicly announced."[277]

Shortly after China's announcement, the Swiss Financial Markets Supervisory Authority announced it was investigating a number

---

[270] *Id.*

[271] *See* DEP'T OF TREASURY, FIN. CRIMES ENF'T NETWORK, GUIDANCE ON APPLICATION OF THE DEFINITION OF MONEY TRANSMITTER TO BROKERS AND DEALERS IN CURRENCY AND OTHER COMMODITIES (2008), https://www.fincen.gov/sites/default/files/guidance/fin-2008-g008.pdf [https://perma.cc/TKT8-LTQ6].

[272] *See* Breu & Seitz, *supra* note 234, n.2 ("Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03). The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across the globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high." (quoting European Banking Authority [EBA], *EBA Opinion on Virtual Currencies*, at 33, EBA/Op/2014/08 (July 4, 2014))).

[273] *See,, e.g.*, Council Directive 2018/843, 2018 O.J. (L 156) (EU). For other reforms discussed in this Article, see *infra* Part III.A.

[274] *See* Breu & Seitz, *supra* note 234; Adhami et al., *supra* note 186, at 67.

[275] *See* Breu & Seitz, *supra* note 234.

[276] *See id.*; *see also China Widens Ban on Crypto Transactions; Bitcoin Tumbles*, BLOOMBERG, https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown [https://perma.cc/9TER-4LML] (Sept. 24, 2021, 9:16 AM).

[277] *See* Breu & Seitz, *supra* note 234.

of ICOs for breaching anti-money laundering and terrorism financing provisions, among other regulations.[278] Recently, Canada's federal government has invoked, for the first time, its Emergencies Act. Under the Emergencies Act, crowdfunding platforms and payment services (including crypto) which are linked to them must now register with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC").[279] This is an attempt to broaden anti-money laundering and terror financing rules so that they cover all sorts of payment systems, including crypto.[280]

Yet despite these regulatory initiatives, regulatory uncertainty still dominates the market; regulators and courts around the world have yet to come up with a coherent solution to prevent money laundering and financing of terrorism through cryptocurrencies.[281]

Indeed, a key task of the policy enforcement, intelligence, and financial regulatory communities must be to prevent terrorist groups from using cryptocurrencies on a large scale.[282] However, regulation should not ban ICOs altogether, "throwing the baby out with the bathwater" and relinquishing the tremendous benefits of cryptocurrencies. Instead, this Article proposes to focus on the illicit activities and design identification and verification mechanisms that could be embedded into technology to unmask illicit actors who abuse cryptocurrencies for illegal operations. This Article argues that the broad anonymity in cryptocurrencies makes it easier for terrorists and criminals to use cryptocurrencies for illicit purposes. It proposes to consider the scope of anonymity in cryptocurrencies and outlines ways to narrow the anonymity. Narrowing the scope of anonymity

---

[278] *See id.* (citing *FINMA Is Investigating ICO Procedures*, FIN. MKT. SUPERVISORY AUTH. (Sept. 29, 2017), www.finma.ch/en/news/2017/09/20170929-mm-ico/ [https://perma.cc/XW46-RFAG]).

[279] Sebastian Sinclair, *Crypto Payment Systems Face New Restrictions Under Canada's Blockade Crackdown*, BLOCKWORKS (Feb. 14, 2022, 8:05 PM), https://blockworks.co/crypto-payments-firms-face-new-restrictions-under-canadas-blockade-crackdown/ [https://perma.cc/R8FH-MN9B].

[280] *Id*.

[281] *See, e.g.*, Council Directive 2018/843, 2018 O.J. (L. 156) (EU) (mandating that crypto exchanges and custodial wallet providers adhere to the same regulatory requirements as banks and other financial institutions); The Payment Services Act 2019 (Sing.) (requiring that anyone issuing a cryptocurrency adhere to Anti-Money Laundering regulation and fill in a KYC on all people buying the token from the issuing firm).

[282] *See* Goldman et al., *supra* note 16, at 2.

will allow to fight more efficiently against money laundering and financing of terrorism via cryptocurrencies.[283]

b) Terrorists Adopting Cryptocurrencies: Current Limitations and the Future

As this Article demonstrates, anonymous cryptocurrencies can be attractive to terrorists; however, terrorists have yet to adopt cryptocurrencies on a large scale.[284] This is likely due to cryptocurrencies' instability[285]—by using cryptocurrencies, terrorist organizations are exposed to unwanted uncertainty. Another reason for the limited use is that such tokens diminish terrorist leaders' ability to exercise control over funds entrusted to agents.[286] In addition, difficulties associated with exchanging cryptocurrencies into fiat currencies persist.[287] Finally, technical communication tools (such as internet reception) are difficult to penetrate in some geographical areas where terrorist organizations also affect the scale of adoption.[288] After all, if a terrorist organization cannot easily exchange cryptocurrencies for large quantities of fiat currency or easily use them to purchase weapons, food, housing in the areas where they operate, and other necessary materials, these currencies do not contribute to their operations.[289]

In the future, however, cryptocurrencies' utility will likely grow as both terrorist methods and technologies develop. Cryptocurrencies are expected to become sufficiently liquid and convertible.[290] Such expected advances could facilitate the use of cryptocurrencies for all users, allowing terrorist groups and organizations to engage

---

283 *See* HOUBEN & SNYERS, *supra* note 193, at 11.

284 *See* Goldman et al., *supra* note 16, at 2.

285 DION-SCHWARZ ET AL., *supra* note 17, at 30.

286 *See* Krishnan, *supra* note 186, at 45.

287 *See* Carroll & Windle, *supra* note 233, at 289.

288 *See* Goldman et al., *supra* note 16, at 6; *see also* Carroll & Windle, *supra* note 233, at 291.

289 *See* Goldman et al., *supra* note 16, at 6 ("This is true, for example, of al Qaeda in the Islamic Maghreb (AQIM) in the Sahel, Al Qaeda in the Arabian Peninsula (AQAP) in Yemen, and, in some measure, ISIS in Iraq and Syria."); *see also id.* at 27 ("If the areas in which these groups operate lack the basic technical and telecommunications infrastructure for their ecosystems to support the use of Bitcoin, then there is no reason for terrorist groups to accept value from outside donors in that form.").

290 *See id.* at 2.

in transnational fundraising and plan vast terror operations and attacks. Thus, one should not underestimate the future risks to national security flowing from terrorists' use of cryptocurrencies.

III. SPEAK OUT: THE CASE FOR EX ANTE VERIFICATION AND VALIDATION OF CRYPTOCURRENCY USER IDENTITY

The growing trend of using anonymous cryptocurrencies for terrorist purposes makes it significantly more important to identify the users behind the tokens.[291] The anonymity offered by some cryptocurrencies is one of the biggest problems in combating money laundering and terrorism financing, as it prevents cryptocurrency transactions from being adequately monitored. This lack of monitoring leaves room for "shady transactions to occur outside of the regulatory perimeter," and enables terrorist organizations "to use cryptocurrencies to obtain easy access to 'clean cash.'"[292]

Researchers have recommended considering a system of mandatory user registration.[293] However, "financial regulatory officials have not devoted . . . adequate resources to regulating and examining non-bank financial institutions."[294] With respect to unveiling the anonymity of users, no immediate action has been taken and, in some jurisdictions, there is no mandatory obligation to register and validate the identity of cryptocurrency users.[295]

At the time of writing this Article, regulatory oversight in the United States is limited to KYC measures, which only partially reduce the anonymity built into cryptocurrency systems by making it difficult to obtain cryptocurrencies anonymously on an exchange.[296]

---

291 *See* HOUBEN & SNYERS, *supra* note 193, at 53.

292 *See id.*

293 *See id.* at 14.

294 Goldman et al., *supra* note 16, at 30.

295 *See* HOUBEN & SNYERS, *supra* note 193, at 9.

296 *See, e.g.*, Shahla Hazratjee, *Bitcoin: The Trade of Digital Signatures*, 41 T. MARSHALL L. REV. 55, 76 (2015); DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, GUIDANCE ON APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [https://perma.cc/8NQY-LMC4].

As mentioned earlier, KYC measures place an obligation on financial intermediaries to become familiar with their clients.[297] The main reason behind this requirement is that the financial intermediary needs to be able to identify unusual transactions in the client's account and report them to the anti-money laundering authorities or the police.[298] Requiring a KYC from people receiving cryptocurrencies on an exchange is a first measure, but it is not at all sufficient to completely block illicit transactions.[299] People trading cryptocurrencies on exchanges sometimes only make a single transaction on an exchange and records from the exchange alone may be insufficient.[300] This means that the exchange is not familiar with their usual trade patterns in virtual assets and likely cannot detect what seems to be irregular cryptocurrency activity.

Since cryptocurrencies are not restricted to a geographical setting, if exchanges operating in the United States or the European Union become too nosy about the identity of the client, terrorists and other criminals might simply use an exchange operating in a different jurisdiction that does not require a KYC.[301] Lastly, KYC requirements on exchanges will not prevent funding at the ICO stage, because during the ICO, people usually do not purchase the token through an exchange but rather pay the issuing firm directly with a credit card.[302] Thus, funds can be collected by terrorists or criminals directly from the public; they can purchase the token in an ICO, and then use it on the dark net to purchase weapons and other equipment

---

297 *See* Christian Leuprecht et al., *Tracking Transnational Terrorist Resourcing Nodes and Networks*, 46 FLA. ST. U. L. REV. 289, 310–11 (2019).

298 *See* Will Kenton, *Anti Money Laundering (AML)*, INVESTOPEDIA, https://www.investopedia.com/terms/a/aml.asp [https://perma.cc/G48E-DCYP] (Mar. 16, 2022).

299 *See* Scott D. Hughes, *Cryptocurrency Regulations and Enforcement in the U.S.*, 45 W. ST. L. REV. 1, 5 (2017) ("Bitcoin transactions are not facilitated within a consumer protection framework and measures, such as anti-money laundering (AML) or know-your-customer (KYC) policies, are not inherent to the system. Once a transaction is sent, there is no way to perform a chargeback.").

300 Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DEP'T JUST. J. FED. L. & PRAC. 233, 250 (2019).

301 *See* Olly Jackson, *Cryptocurrency Exchanges Avoiding the US Due to Confusing Regulation*, INT'L FIN. L. REV. (Apr. 9, 2018).

302 For a proposal to develop a compliant-by-design blockchain-based KYC system that is integrated into the investment flow of an ICO, see Nadine Kathrin Ostern & Johannes Riedel, *Know-Your-Customer (KYC) Requirements for Initial Coin Offerings*, 63 BUS. INFO. SYST. ENG'G 551, 552 (2021).

needed to commit crimes and attacks.[303] This means that the regulatory oversight, however, is limited:

> In the United States, oversight does not cover non-exchange transactions, such as those brokered by localbitcoins.com, and does not cover fully on-blockchain transactions that occur outside of a regulated entity, such as trading one cryptocurrency for another.[304]

It is for this reason, among others, that the Biden administration intends to deepen the regulatory demands and issue a presidential order to address the challenges posed by cryptocurrencies.[305]

A. Proposed Reform for Verifying, Validating, and Unmasking Cryptocurrency User Identity

This juncture—when terrorists are beginning to discover cryptocurrencies' benefits to commit terror attacks—is precisely the time to consider whether anonymous tokens are truly necessary.[306] This is the key issue that needs to be addressed in the fight against money laundering and terrorism financing via cryptocurrencies.[307] This Part proposes a mandatory obligation on wallet providers, exchanges, and firms issuing new tokens to identify the cryptocurrency users on the blockchain. This identification would be anonymized and not available for all to see. However, law enforcement agencies could

---

303 Weimann, *supra* note 15 ("Terrorists too can use the Dark Net for fundraising, money transfers and illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies.").

304 DION-SCHWARZ ET al., *supra* note 17, at 49. For information on localbitcoins.com, see *Buy and Sell Bitcoins Everywhere*, LOCALBITCOINS.COM, https://localbitcoins.com/ [https://perma.cc/STL5-SN2X].

305 *See* Exec. Order No. 14067 Fed. Reg. 05471 (Mar. 14, 2022); Hadar Y. Jabotinsky, Roee Saral, *When Biden Met Crypto: Thoughts on the President's Executive Order*, BLUE SKY BLOG (Apr. 1, 2022), https://clsbluesky.law.columbia.edu/2022/04/01/when-biden-met-crypto-thoughts-on-the-presidents-executive-order/ [https://perma.cc/FUZ9-W7AF]; *US Executive Order on Crypto: What Does It Mean?*, ECON. TIMES, https://economictimes.indiatimes.com/markets/cryptocurrency/us-executive-order-on-crypto-what-does-it-mean/articleshow/90373461.cms [https://perma.cc/83C9-JXAR] (Mar. 22, 2022).

306 *See* HOUBEN & SNYERS, *supra* note 193, at 10.

307 *See id.* at 11 ("[M]andatory registration and a pre-set date as of which it applies would be a better approach to unveil the anonymity of cryptocurrency users.").

request wallet providers, exchanges, and issuing firms to "speak out" and unmask the identities of cryptocurrency users and holders when there is probable cause to suspect illegality in their activities. Our suggestion is not that blockchain transactions be exposed by name to everyone, but rather that the firms issuing cryptocurrencies be permitted to sell them only to clients individually screened via a KYC.

In addition, all new users of the token (those buying from users who purchased the token at an ICO) will have to identify themselves to the firm that issued the token. This way, if a money laundering activity is detected, the identity of the people behind the wallets can be revealed to authorities. Both the Diem token and the non-anonymous digital tokens issued by Saga are examples of this idea.[308] Both of these tokens were designed to create international tokens that would replace fiat currencies in part and enable global transactions.[309] Ideally, everyone entering the blockchain to purchase one of these tokens would have been required to identify themselves to the corporation issuing the token.[310] This would mean that at any given time, the issuing firm or institution would have a registrar of all blockchain users and could assist authorities in combating money laundering and terrorism financing.

In fact, this suggestion is currently mirrored in part by the 5th European Anti-Money Laundering Directive ("5AMLD"), which was legislated on May 30, 2018, [311] and took effect in January

---

[308] Saga (now "Sogur") was a non-anonymous digital currency which sought to complement existing national currencies, by working closely with established economic institutions. To read more about the Saga initiative, see *The Closure of Sogur*, SOGUR, https://www.sogur.com/ [https://perma.cc/N7PW-GMDE].

[309] Rrustemi & Tuchschmid, *supra* note 206, at 21.

[310] Identification can be conducted via video conferencing by having a KYC conversation with potential users during which they would also hold up identification documents such as an ID and a passport or a video KYC. *See* Emily Daniel, *Video KYC Onboarding: Fintechs Meeting KYC Compliance with Video Identifications*, SHUFTIPROBLOG (Feb. 24, 2020), https://shuftipro.com/blog/video-kyc-onboarding/ [https://perma.cc/3LHA-N8LF]. Another method, practiced by Saga, is using a selfie taken by the client while also holding a written sentence provided exclusively to him/her by Saga together with an identification document. *See* Steve Cook, *Selfie Banking: Is It a Reality*?, BIOMETRIC TECH. TODAY, Mar. 2017, at 9, 9–11.

[311] Council Directive 2018/843, 2018 O.J. (L 156) (EU).

2020.[312] This Directive is designed to achieve greater transparency in financial transactions to prevent money laundering and terrorism financing.[313] This is the first time a directive has covered cryptocurrency transactions, since it applies to crypto service providers such as virtual-fiat exchanges and crypto wallet providers.[314] According to the 5AMLD fact sheet: "[t]he rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies."[315] It further specifies that the law will increase transparency as to the real ownership of legal entities and provide EU authorities with valuable information to help tackle terrorist financing risks linked to the use of anonymous tokens.[316]

Moreover, on July 20, 2021, the European Commission presented legislative proposals to strengthen the EU's Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") rules. Accordingly, anonymous crypto asset wallets will be prohibited. The regulation compares such wallets to anonymous bank accounts which are already prohibited. Thus, fully applying EU AML/CFT rules to the crypto sector.[317]

---

312 Adriana M. Baranello, Comment, *Money Laundering and the Art Market: Closing the Regulatory Gap*, 45 SETON HALL LEGIS. J. 695, 730 (2021) ("The European Parliament passed 5AMLD in 2018, and it took effect on January 10, 2020.").

313 *See, e.g.*, Matt Taylor, *The Five Main Impacts of 5AMLD Regulation for Financial Institutions*, CONSULTANCY.UK (June 27, 2017), https://www.consultancy.uk/news/13624/the-five-main-impacts-of-5amld-regulation-for-financial-institutions [https://perma.cc/2625-BQQ7]; Dominic Kavakeb, *Patchy Progress in Setting Up Beneficial Ownership Registers in the EU*, GLOB. WITNESS (Mar. 20, 2020), https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/5amld-patchy-progress/ [https://perma.cc/QU25-F84J].

314 *See* Council Directive 2018/843, art. 1(2)(d)(19), 2018 O.J. (L 156) (EU) ("'[C]ustodian wallet provider' means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.").

315 VĚRA JOUROVÁ, EUR. COMM'N, STRENGTHENED EU RULES TO PREVENT MONEY LAUNDERING AND TERRORISM FINANCING (July 9, 2018), https://ec.europa.eu/info/files/factsheet-main-changes-5th-anti-money-laundering-directive_en [https://perma.cc/VKP8-R78F].

316 *See id.*

317 *Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules*, EUR. COMM'N (July 20, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690 [https://perma.cc/TX6Y-SJ5L] ("In addition, anonymous crypto asset wallets will be

In the United States, Congress recently also initiated expansion of cryptocurrency exchanges' obligations. The Anti-Money Laundering Act of 2020, passed by Congress in early 2021, broadened the Bank Secrecy Act's definition of "financial institution" to cover businesses that exchange cryptocurrencies.[318] Accordingly, exchanges should verify the identity of their consumers, develop customer risk profiles, and monitor transactions to submit suspicious activity reports.[319] This new regulation, however, focuses on exchanges.

As noted,[320] recently, President Biden signed the Infrastructure Investment and Jobs Act.[321] Accordingly, cryptocurrency asset exchanges and custodians would need to collect information from their customers, and keep track of the holding period and the buy and sell prices of the digital assets in its customer's accounts.[322] Companies that receive, or may in the future receive, payments in cryptocurrency, of over $10,000 (USD) worth, would need to file an IRS form upon the receipt of cryptocurrency.[323]

On October 15, 2021, the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury, published a more extensive Sanctions Compliance Guidance for the Virtual Currency Industry.[324] OFAC's compliance obligations apply equally to transactions involving virtual currencies as well as to those involving traditional fiat currencies. As stated in the guidance: "[m]embers of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related

---

prohibited, fully applying EU AML/CFT rules to the crypto sector."); Ramin Farinpour, *A Snapshot of Recent Developments Regarding EU Counterterrorism Policies and Legislation*, 22 ERA F. 363, 369 (2021).

318 William M. Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6003(5), 134 Stat. 3387, 4548 (2021).

319 31 C.F.R. § 1010 (2020). For further information, see Kirkpatrick et al., *supra* note 65.

320 *See supra* note 60 and accompanying text.

321 Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021).

322 *See* Jacobs et al., *supra* note 61.

323 *Id.*

324 OFF. FOREIGN ASSET CONTROL, SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY 1 (2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf [https://perma.cc/JK4M-75DP].

transactions."[325] Accordingly: "[a]ll companies in the virtual currency industry, including technology companies, exchangers, administrators, miners, and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers, are encouraged to develop, implement, and routinely update, a tailored, risk-based sanctions compliance program."[326] The Guidance further provides best practices such as management's commitment to a "company's sanctions compliance program";[327] risk assessment to the exposure to OFAC sanctions and steps taken to minimize their risks;[328] and implement internal controls including obtaining information about customers (KYC). The KYC should be taken "during onboarding and throughout the lifecycle of the customer relationship and use such information to conduct due diligence sufficient to mitigate potential sanctions-related risk."[329] While many digital currency companies will be able to build out a compliance program that satisfies OFAC under the framework provided in this Guidance, aspects of the Guidance need more clarity as to how they may apply to Decentralized Autonomous Organizations ("DAOs"),[330] especially as these DAOs play a critical role in the new evolving industry of non-fungible tokens ("NFTs").[331]

This Article takes the idea of unveiling anonymity one step further: it argues that the firms issuing the tokens should also be obligated to unmask the identity of their clients by requiring a KYC from anyone entering their blockchain and using their token.

---

325 *Id*.

326 *Id*. at 10.

327 *Id.* at 11.

328 *Id.* at 12.

329 *Id.* at 14.

330 Steven Merriman et al., *OFAC Releases New Detailed Guidance for the Digital Currency Industry*, JD SUPRA (Oct. 20, 2021), https://www.jdsupra.com/legalnews/ofac-releases-new-detailed-guidance-for-5887592/ [https://perma.cc/2E5V-EV43].

331 Hadar Y. Jabotinsky & Michal Lavi, NFT for Eternity (2022) (unpublished manuscript) (on file with author).

B. Unmasking and the Fourth Amendment After Carpenter*: The Need for Court Warrant*

As previously mentioned, this Article proposes that cryptocurrency wallet providers, issuers of new cryptocurrencies, and exchanges should "speak out" and unmask the identity of their users when law enforcement and intelligence agencies require this information for their investigations. The following Subsection will explain that in light of the recent Supreme Court decision in *Carpenter v. United States*,[332] government agencies cannot compel wallet providers, issuers of new cryptocurrencies, or exchanges to unmask and turn over an internet user's identifying records without a warrant. A warrant requirement is desirable, as it safeguards the legitimate privacy interests of users, while allowing law enforcement and intelligence agencies to conduct investigations and enforce the law.[333] Without a warrant, courts are likely to conclude that regulations for unmasking cryptocurrency user identities are unconstitutional under the Fourth Amendment,[334] and therefore would likely strike it down.

1. The Fourth Amendment: Reasonable Expectations of Privacy

The Fourth Amendment is "at the heart of American democracy."[335] It is key in protecting U.S. citizens against governmental power[336] and ensuring that the government cannot gather information about citizens without proper oversight and limitations.[337] It requires the government put forth a compelling reason for its interest

---

[332] 138 S. Ct. 2206, 2220 (2018) (accessing historical records containing physical locations of cellphones necessitates a search warrant).

[333] *Id.* at 2213–14; Evan Caminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 441 (2019).

[334] U.S. CONST. amend. IV.

[335] Travis Panneck, Note, *Incognito Mode Is in the Constitution*, 104 MINN. L. REV. 511, 537 (2019).

[336] *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727 (2020) (explaining that the American constitutional system has no explicit constitutional right to privacy, however, it protects individuals against governmental violations of privacy). For further elaboration on this point, see DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 93 (2011).

[337] *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1513, 1529 (2010).

in personal information.[338] Government officials are required to obtain warrants supported by probable cause before they can place individuals under surveillance or search them.[339] In other words, the government needs to demonstrate reasonably trustworthy information that the government's search will uncover evidence of illegality.[340] If the government fails to follow these procedures, the information will be excluded from trial.[341] Warrant obligations lead to better decisions regarding searches, as they raise awareness of the consequences of searches and obligate authorities to express their reasoning.[342]

The Fourth Amendment uses the terms "*searches and seizures*" to cover everything from rummaging through people's papers to trespassing.[343] However, technology has challenged this approach.[344] At first, in *Olmstead v. United States*, the Supreme Court held that wiretaps do not violate the Fourth Amendment since they do not involve entry upon premises.[345] Yet, in the 1967 case *Katz v. United States*, the Supreme Court narrowed the permissible scope of surveillance under the Fourth Amendment and declared *Olmstead* a mistake.[346] Whereas the Court previously applied the Fourth Amendment only to physical trespass, it now declared that the Fourth Amendment extends to "people, not places."[347] The current approach to Fourth Amendment application thus emerged from Justice Harlan's concurring opinion in *Katz*.[348] Accordingly, the Fourth Amendment should regulate whenever a person exhibits an "actual (subjective) expectation of privacy . . . that society is prepared to

---

338 *See* SOLOVE, *supra* note 336.

339 *See id.* at 95.

340 *See id.*

341 *See id.* at 95–96.

342 *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1642 (2012).

343 *See* SOLOVE, *supra* note 336, at 96.

344 *See id.*

345 277 U.S. 438, 466 (1928); *see also* SOLOVE, *supra* note 336, at 98 (explaining that this decision enabled the government to gather a lot of private information).

346 389 U.S. 347, 353, 359 (1967) (ruling that warrantless electronic bugging in a public telephone booth is unconstitutional).

347 *Id.* at 351.

348 *See* SOLOVE, *supra* note 336, at 99.

recognize as 'reasonable.'"[349] This approach is the "reasonable expectation to privacy test."[350] The goal of this test is "to permit the Fourth Amendment to respond to changing technology."[351]

2. The Third-Party Doctrine: No Reasonable Expectation to Information Held by Third Parties

A prominent exception to the reasonable expectation of privacy test outlined in *Katz v. United States*, is the third-party doctrine: a constitutional rule that permits the state to access business records and transactional data about a company's consumers without constituting a Fourth Amendment "search."[352] If information is possessed or known by third parties, then for the purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information.[353]

This doctrine was crafted by the Supreme Court in the 1970s.[354] In *United States v. Miller*, law enforcement officials sought the financial records of bank customer Mitch Miller, issuing subpoenas to his bank to obtain "all records of [his] accounts."[355] Without advising Miller, the bank turned over his incriminating records to the

---

349 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

350 *See* SOLOVE, *supra* note 336, at 99. Justice Harlan's concurrence was later adopted by the Court in full in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (using Justice Harlan's two-step formulation to frame the Fourth Amendment analysis that includes subjective expectation of privacy and objective reasonableness of such expectation). For further information, see Panneck, *supra* note 335, at 519–20. *See also* Amitai Etzioni, *iPhone vs. Trump: How Technology Companies Can Protect Both Customers and National Security*, NAT'L INT. (Jan. 19, 2020), https://nationalinterest.org/feature/iphone-vs-trump-how-technology-companies-can-protect-both-customers-and-national-security [https://perma.cc/4RAE-6KH8].

351 *See* SOLOVE, *supra* note 336, at 99.

352 *Katz*, 389 U.S. at 351. *See also* SOLOVE, *supra* note 336, at 102. For an overview on the background of the doctrine, its justifications, and further expansion, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV 561, 566–70 (2009); Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 206 (2015).

353 *See* Kerr, *supra* note 352, at 564 (arguing that the third-party doctrine actually prevents technology from giving a leg up to the criminals and makes it possible to level the playing field). For criticism of such approach, asserting that it gives too much power surveillance power to the government vis-à-vis innocent citizens, see SOLOVE, *supra* note 336, at 109.

354 *See* SOLOVE, *supra* note 336, at 103.

355 425 U.S. 435, 437 (1976). For further information, see SOLOVE, *supra* note 336, at 104; Panneck, *supra* note 335, at 521–22.

government.[356] Miller argued that, under the Fourth Amendment, the government was required to obtain a warrant before receiving the records.[357] Holding that Miller had no reasonable expectation of privacy regarding the bank records, the Court explained that Miller had "voluntarily conveyed" the records to the bank and that the information was "exposed to their employees in the ordinary course of business."[358] From this holding, the Court thus "extended the third-party doctrine beyond conversations to encompass business records."[359]

Three years later, the third-party doctrine was further expanded in *Smith v. Maryland*.[360] The Supreme Court held that the Fourth Amendment did not apply to pen registers—devices that record the phone number a person dials for outgoing calls[361]—denying a reasonably subjective or objective expectation of privacy in such cases.[362] The Court concluded that since people expose their phone numbers to phone companies who have the capacity to record information, customers assume the risk that the numbers dialed will be turned over to the police.[363] Thus, the information is not protected by the Fourth Amendment.[364] Therefore, the Fourth Amendment does not protect bank transactions, dialed phone numbers and contacts, or other records maintained by third parties.[365] Scholars have criticized the third-party doctrine for failing "to comprehend the concept of confidentiality—as well as the concept of a promise."[366]

---

356 *Miller*, 425 U.S. at 438.

357 *Id.* at 441.

358 *Id.* at 442.

359 *See* Panneck, *supra* note 335, at 521–22.

360 442 U.S. 735, 742–44 (1979) (a pen register revealing a telephone number dialed from the defendant's home was not within the Fourth Amendment's scope); SOLOVE, *supra* note 336, at 104.

361 *Smith*, 442 U.S. at 745–46; Panneck, *supra* note 335, at 522.

362 SOLOVE, *supra* note 336, at 104 ("These cases form the backbone of the third party doctrine. If any information is exposed to a third party, then there's no reasonable expectation of privacy in it.").

363 *Smith*, 442 U.S. at 745.

364 *Id.* at 745–46. *See also* Panneck, *supra* note 335, at 522–23; SOLOVE, *supra* note 336, at 104.

365 *See* SOLOVE, *supra* note 336, at 104–05.

366 *Id.* at 108 (explaining that if a bank promises confidentiality, the consumer expects the bank to keep this promise and there should be a reasonable expectation of privacy). For

As the following Subsection explains, the Supreme Court recently called the third-party doctrine into question and has, in fact, narrowed it substantially.

3. Shifting the Approach to the Third-Party Doctrine: *Carpenter v. United States*

"[T]he role of courts is to protect the balance of power between the state . . . and the people, refusing to let technological change eviscerate individual privacy and security from the state."[367] The Supreme Court's decision in *Carpenter v. United States*[368] "presents a new way forward that safeguards legitimate privacy interests," while maintaining law enforcement's ability to police bad actors.[369]

In *Carpenter*, the Court held that law enforcement officials may not collect historical cell site location information ("CSLI") from a cell phone service provider without a warrant showing probable cause.[370] The majority opinion declined to extend the third-party doctrine to the FBI's collection of seven days' worth of CSLI from cell phone service providers.[371] Thus, it reinvented the "reasonable expectation of privacy"[372] and narrowed the third-party doctrine.[373] The majority opinion extends beyond location information;[374] it addresses information that law enforcement authorities can use to locate people generally, not just through CSLI specifically.[375] Although the Court in *Carpenter* expressly declined to overrule *Miller*

---

criticism of the third party doctrine, see NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 136–39 (2015).

367 Ohm, *supra* note 73, at 386.

368 138 S. Ct. 2206 (2018).

369 Panneck, *supra* note 335, at 513.

370 *Carpenter*, 138 S. Ct. at 2223; Ohm, *supra* note 73, at 361; Olivier Sylvain, *The Market for User Data*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1087, 1095 (2019).

371 *Carpenter*, 138 S. Ct. at 2217; Ohm, *supra* note 73, at 363.

372 Ohm, *supra* note 73, at 358; Panneck, *supra* note 335, at 528 (explaining that the Court recognized that it was not merely concerned with an individual's movements, but the private personal information one might discover in knowing about that person's movements.).

373 *See* Ohm, *supra* note 73, at 358.

374 *Id.* at 364 ("[T]he majority opinion is not restricted to CSLI. Instead, this is an opinion about information the police can use to locate people generally, not CSLI specifically.").

375 *See id.* at 369 ("The test that emerges from the majority opinion will also be applied to collections of information maintained by third parties that do not track location, not even by inference, but are of interest to law enforcement.").

and *Smith*,[376] hints throughout *Carpenter* suggest that these two opinions should be interpreted narrowly in the future to the specific facts of the cases being decided.[377] The case of *Carpenter* can open the door "to protecting all kinds of digital information."[378] However, the decision is vague and "leave[s] numerous important issues 'unresolved and uncertain.'"[379] It should be noted that empirical research surveying courts judicial decisions that cited *Carpenter* revealed disagreements among lower courts with regards to the breadth of *Carpenter*. Some courts apply its concepts extensively while others attempt to narrow it down.[380]

4. Extending *Carpenter* to Unmasking Cryptocurrency Users

Carpenter called into question the third-party doctrine and signaled a departure from precedent. Indeed, there are disagreements among courts regarding the scope of *Carpenter*,[381] and at least one court denied a motion to suppress evidence obtained through a search warrant regarding the identification of cryptocurrency identity.[382] As Professor Neil Richards recently explained, the third-

---

[376] *Carpenter*, 138 S. Ct. at 2220 ("We do not disturb the application of *Smith* and *Miller* . . . .") (citing United States v. Miller, 425 U.S. 435, 437 (1976); Smith v. Maryland, 442 U.S. 735 (1979)); Ohm, *supra* note 73, at 359; Panneck, *supra* note 335, at 541.

[377] *See* Ohm, *supra* note 73, at 385 (explaining that *Carpenter* "turns the third-party doctrine inside out, requiring the government to account for the database design and information-gathering decisions of private parties, decisions made without any state intervention").

[378] Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law 2018–2021*, 135 HARV. L. REV. (forthcoming 2022) (manuscript at 8) (on file with author).

[379] *Id.*

[380] *See id.* (manuscript at 9).

[381] *Id*. (manuscript at 13) ("Several scholars have conjectured about the meaning of *Carpenter* going forward, but they have reached sharply different conclusions.").

[382] See generally United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020). In this case, federal agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by a child pornography website that defendant used to download material. Id. at 309. The court held that defendant lacked a reasonable expectation of privacy in his information on the Bitcoin Blockchain where the nature of the information on the Bitcoin blockchain and the voluntariness of the exposure weigh heavily against finding a privacy interest in an individual's information on the blockchain. Id. at 310. The court also held that transactions and records that exchanges have do not receive Fourth Amendment protection. Id. at 312; see also Daniel Penn, Note, The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from

party doctrine is not dead. The legacy of *Carpenter* means requiring courts to undertake "a delicate balance between the remnants of the third-party doctrine and a notion of Fourth Amendment protection."[383] We, however, believe that *Carpenter*'s departure from precedent can justify further extensions beyond the explicit holding,[384] and with time, more courts are likely to follow a broad interpretation of the case.[385]

This Article argues that unmasking cryptocurrency users' identities should also be subject to a warrant and require the government to show probable cause of illegality. Cryptocurrency users have a reasonable expectation of privacy. Cryptocurrencies are different from banks that are subject to governmental regulation and reporting obligations. The anonymity of the token is exactly the reason for using such tokens. Unmasking the identities of cryptocurrency users can reveal information regarding users' financial activities. Thus, such unmasking should be exempt from the third-party doctrine as applied in *Carpenter*.

Applying the third-party doctrine to cryptocurrency users and unmasking cryptocurrency user identities without a warrant would hinder sufficient protection for users against governmental intrusion. Consequently, users would be disincentivized from using such tokens for legitimate purposes. Without a warrant requirement, even beneficial uses of cryptocurrency would likely grind to a halt,[386] resulting in losses for the economy and society. This is especially alarming as cryptocurrencies are now used also to trade in crypto-assets like NFTs, which could in the future become the engine of

---

the Court's First Ruling on Bitcoin Privacy, 24 SMU SCI. & TECH. L. REV. 125, 128 (2021); David Zaslowsky, Court Analogizes Coinbase to 'Traditional Bank' for Purposes of Fourth Amendment Privacy Protection, BAKER MCKENZIE: BLOCKCHAIN BLOG (July 2, 2020), https://blockchain.bakermckenzie.com/2020/07/02/court-analogizes-coinbase-to-traditional-bank-for-purposes-of-fourth-amendment-privacy-protection/ [https://perma.cc/7WXP-P6EW].

383 RICHARDS, *supra* note 91, at 59 (referring the third-party doctrine as an outdated privacy rule but clarifying, however, that *Carpenter* did not abolish the doctrine).

384 *See* Panneck, *supra* note 335, at 542.

385 Tokson, *supra* note 378 (manuscript at 4) ("[T]he proportion of cases employing narrow interpretations of *Carpenter* has decreased over time, as familiarity with the *Carpenter* standard has likely increased.").

386 *See* SOLOVE, *supra* note 336, at 109 (expanding on the importance of a warrant).

speech.[387] Therefore, this Article concludes that necessitating a warrant to unmask cryptocurrency users' identities achieves the proper balance between individuals' legitimate privacy interests and national security concerns, allowing law enforcement to police bad actors in the age of advancing technology.

IV. ADDRESSING THE OBJECTIONS AND LIMITATIONS

Verifying and unmasking cryptocurrency identities is not a "silver bullet," and may have certain limitations and shortcomings. Several objections to the proposed framework can be anticipated and should be addressed accordingly. This final Part of the Article addresses such concerns.

A. The First Amendment

In the United States, freedom of speech enjoys stronger protections than in other Western democracies.[388] The First Amendment protects freedom of speech against governmental censorship.[389] The "right to record" can protect data collection;[390] raw data may also enjoy First Amendment protections;[391] and even a source code can be considered protected speech.[392] The following Subsections

---

[387] *See generally* Jabotinsky & Lavi, *supra* note 331.

[388] *See* Evelyn Douek, *Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability*, 121 COLUM. L. REV. 759, 772 (2021); Oreste Pollicino & Marco Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, *in* RESEARCH HANDBOOK ON EU INTERNET LAW 513–28 (Andrej Savin & Jan Trzaskowski eds., 2014). For criticism, see MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION *18–20* (2019) (arguing that legislators, courts, and civil rights organizations have interpreted the First Amendment selectively, almost like religious fundamentalists, and in fact shifted even more power from vulnerable populations to powerful ones).

[389] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . .").

[390] *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 180–81 (2017).

[391] *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 65, 72 (2014) (explaining that the First Amendment can protect raw data as it promotes the creation of knowledge).

[392] *See generally* Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 100–05 (2017); *see also* Justin S. Wales & Richard J. Ovelmen, *Bitcoin Is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment*, 74 U. MIA. L. REV. 204, 255 (2019); Kyle Langvardt, *The Doctrinal Toll of "Information as Speech*," 47 LOY. U. CHI. L.J. 761, 770

address freedom of expression objections to the proposed verification, validation, and unmasking of cryptocurrency user identity.

1. Cryptocurrency Users: Identity Verification, Unmasking, and Freedom of Expression

One can argue that imposing an obligation to verify the identity of cryptocurrency users and allowing unmasking thereof infringes on users' freedom of expression, as it limits their anonymity. This, in turn, can censor their speech as reflected in their use of cryptocurrencies. As such, courts could arguably strike down this regulation.

Identifying speakers can often provide information about their activities, even without knowing the content of communication.[393] Therefore, the right to communicate anonymously is protected by U.S. law.[394] A line of cases made clear that there is a constitutional right to anonymous religious and political speech.[395]

Upon first glance, it can be argued that individuals' use of cryptocurrencies is not speech and that restrictions on the anonymity of cryptocurrency users do not constitute restrictions on the marketplace of ideas, but rather on the marketplace of commerce.[396] Yet, one might still argue that cryptocurrencies are not just forms of digital payment; they also have non-financial applications. Such tokens facilitate users' engagement in expressive activities with one

(2016) (referring to Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996)); *see also Bernstein*, 922 F. Supp at 1435 (holding that source code, whether functional or not, is *always* speech protected by the First Amendment, because "the functionality of a language does not make it any less like speech.").

393 *See* Froomkin, *supra* note 392, at 99.

394 *See id.* at 149.

395 *See generally, e.g.*, Talley v. California, 362 U.S. 60 (1960) (voiding a Los Angeles City ordinance that forbade the distribution of any handbills in any place under any circumstances, if the handbills did not contain the name and address of the person by whom they were prepared); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (voiding an Ohio statute prohibiting anonymous campaign literature, and holding that such a law violates the First Amendment and as such is unconstitutional); Buckley v. Am. Const. L. Found., Inc., 525 U.S. 182, 198–200, 204 (1999); Watchtower Bible & Tract Soc'y of N.Y. v. Vill. of Stratton, 536 U.S. 127, 165–70 (2002).

396 *See* Alexander Tsesis, *Marketplace of Ideas, Privacy, and Digital Audiences*, 94 NOTRE DAME L. REV. 1585, 1588 (2019) (differentiating between marketplace behavior and freedom of expression).

another.[397] Cryptocurrencies also enable users "to include non-financial data (called 'arbitrary data') that, once the associated (often nominal) transaction is validated, become[] immutably published onto [the cryptocurrency's] blockchain . . . ."[398] In addition, cryptocurrencies have communicative value as they allow users to communicate in ways previously unimaginable and to express their lack of trust in central economies.[399] Verifying cryptocurrency users' identities and subjecting them to possible unmasking could result in censorship of expressive activities.

However, although the use of cryptocurrencies can be considered speech, the proposed regulation focuses on illegal aspects of *financial activities and applications* enabled by cryptocurrencies, and not on expressive values. Focusing on financial conduct can be treated, *at most*, as commercial speech.[400] Even if recognized as speech, regulations should only be subject to intermediate scrutiny standards.[401]

Identity verification and validation of cryptocurrency users applies to all users in a content neutral way, irrespective of the content of their transactions.[402] Unmasking reveals users' identities and does not restrict their choice to use cryptocurrencies. Moreover, there are safeguards preventing authorities from unmasking identities of cryptocurrency users regularly, posing a high standard of probable cause. Such safeguards are likely to prevent infringement of

---

397 Wales & Ovelmen, *supra* note 392, at 204.

398 *Id.* at 222.

399 *Id.* at 241.

400 Scholars have criticized the court's treatment of market behavior as speech. However, if courts are to treat the financial aspects of cryptocurrency use as speech, they should be treated as commercial speech at most. For criticism on the lack of differentiation between market behavior and speech in a related context of platform immunity from liability for harmful speech, see Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, U. CHI. LEGAL F. 45, 51 (2020) ("Section 230's liability shield has been extended to activity that has little or nothing to do with free speech, such as the sale of dangerous products.").

401 *See generally* Felix T. Wu, *Commercial Speech Protection as Consumer Protection*, 90 U. COLO. L. REV. 631 (2019); *see* Tsesis, *supra* note 396, at 1585, 1620, 1626.

402 For discussion of content neutral restrictions, see Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 48 (1987) ("Content-neutral restrictions limit expression without regard to the content or communicative impact of the message conveyed.").

legitimate free choice to use cryptocurrency. A substantial chill on the legitimate use of cryptocurrencies is not expected; users would know that unmasking only occurs when a warrant is issued and when there is probable cause that cryptocurrency is being misused for illegal transfers or transactions. Thus, identity verification and unmasking obligations are likely to survive intermediary scrutiny in terms of preserving users' free speech. Such regulations are constitutionally justified—it is narrowly tailored to serve the substantial national security interest.[403]

2. Wallet Providers, Exchanges, and Issuing Firms: Identity Verification, Unmasking, and Freedom of Expression

Another objection concerns wallet providers and issuing firms' freedom of expression. It can be argued that the proposed identity verification and unmasking obligations limit these parties' freedom to shape their systems' software codes; code is information, and information is speech.[404] Because computer language and code are forms of speech, specific obligations to program a system in this way—ex ante identity verification and ex post unmasking—infringes wallet providers, exchanges, and issuing firms' freedom of expression.[405]

It should be noted that the rush to claim First Amendment protections for non-expressive, but code-dependent technologies has been criticized by scholars as diluting the First Amendment's core principles and threatening its strength.[406] However, courts currently recognize freedom of expression interests in code.[407] Thus, one

---

403 *See* Tsesis, *supra* note 396, at 1614 (explaining the intermediary scrutiny test and the focus of speech restrictions on reasonable time, place, and manner restrictions).

404 *See generally* Bambauer, *supra* note 391 (arguing that data can enjoy First Amendment protection when it promotes the right to create knowledge); *see also, e.g.*, Ellen Nakashima & Mark Berman, *Apple Says FBI Seeks 'Dangerous Power,' Files Motion Opposing Court Order to Help Unlock iPhone*, WASH. POST (Feb. 25, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/02/25/apple-files-motion-opposing-court-order-to-help-fbi-unlock-iphone/ [https://perma.cc/B8JG-9L9H].

405 *See* Langvardt, *supra* note 392, at 771, 798–99.

406 *See id.* at 761.

407 *See, e.g.*, Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

might argue that courts could strike down the proposed regulations for violating wallet providers' First Amendment rights.

However, although such technological tools can be considered speech, the value of this speech is not absolute. Such technological tools do not raise the kind of core expressive interests that warrant First Amendment protection.[408] Programming a technological tool that instructs financial systems is not a way to participate in the marketplace of ideas, but rather a form of market behavior that uses speech.[409] A product or tool's code is constructed by speech that is commercial in nature. Accordingly, the obligation to embed identity verification and unmasking capabilities within the code should not be subject to strict scrutiny standards; it should only be subject to intermediary scrutiny instead. The government has a substantial interest in this regulation due to its importance in stifling terror operations and attacks. This regulation is content neutral: it avoids dictating exactly how to program the code. Furthermore, it does not interfere with the system's general operations. Rather, it sets enabling identity verification and unmasking capabilities as goals. As such, it is narrowly tailored to serve national security interests.

B. From the Cathedral to the Bazaar and Back to the Cathedral Again? Concerns Regarding Centralized Power Distribution

The Cathedral and the Bazaar are two well-known models to engineer a software.[410] The Cathedral model restricts the code developed to an exclusive centralized group of software developers. In contrast, the Bazaar model is decentralized. The code developed is an open-source code and can be viewed by the public. Although these models originally refer to engineering software, these models and metaphors of Cathedral and Bazaar can describe broader social contexts and structures, such as the structure of financial systems.

---

408 RICHARDS, *supra* note 91, at 182.

409 For discussion in the related context of algorithmic speech, see Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 502 (2020).

410 This metaphor of cathedral and bazaar was coined by Eric S. Raymond in a related context, comparing centralized licensed computer code and Linux. *See generally* ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY (1999).

The traditional financial system can be conceptualized within the Cathedral model; the medium of currency exchange requires large, centralized government institutions' involvement and regulatory authorities.[411] In contrast, cryptocurrencies can be conceptualized within the Bazaar model, as they operate in an autonomous and distributed manner, independent of any trusted authority or centralized operator.[412] They lack sovereign backing and many features of national currency systems.[413] Cryptocurrency systems can be likened to a "bazaar,"[414] as a "libertarian ethos that animates many of the individuals and entities involved in the creation and growth of the [cryptocurrency] movement."[415]

However, placing legal obligations on wallet providers, exchanges, and issuing firms might lead to centrality and, in fact, signal a shift back to the Cathedral model, where central intermediaries regulate the market. Similarly, the internet was once thought to be a harbinger of disintermediation—a sovereign medium controlled by users from the bottom up. Now, the internet has shifted and created new gatekeepers: online intermediaries.[416] A similar development could occur in the cryptocurrency system, which is already becoming less decentralized.[417] It is theoretically true that imposing

---

411 This model includes central banks. Reem Heakal, *What Central Banks Do*, INVESTOPEDIA, https://www.investopedia.com/articles/03/050703.asp [https://perma.cc/F5TV-UJMU] (June 23, 2021).

412 Primavera De Filippi et al., *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, 62 TECH. SOC'Y, Aug. 2020, at 11, Article 101284 ("[B]lockchain technology is often described as a 'trustless' technology because it eliminates the need for a trusted authority and replaces it with a system of publicly verifiable proofs.").

413 *See* Goldman et al., *supra* note 16, at 14.

414 RAYMOND, *supra* note 410.

415 *See* Goldman et al., *supra* note 16, at 7.

416 *See supra* Part II (expanding on the role of intermediaries as gatekeepers); *see also* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM 75 (2019) (explaining that some aspects of the conception of "technologies of freedom" have changed beyond recognition and "[t]oday's networked digital information infrastructures have different and more complicated affordances[]"); Michal Lavi, *Targeting Exceptions*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65, 138 (2021).

417 *See* De Filippi, *supra* note 19 ("Over the years, the governance of the most popular blockchain networks has become highly centralized, and only a few large corporations (such as the main blockchain exchanges and wallet providers) are responsible for making blockchain technology accessible to the wider public.").

identity verification and unmasking obligations on wallet providers, exchanges, and issuing firms could increase these parties' involvement in regulation, distort the power distribution in the infrastructure, and undermine the decentralized model that avoids shortcomings of traditional financial institutions and state control. Such obligations might impair user trust in the system and hinder innovation. Therefore, one could reason that it is unwise to discourage a successful and innovative model just because illicit actors, such as terrorists, use it.[418]

Indeed, imposing obligations on wallet providers, exchanges, and issuing firms is no panacea. However, identity verification and unmasking obligations subject to court warrants are not directed at transactions or at the technologies. Thus, they are different from traditional gatekeepers, such as payment blockades.[419] Because users' identities are encrypted and can only be unmasked subject to a warrant with probable cause, such regulation would primarily target illicit actors using the system.[420] It is likely to have little impact on legitimate financial transactions or transfers by innocent users. Therefore, it is not expected to have far-reaching influence on the system's special structure or on the trust of innocent users therein.

Admittedly, the proposed regulation allocates increased power to wallet providers, exchanges, and issuing firms. Despite targeting illicit actors, it might disrupt the decentralized structure of the system. However, when balancing the possible social costs of such disruption against the national security benefits, the proposed intervention is worthwhile.

C. Administrative Costs

The third objection concerns the administrative costs associated with user identity verification, information storage and security, and unmasking procedures. Any new and heavy regulatory regime would make all transactions costlier and less convenient.[421] Arguably, imposing such costs on wallet providers, exchanges, and issuing

---

418 For this argument, see HOUBEN & SNYERS, *supra* note 193, at 10.

419 On payment blockade, see the discussion *supra* Part I. *See generally* Bridy, *supra* note 100.

420 *See* HOUBEN & SNYERS, *supra* note 193, at 55–56.

421 *See* Breu & Seitz, *supra* note 234.

firms places a heavy burden on these actors. Such regulation might even cause them to exit the market.[422] Moreover, new investors might refrain from investing in such systems and decline to develop new types of innovative cryptocurrencies. Thus, such regulation could lead to market inefficiencies.[423]

Though the proposed regulation has costs, the benefits of such a solution in stifling terrorist activities and enhancing national security exceed the costs of implementing an identity verification framework. Overall, the proposed regulation promotes welfare maximization.[424] In the United States, similar obligations are common, such as unmasking procedures that involve costs of litigation, despite the burdens they impose.[425] For example, there are John Doe subpoenas to unmask anonymous speakers from their ISP or the website on which they posted defamatory comments.[426] Imposing obligations on traditional intermediaries to provide information in John Doe procedures can be justified from an economic perspective, because such intermediaries are best positioned to collect, store, and provide helpful information in legal procedures.[427] The proposed regulation is justified based on similar arguments.

---

422 This is indeed already happening following the 5th European Anti-Money Laundering Directive. Bottle Pay, a UK-based crypto wallet provider, announced its decision to cease operations at the end of last year. *See* Rachel Wolfson, *What the 5th Anti-Money Laundering Directive Means for Crypto Businesses*, COINTELEGRAPH (Jan. 10, 2020), https://cointelegraph.com/news/what-the-5th-anti-money-laundering-directive-means-for-crypto-businesses [https://perma.cc/TUX8-9CV8] ("As we are a UK based custodial Bitcoin wallet provider, we will have to comply with the 5AMLD EU regulation coming into effect on January 10, 2020. The amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community.").

423 *See generally* Jabotinsky & Sarel, *supra* note 26.

424 On the role of legal rules in promotion of welfare maximization, see generally John R. Hicks, *The Foundations of Welfare Economics*, 49 ECON. J. 696 (1939).

425 *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 39, 225, 258 (Yale Univ. Press, 1970) (discussing the costs of litigation).

426 Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 325 (2008) (explaining the consideration and standards that U.S. courts apply when considering whether to order John Doe subpoenas). *See also* Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn From John Doe?*, 50 B.C. L. REV. 1373, 1374–75 (2009).

427 *See generally* Jacqueline D. Lipton, *Cyberbullying and the First Amendment*, 14 FLA. COASTAL L. REV. 99, 114 (2012) ("The downside of limited liability for online service providers is that there is little onus placed on the parties in the best position to curb harmful

Similarly, an EU proposal regarding digital services, the Digital Services Act ("DSA"),[428] attempts to impose obligations on online marketplaces to identify traders that offer products or services and to collect detailed information on the identity of these traders.[429] According to the regulation, platforms must make reasonable efforts to ensure that the information provided to them by the traders is accurate and complete. This new duty is expected to increase administrative costs. However, because such a duty is expected to assist in detecting rogue traders and protect online shoppers from counterfeit or dangerous products, and because it allows enforcement of such violations,[430] it can be justified.

The U.S. Congress followed this direction; thus, the House Energy and Commerce Committee is marking up the proposed bill.[431] The bill is in fact a "know your customer" law for sellers online, requiring marketplaces to collect information from high-volume sellers, verify the information, make high-volume sellers disclose contact information to consumers, and enable electronic and telephonic reporting of "suspicious activity" in the marketplace.[432]

Cryptocurrency identity verification is thus not revolutionary. Moreover, such verification was already planned to be conducted voluntarily by Diem and Saga, which intended to verify the credentials of all coin users.[433] It follows that costs of identity verification

---

conduct to take active steps or expend significant resources to do so."); Winhkong Hua, Note, *Cybermobs, Civil Conspiracy, and Tort Liability*, 44 FORDHAM URB. L.J. 1217, 1230 (2017).

428 Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM (2020) 825 final (Dec. 15, 2020).

429 *Id*. at para. 46.

430 *See* Miriam C. Buiten, *The Digital Services Act: From Intermediary Liability to Platform Regulation*, 12 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 361, 376 (2021).

431 H.R. 5502, 117th Cong. (2021).

432 Eric Goldman, *Comments on HB 5502, the "INFORM" Act*, TECH. & MKTG. L. BLOG (Nov 17, 2021), https://blog.ericgoldman.org/archives/2021/11/comments-on-hb-5502-the-inform-act.htm [https://perma.cc/CQ8X-YQUY].

433 *See, e.g.*, LIBRA WHITE PAPER, *supra* note 70; *The Closure of Sogur*, *supra* note 308. *See also* Mike Orcutt, *The Radical Idea Hiding Inside Facebook's Digital Currency Proposal*, MIT TECH. REV. (June 25, 2019), https://www.technologyreview.com/2019/06/25/800/how-facebooks-new-blockchain-might-revolutionize-our-digital-identities/ [https://perma.cc/AL83-4VR4].

are not inherently unreasonable. Therefore, in light of the importance of verification and unmasking for national security and crime prevention, such verification should be obligatory for all cryptocurrency wallet providers, exchanges, and issuing firms.

D. Data Breach Concerns

The fourth objection focuses on data breach concerns. The proposed regulation obligates wallet providers to verify their users' identities. Such dossiers of personal information can be hacked and misused by illicit actors, raising security and privacy risks,[434] such as identity theft[435] and fraud.[436] Many privacy laws focus on the obligations of data collectors and processors to obtain informed and explicit consent before collecting personal data, but such laws still do not protect personal information from hacks.[437] Such data breaches can result in tremendous harm, including identity theft and other economic and emotional harms.[438]

Indeed, stored personal information regarding cryptocurrency users' identities can be hacked and misused by illicit actors.[439] Data breaches are a major problem in the information age in general.[440] However, the risk of a data breach should not prevent personal

---

[434] For such a concern in a related context, see Fennie Wang & Primavera De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, FRONTIERS IN BLOCKCHAIN (Jan. 23, 2020), https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full [https://perma.cc/SK3P-78VC].

[435] *See* Sara S. Greene, *Stealing Identity from the Poor*, 106 MINN. L. REV. 59, 62 (2021) (discussing identity theft and the difficulties to recover from it); CARISSA VELIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 110 (2006).

[436] *See generally* Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019).

[437] DION-SCHWARZ ET AL., *supra* note 17, at 53 (expanding on increasing security breaches and hacks); *see also* Wang & De Filippi, *supra* note 434; VELIZ, *supra* note 435 ("[E]very day of every week hackers break into networks and steal data about people. Sometimes they use that data to commit fraud. Other times they use it for shaming, extortion or coercion.").

[438] *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (discussing the tremendous damage caused by data breach).

[439] Stored information can be hacked. *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1894–95 (2019).

[440] *See* Solove & Citron, *supra* note 438, at 745.

information from being collected and stored. Rather, regulators should focus on effective data security and restrict insecure designs that create unwarranted privacy risks.[441]

Two design features can mitigate the risk of data breach harm. First, users' personal data should be encrypted. Encryption will enable a high level of confidentiality.[442] It is an effective tool for citizens and businesses to defend themselves against technological abuse, such as hacking, identity and personal data theft, fraud, and improper disclosure of confidential information.[443] Enhancing privacy protections promotes the security of technology users.[444] Various legal regimes governing data breaches even exempt encrypted information from data breach notification requirements.[445]

Second, encryption can be combined with anonymization techniques.[446] The personal identifiers can be de-anonymized and identified only when a court warrant requires. Though such a design is not absolute because hackers can de-anonymize information,[447] it

---

441 *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 50 (2021).

442 *See* Rocio de la Cruz, *Privacy Laws in the Blockchain Environment*, ANNALS EMERGING TECHS. COMPUTING, Dec. 2019, at 34, 39 ("[E]ncrypting the data by choosing an encryption option that ensures a high level of confidentiality. The solution I recommend here to minimise risks of breaching the law and/or facing a data breach incident, is anonymizing the personal data to the maximum extent that still allows the Blockchain achieve it [sic] purpose.").

443 *See Encryption*, EUR. COMM'N, https://ec.europa.eu/home-affairs/cybercrime/encryption_sv [https://perma.cc/5PCY-UG8G].

444 *See* HOUBEN & SNYERS, *supra* note 193, at 55; *see also* A. Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L REV. 141, 159 (2020).

445 *See* Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 811–12 (2020) (referring to GDPR, Article 34(3)(a)); *see also* Jennifer J. Hennessy et al., *State Data Breach Notification Laws*, FOLEY & LARDNER LLP, https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws [https://perma.cc/7767-ZDRZ] (Mar. 1, 2022).

446 *See* de la Cruz, *supra* note 442, at 39 (proposing to combine encryption with anonymization techniques).

447 For information on the shortcomings of anonymization, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703 (2010).

increases the price they pay for data misuse, reducing the risk of identity theft.[448]

Beyond mitigating data misuse risks, anonymization and encryptions will make it easier to implement the proposed reform. By anonymizing and encrypting the users' identities, cryptocurrency issuers, exchanges, and wallet providers can avoid violations of the shifting regulatory landscape under the EU General Data Protection Regulation ("GDPR").[449] This regulation is a component of EU policies meant to limit commercial audiences' abilities to resend, sell, and share private information.[450] It protects EU citizens' data; yet it also applies to non-EU companies offering goods or services to EU consumers.[451] Thus, it can affect data protection throughout the world.

The GDPR contains a threshold test for international transfers of personal data to non-member states and a legal basis for blocking data exports to states that do not meet its "adequacy" standard.[452] With regard to transmissions to the United States, instead of an adequacy determination, the European Union and the United States reached an arrangement called the "Privacy Shield": a voluntary, private-sector compliance program.[453] Yet, recently the European

---

448 *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 703 (2016) (arguing that anonymization should focus on the process of minimizing risk of reidentification and sensitive attribute disclosure, not preventing harm).

449 Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR]; Alexandra Giannopoulou, *Putting Data Protection by Design on the Blockchain*, 7 EUR. DATA PROT. L REV. 388, 399 (2021) ("The use of encryption techniques as central features to the design of blockchains, would make them appear in compliance with part of the data protection by design obligations, since encryption is particularly underlined in article 25(1) GDPR.").

450 Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 594 (2019).

451 Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices*, 52 SUFFOLK U. L. REV. 227, 228 (2019).

452 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 771 (2019).

453 The privacy shield replaced the safe haven agreement. In *Schrems v. Data Protection Commissioner*, the ECJ declared that this safe harbor was invalid. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015). Following this decision, the US and the EU reached a new arrangement called the Privacy Shield. It should be noted

Court of Justice in Luxembourg struck down the privacy shield in the case of *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*,[454] determining that the Privacy Shield did not limit access to data by U.S. authorities "in a way that satisfies requirements that are essentially equivalent to those required under EU law. . . ."[455] The long-term impact of the ruling remains unclear.[456] but it is obvious that the GDPR has a global impact today, now more than ever.

As explained above, the GDPR poses limitations on data processing and retention, and aims to better safeguard data subjects' personal autonomy and dignity.[457] The limitations and restrictions posed by the GDPR apply to "personal data," that is, "any information relating to an identified or identifiable natural person."[458] However, anonymizing data can render the GDPR inapplicable; if anonymization is fully achieved, the data does not relate to an identified person anymore.[459] Indeed, the method of anonymization must achieve full anonymity[460] and not settle with pseudonymization.[461] If data on cryptocurrency identities is only pseudonymized, cryptocurrency companies (as controllers of the data) will be required to

---

that the legal future remains uncertain and is dependent on the outcome of another ruling by the CJEU. *See* Case C-311/18, Data Protect. Comm'r v. Facebook Ir. & Schrems, ECLI:EU:C:2020:559 (July 16, 2020); *see also The Schrems Saga Continues: Schrems II Case Heard Before the CJEU*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (July 10, 2019), https://www.huntonprivacyblog.com/2019/07/10/the-schrems-saga-continues-schrems-ii-case-heard-before-the-cjeu/ [https://perma.cc/HEU3-LFRE].

454 C-311/18, Data Prot. Comm'r v. Facebook Ir. & Schrems, ECLI:EU:C:2020:559, ¶¶ 198–200 (July 16, 2020).

455 *Id*. ¶ 185.

456 *See* Edward W. McLaughlin, Schrems*'s Slippery Slope: Strengthening Governance Mechanisms to Rehabilitate EU-U.S. Cross-Border Data Transfers After* Schrems *II*, 90 FORDHAM L. REV. 217, 226 (2021).

457 *See* Tsesis, *supra* note 450, at 594.

458 GDPR, *supra* note 449, at art. 4(1).

459 *See id.* at Recital 26.

460 Information is anonymized if the information cannot be associated with a natural individual (taking into account the means it is reasonably likely to be used, including the available technology at the time of the processing and technological developments). *Id*.

461 *Id.* at art. 4(5) (defining pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.").

implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the GDPR.[462] However, they can still benefit from several relaxed standards under the GDPR[463] but will bear costs in complying with GDPR standards as information controllers.

Yet, if the goal of full anonymization is achieved and the data subject is no longer identifiable, cryptocurrency issuers, exchanges, and wallet providers will not be subject to additional data protection obligations under the GDPR.[464]

E. Global Law Enforcement

The fifth difficulty is a pragmatic one. Enforcement of identity verification and unmasking obligations raises jurisdictional enforcement concerns. Because terrorists use cryptocurrencies globally and rarely limit their financial activities to a single territory, enforcing the proposed regulation on wallet providers in different jurisdictions presents challenges.[465] Regulatory efforts of countries that are limited to local regulation are likely to be futile.[466] This claim is supported by recent calls of members from the G20 forum to regulate cryptocurrencies on a global level.[467]

Yet, as in other domains, in the absence of global regulatory standards, there are multiple tools for coordination among regulators

---

462 *See id.* at art. 5.

463 *See, e.g.*, *id.* at art. 6(4)(e) (referring to processing for other compatible purposes that can be allowed for pseudonymized data).

464 *See* Waltraut Kotschy, *The New General Data Protection Regulation—Is There Sufficient Pay-Off for Taking the Trouble to Anonymize or Pseudonymize Data?*, LUDWIG BOLTZMANN INST. FOR HUM. RTS., VIENNA (Nov. 2016), fpf.org/wp-content/uploads/2016/11/Kotschy-paper-on-pseudonymisation.pdf [https://perma.cc/RY5Y-4TBZ].

465 *See* Israel Klein, *It's Time to Mind the GASB*, 54 SAN DIEGO L. REV. 565, 608 (2017) (suggesting tax benefits related to bonds issued by a political subdivision be conditional upon compliance with better financial disclosure).

466 For the related context of data flows between borders, see VELIZ, *supra* note 435, at 188; *see also* Hadar Y. Jabotinsky & Barak Yarkoni, *The Network Effects of International Financial Regulation* 30 (Hebrew Univ. Jerusalem Legal Stud. Rsch. Paper Series No. 19-04, 2018).

467 Try Ted Knutson, *Crypto Assets Could Threaten Financial Stability Globally Warns G20 Group*, FORBES (Feb. 16, 2022, 8:34 AM), https://www.forbes.com/sites/tedknutson/2022/02/16/crypto-assets-could-threaten-financial-stability-globally-warns-g20-group/?sh=1b6a914f68a1 (last visited Apr. 5, 2022).

and law enforcement agencies.[468] For example, in the context of finance, "a global policy framework—grounded in UN Security Council resolutions, national legislation, and global standards—" was established to block terrorists' access to the formal financial system.[469] Still, agencies, financial intelligence units, and law enforcement officials should "work to stay ahead of the evolving threat of terrorist financing, which is influenced by changes in the global financial system" and emerging financial technologies.[470] Thus, they should also work together to develop a framework for cooperation in the context of enforcing obligations imposed on cryptocurrency wallet providers, exchanges, and issuing firms.[471] "International collaboration is crucial to successfully impose and enforce rules on combating . . . terrorist financing" and strengthening the global fight against terrorism as a whole.[472] Developing a global framework to address these challenges does not undermine the proposed regulation. To the contrary, a global framework of international enforcement and collaboration would enable complete global application of the proposed regulation, rendering it more efficient.

CONCLUSION

Terrorism is not new; the first acts of terrorism were perpetrated at least 2,000 years ago.[473] Yet, new technologies are emerging rapidly, expanding the extensive reach of terrorism and rendering it more dangerous and deadly.[474] New technologies raise new questions and problems that legislators, policymakers, law enforcement, and intelligence agencies must address to mitigate national security

---

468 *See* DION-SCHWARZ ET AL., *supra* note 17, at 52. In the context of child pornography, states can rely on assistance from other states in accordance with the Convention on Cybercrime, which requires cooperation to promote criminal investigations and procedures. Convention on Cybercrime art. 14, Nov. 23, 2001, E.T.S. 185.

469 Goldman et al., *supra* note 16, at 4.

470 *Id.* at 10.

471 *See id.* at 34.

472 *See* HOUBEN & SNYERS, *supra* note 193, at 10, 58.

473 *See* Mark Burgess, *A Brief History of Terrorism*, POGO (Feb. 13, 2015), https://www.pogo.org/investigation/2015/02/brief-history-of-terrorism/ [https://perma.cc/3DRX-U2FG].

474 *See* Lavi, *supra* note 42, at 489.

risks. This Article focused on the problem of cryptocurrencies as an enabler for the flow of terrorist funding. It argued that the law should respond to changes in the terrorism financing ecosystem and address the challenges arising from terrorists' use of cryptocurrencies that threaten national security.

Because cryptocurrencies are built on peer-to-peer networks, allowing users to trade tokens without relying on financial institutions as intermediaries, traditional solutions that target the flow of finance are infeasible. Therefore, policymakers should adopt a new framework to address cryptocurrencies' role in illicit funding.

This Article then proposed new user identity verification obligations on wallet providers, cryptocurrency exchanges, and the firms issuing the tokens. It further offered that the identity of users should not be available to all, but rather should only be unmasked by a court warrant where there exists probable cause of illicit financial transactions or transfers. Thus, the proposed framework endeavors to reach a balance between national security concerns and the fundamental Fourth Amendment rights of users.

Finally, this Article responded to potential objections and shortcomings of the proposed framework. This Article explained that the proposed framework has a vast potential to meet the challenges posed by illicit cryptocurrency use for financing terrorism, and to mitigate the growing national security and public safety risks. Such a framework is preferable to turning a blind eye to the growing use of cryptocurrency for illicit funding. It is also superior to banning the use of cryptocurrencies altogether. We therefore conclude with a call for policymakers and legislators to adopt the proposed framework.