4

Eternal Solutions for an Ephemeral Problem: Suggestions on Cybercrime

Kylie HEITZENRATER

Abstract: With the steady, all-consuming march of the Information Age, new avenues for crime emerge daily. Yet, the legal landscape faces a challenge in addressing these crimes due to the paradoxical need for stable laws that will last, and flexible laws that can bend to the rapidly evolving digital world. This paper analyzes two types of cybercrime – cryptocurrency laundering and doxxing, assessing the existing laws surrounding them, and proposes amendments and future considerations for cyber legislation and regulation. The first crime falls into an existing structure of laws against money laundering, but must adapt to the ways in which blockchain and cryptocurrency further obfuscate financial traceability and attribution. The second type is a contemporary form of harassment that exists in a liminal space of gray morality and technical legality, but which abuses speech to provoke violence. By reviewing current legislation and establishing proper definitions for these crimes, this paper will formulate suggestions for potential improvements to the legal systems surrounding these digital issues.

Keywords: cybersecurity, cybercrime, international law, internet policy, forensic linguistics, cryptocurrency, doxxing

Introduction

Globalization and the extended reach of the cyber dimension pose a problem for lawmakers and law enforcers as the law-making process fails to keep pace with the evolution of crime on the internet. Cyber

defense up to the present has been reactive rather than proactive. This tends to be in large part due to the fast and far-reaching evolution of technology and globalization, especially in the wake of the coronavirus pandemic. As many governments, schools, and businesses quickly jump into the online world, cyber security will continue to be a top priority in international security. The devious financial resources of crime and the malicious invasion of privacy continue to plague the internet. Investigating a long-standing form of crime, money laundering alongside a legally dubious internet activity, doxxing, provides insight into the wide spectrum of illicit happenings in the cyber realm. In this paper, information on the ease of crypto-laundering will be combined with understanding of current laws to provide suggestions for cryptocurrency regulation. This paper will also present a case for why doxxing should receive more legal scrutiny.

Lexical and Analytical Framework

In searching for holes in the legal framework, we must first establish a lexical paradigm with which to assess current laws and to properly suggest amendments.

Cybercrime

To litigate against and to combat cybercrime, we must first understand what cybercrime is. The European Commission provides an excellent and succinct definition:

Cybercrime is a borderless issue that can be classified in three broad definitions:

- crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)

- online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code
- illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse and drugs (sic) trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital component[175].

For the purpose of this paper, I will analyze cryptocurrency laundering and doxxing and propose regulation on a new form of online harassment. The established illegal act of money laundering with the added element of blockchain networks and cryptocurrency demonstrates the integration of old crime finding new techniques in cyberspace. Assessing the morally gray act of doxxing, which does not currently technically violate internet policy, provides insight into new types of crime on the internet.

Crypto-currency

The term "cryptocurrency" refers to a wide variety of digital currencies that all operate through a cryptographic records system known as blockchain (not to be confused with the cryptocurrency company Blockchain). Loosely, blockchain and cryptocurrency operate through 'blocks' of digital information that, through peer-to-peer networking, legitimize transactions, allow degrees of identification, and constitute the cryptocurrency market. The three most popular and prominent cryptocurrencies as of the writing of this article according to Time magazine and CoinDesk are Bitcoin, Ethereum, and XRP. Bitcoin dwarfs all other cryptocurrencies

[175] "Cybercrime," European Commission, Policies, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en.

by a factor of 3 for Ethereum and 10 for XRP[176,177]. Bitcoin is the first cryptocurrency and generally the one that appears the most frequently in media. Ethereum is a blockchain network that hosts the cryptocurrency, Ether. XRP, or Ripple, is a currency exchange network that operates through its own blockchain network. The essential difference between all of these currencies is akin to the differences between US dollars, Japanese yen, and European euros. Each currency exists within its own blockchain network, can be exchanged for other currencies (cryptocurrency or USD, etc.), and functions as fiat currency on the digital market.

Doxxing

According to cybersecurity technology company, Kaspersky Lab, doxxing is the "the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information. That information is then circulated to the public — without the victim's permission"[178]. Other sources, such as Google, often identify an underlying malicious intent or call to violence alongside the dissemination of the private documents. The term "doxxing" (also spelled "doxing") is a shortening and anthimerization of "docs" or documents, stemming from the 1990's hacker phrase "dropping the documents" on a certain individual. General examples of doxxing include the prominent hacker group, Anonymous and their exploits revealing personal information on corrupt law enforcement officers, KKK members, and Q-Anon leaders. Other examples from the Kaspersky website include data leaks from pro-infidelity dating site (Ashley Madison, or The Ashley Madison Agency) and the spreading of the personal details of an American dentist who illegally

---

[176] Ryan Haar, "The 10 Most Popular Cryptocurrencies, and What You Should Know About Each Before You Invest," NextAdvisor, July 1, 2021, https://time.com/nextadvisor/investing/cryptocurrency/types-of-cryptocurrency/.

[177] "The CoinDesk 20," CoinDesk, Accessed July 13, 2021, https://www.coindesk.com/coindesk20.

[178] "What is Doxing – Definition and Explanation," Kaspersky Lab, Resource Center, Definitions, https://www.kaspersky.com/resource-center/definitions/what-is-doxing.

hunted and killed a lion on a protected African preserve[179]. The primary objective of doxxing is to intimidate, to humiliate, and ultimately to endanger the victim whose information is being proliferated on the internet. This paper identifies approximately four levels of doxxing, ranked so by the degrees of identifying information leaked and the malintent behind the leak. The chart is an original analysis of the various types of harassment that occur in doxxing scenarios and is a prototype for future investigations into harassment and privacy violation on the internet. Levels of doxxing range from 1 to 4 in terms of intention and maliciousness. Level 1.5 for example, is included as a form of doxxing as an isolated and impersonal incident associated with company database leaks, but also as a form that can be intentional and malicious, such as the Ashley Madison leak. It should be noted that many forms of doxxing are not illegal as information obtained and disseminated generally comes from the public domain as illustrated below in Table 1.

Table 1. Levels of Doxxing

	Information released	**Perpetrator (P) and Victim (V)**	**Intent**
Level 1: Identity Reveal	• full legal name • photo • sometimes leaking personal accounts to professional sphere	• P: typically individual (though group is possible), anonymous or identifiable • V: typically singular individual	• personal vendetta • humiliation based on perceived wrongdoing • damage victim's reputation
Level 1.5: Database Leak	• full legal name • password to account from leaked site • personal data from leaked site	• P: hacker or hackerbot • V: clientele list of target site	• generally a broadscale attempt to obtain financial and account information • can be more malicious and targeted

[179] Ibid.

Level 2: Public Domain Doxxing	• Level 1 • home addresses of victim and/or victim's friends and family • criminal history • personal phone numbers • workplace details • private photos	• P: individual, anonymous or identifiable, with or without programming skills, with access to public domain information • V: individual or group of individuals	• personal vendetta • humiliation based on perceived wrongdoing • damage victim's reputation • harassment and call to harassment • sometimes call to violence
Level 3: Hacking Doxxing	• Level 1 and 2 • social security number or equivalent • bank statements and account information • private correspondence • private photos (oftentimes nude or explicit photos)	• P: individual or group, anonymous or identifiable, with programming skills • V: individual, family and friends of individual, professional colleagues of individual	• personal vendetta • humiliation based on perceived wrongdoing • damage victim's reputation • harassment and call to harassment • hijacking identity, finances, reputation • call to public violence
Level 4: SWATing and Physical Intervention	• Any amount of Levels 1–3 preceding event • call made to local law enforcement requiring a SWAT investigation	• P: individual, anonymous or identifiable, with or without programming skills, with knowledge on what call situations require SWAT intervention • V: individual, family and friends of individual, professional colleagues of individual	• direct physical harm and/or distress to the victim or victim's family • total harassment of victim

Source: Kylie Heitzenrater, Forensic linguistics.

The International Association of Forensic Linguistics states that, "in its broadest sense, "forensic linguistics" covers all areas where law and language intersect"[180]. We will focus on three subtypes known as "linguistics and the law," "linguistics as evidence", and "research/teaching". These intersections apply generally to legal analysis and discourse, semantics and pragmatics used in court cases, and educating law professionals and law enforcement on legal language, respectively. These aspects of forensic linguistics aid in evaluating the legal landscape of the internet, how cryptocurrency and doxxing fit in, and where legislation could potentially improve. Forensic linguistics will appear again under labels like 'precedent', 'attribution,' and 'suggestions'.

The Crypto-laundering Problem

How does it work?

Sicignano argues, "the primary risk associated with the use of bitcoins is money laundering"[181]. Toolkitaki Technologies coalesced multiple reports to outline how cryptocurrency specifically is laundered suggesting:

> Criminals use a number of methods involving cryptocurrencies to hide the illicit origin of funds. All these methods make use of some of the other vulnerabilities of cryptocurrencies such as their inherent pseudonymity, easy cross-border transactions and decentralized P2P payments. As in the case of cash-based money laundering, there are three main stages in money laundering using cryptos.
> (1) Placement – In this state, illicit funds are brought into the financial system through intermediaries such as financial institutions,

[180] "Forensic Linguistics," The International Association of Forensic Linguists, About, https://www.iafl.org/forensic-linguistics/.

[181] Gaspare Jucan Sicignano, "Money Laundering using Cryptocurrency: The Case of Bitcoin!," Athens Journal of Law 7, no. 2 (April 2021): 253–264, https://www.athensjournals.gr/law/2021-7-2-7-Sicignano.pdf.

exchanges, shops and casinos. One type of cryptocurrency can be bought with cash or other cryptocurrencies. It can be done through online cryptocurrency exchanges. Criminals often use exchanges with less levels of compliance with AML regulations for the purpose.
(2) Layering – In this phase, criminals obscure the illegal source of funds through structure (sic) transactions. This makes the trail of illegal funds difficult to decode. Using crypto exchanges, criminals can convert one cryptocurrency into another or can take part in an Initial Coin Offering where payment for one type of digital currency is done with another type. Criminals can also move their crypto holdings to another country.
(3) Integration – Here, illegal money is put back into the economy with a clean status. One of the most common techniques of criminals is the use of over the counter (OTC) brokers who act as intermediaries between buyers and sellers of cryptocurrencies. Many OTC brokers specialize in providing money-laundering services and they get very high commission rates for the same[182].

Methods such as crypto mixing (or tumbling), peer-to-peer crypto networks, crypto ATMs, or online gambling result in additional illegal activities and aid in criminals conducting business.

Statistics

Locating concrete statistics for crypto-crime is impossible due to its very nature; it is often undetectable and untraceable. The United Nations "estimates, between US$800 billion and US$2 trillion are being laundered every year across the globe, representing 2–5% of the global gross domestic product. Out of this, more than 90% goes undetected.

[182] Tookitaki, "Money Laundering via Cryptocurrencies: All You Need to Know," Tookitaki Inc., Accessed July 14, 2021, https://www.tookitaki.ai/news-views/moneylaundering-via-cryptocurrencies/.

The exact volume of crypto laundering is yet to be ascertained"[183]. Therefore, all crypto-based cybercrime is inherently under-studied, poorly understood, and desperately in need of increased regulation and monitoring.

Jurisdiction

While there are many reports of successful operations seizing cryptocurrency involved in crime, who holds jurisdiction over such cases remains a complex situation[184]. While crime committed in the physical realm has a distinct location that can provide insight into attribution and therefore jurisdiction, crimes exclusively in cyberspace require more nuanced evaluations. If a blockchain firm can be responsible for what is done with their currency, then in theory the world's governments should be liable for the crimes paid for with their currencies. Websites for 'mixing cryptocurrency to further remove identifying markers could hold responsibility for those who use their services. Since most cryptocurrency exchanges go under the radar, simply finding a culprit takes priority over how international law comes into play[185,186].

Attribution and Non-state actors

In recent times, non-state actors have emerged as a threat that cannot be ignored in security analysis, especially in the cyber sphere. They exploit the freedom of cyber infrastructure to conduct illicit business, cyber attacks, and engage in conflict in the physical dimension.

---

[183] Ibid.

[184] Guy Faulconbridge (Sarah Young and Michael Holden, ed), "British police seize record $408 million haul of cryptocurrency," Reuters, July 13, 2021. https://www.reuters.com/world/uk/british-police-seize-250-million-cryptocurrency-2021-07-13/.

[185] Francesco Calderoni, "The European legal framework on cybercrime: striving for an effective implementation," Crime, Law and Social Change 54, no.5 (2010): 339–357, https://doi.org/10.1007/s10611-010-9261-6.

[186] Susan Huanfeng Ning and Han Wu, "China: Cybersecurity Laws and Regulations 2021," International Comparative Legal Guides, (February 2020), https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china.

Cryptocurrency is often used to fund the illicit activities of non-state actors. CipherTrace provides a detailed outline on how to monitor the process of cryptocurrency crime stating:

> Financial Institutions employ Know Your Customer (KYC) processes to confirm the identity of their customer. These processes typically involve the collection and verification of a customer's personally identifiable information (PII)—including, but not limited to, government-issued ID, phone number, email address, physical address, and more. Exact KYC requirements vary by jurisdiction, meaning criminals can use jurisdictional arbitrage to choose geos with lax KYC procedures to further obfuscate their flow of funds.[187]

In what ways can states hold each other accountable for crimes committed within their cyber borders or by state actors?

The Doxxing Problem

'Good' Intentions, Bad Outcomes

Under the technical definitions of this paper, perhaps, incidents such as the NSA WikiLeaks incident with Edward Snowden (doxxing the US government is already illegal), the FBI Investigation into the leaked emails of former Secretary of State Hillary Clinton, and other types of document dropping that supposedly come from a place of benevolence should not be included in doxxing laws. Even individual doxxing such as the surging doxxing of people revealed to be in some way bigoted could be construed as informing the public with good intentions. This article reflects that intentions do matter in doxxing: perpetrators always anticipate retribution and humiliation of the victim. There is no reasonable person who would willfully find and spread identifying information

[187] "2020 Geographic Risk Report: VASP KYC by Jurisdiction," CipherTrace, Accessed July 13, 2021, https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/.

about another person on the internet without the knowledge that bad things will come of it. Be it stolen identity, brutal harassment, or violence, those who doxx are well aware of the potential outcomes. The kind of speech umbrella that doxxing falls under is not protected, even by the United States Constitution. Doxxing, no matter what level, is intended to harass the victim and provoke violence or negativity against them. This should be illegal.

Globalization and Digital Evolution

Laws must be stable and the internet must be flexible. The good news is that a lot of cybercrime is simply normal crime conducted on the internet, such as cryptocurrency laundering, which is generally covered by anti-money laundering laws. However, activities like doxxing are a wholly new dilemma birthed by the Information Age and any regulation surrounding them has consequences that ripple far beyond the initial act. Doxxing sheds light on the ubiquitous practice of data mining by individuals and companies alike to better target world citizens. If limitations are placed on information and data retrieval, large corporations and some governments will not accept restraints on their access to citizens' lives. For example, in spring of 2021, Hong Kong attempted to broaden legislation regarding privacy and personal data protection in the wake of multi-directional doxxing of pro-independence and pro-Chinese police. This was met with immediate backlash by the Chinese government and American internet corporations with large branches in Hong Kong[188,189]. It is all too easy to create a law that is too broad or too narrow. However, no matter how flexible and evolution-friendly a law may be, various interest groups will attack it. Restrictions on

[188] Jeffie Lam and Chris Lau, "Hong Kong's proposed doxxing law is too broad and more safeguards are needed, legal experts say," South China Morning Post, May 12, 2021, https://www.scmp.com/news/hong-kong/politics/article/3133218/hong-kongs-proposed-doxxing-law-too-broad-and-more.

[189] Paul Mozur. "American Internet Giants Hit Back at Hong Kong Doxxing Law," The New York Times, July 5, 2021, https://www.nytimes.com/2021/07/05/technology/hong-kong-doxxing-national-security-law.html.

doxxing generally eat at the heart of data mining and privacy invasion on the internet, which benefit those same interest groups. The freedom and openness of globalization must be balanced with the trepidation of overreaching into a person's existence.

Reactivity vs Proactivity

While cyber defense should be proactive in its protection of people and the state, it runs the risk of devolving into discriminatory profiling and assumption-based surveillance. Although this type of monitoring already to some extent exists, we must be careful to not leap into the dystopian Big Brother state in order to produce even an iota more of security. Doxxing toes a tight line intersecting in speech protection and privacy protection. Unlike in the case of crypto-laundering, doxxing laws should aim to be case-by-case reactions rather than anticipatory assessments.

The Current Solutions

Laws pertaining to crypto-laundering

International law has created basic frameworks for anti-money laundering[190,191]. Flexibility is a good model that appears frequently in international conventions. US codes 18 USC §§ 1956 and 1957 stipulate against most forms of money laundering, and appear to cover crypto-laundering[192]. Articles 4, 6, 7, and 8 of the Budapest Convention provide

---

[190] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Geneva, Switzerland: International Committee of the Red Cross, 2009), https://www.icrc.org/en/publication/0990-interpretive-guidance-notion-direct-participation-hostilities-under-international.

[191] Marco Gercke, "Understanding cybercrime: phenomena, challenges and legal response," International Telecommunication Union, last modified September, 2012, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf.

[192] Joel Cohen and Linda Noonan, "USA: Anti-Money Laundering Laws and Regulations," International Comparative Legal Guides, (May 2021), https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/usa.

for cooperation against economic cybercrime[193]. Likewise, articles 5 and 6 in EU Directive 2019/713[194] forbid willful and nefarious money practices. Case-by-case basis judgement is optimal for situations like doxxing, where a thorough examination of the situation yields the best results. However, documents that attempt to circumnavigate the different legal systems in every state tend to be overly vague as opposed to beneficially flexible.

Flaws/Critique[195,196,197]

The issue with flexibility is that the lack of concreteness in language allows for too much plausible deniability. This is a problem given the already challenging task of attribution in cybercrime. Additionally, "an illegal act needs to be clearly described in and prohibited by law. Pursuant to the moral principle of nullum crimen sine lege (Latin for "no crime without law") a person cannot be punished for an act that was not proscribed by law at the time the person committed the act (UNODC, 2013, p. 53)"[198]. If there is not an explicit ban on the most commonly used methods of identification interference, then the legal process is slowed. Law enforcement needs a clear avenue of locating fraudulent and laundered transactions, as they go on to fuel more corporally dangerous affairs such as terrorism and trafficking.

---

[193] "Details of Treaty No. 185: Budapest Convention," Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185.

[194] http://data.europa.eu/eli/dir/2019/713/oj.

[195] "Assessing the implementation of the Budapest Convention," Council of Europe, Assessments, last modified 2017, https://www.coe.int/en/web/cybercrime/assessments.

[196] Paul Mozur. "American Internet Giants Hit Back at Hong Kong Doxxing Law," The New York Times, July 5, 2021, https://www.nytimes.com/2021/07/05/technology/hong-kong-doxxing-national-security-law.html.

[197] Jeffie Lam and Chris Lau, "Hong Kong's proposed doxxing law is too broad and more safeguards are needed, legal experts say," South China Morning Post, May 12, 2021, https://www.scmp.com/news/hong-kong/politics/article/3133218/hong-kongs-proposed-doxxing-law-too-broad-and-more.

[198] United Nations Office on Drugs and Crime. "The role of cybercrime law". In E4J University Module Series: Cybercrime; Module 3: Legal Frameworks and Human Rights. Accessed July 13, 2021. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

Suggestions for Cryptocurrency Laundering

Future legislation on cryptocurrency laundering should utilize the existing framework for money laundering, including language about mixing websites and other methods of making crypto untraceable. Current laws already prohibit the laundering itself as well as many forms of intentional obfuscation. However, the language should include, where possible, explicit reference to websites designed to further encrypt cryptocurrency. Many countries need stricter laws on Know Your Customer data and other methods of de-anonymizing exchanges and transactions. Mixing websites and other mechanisms of inhibiting the traceability of cryptocurrency should be banned and razed from the internet where possible. To a reasonable extent, no transaction should be completely anonymous.

Suggestions for Doxxing Regulation

In the United States: The Brandenburg Test

According to our definitions and analysis of doxxing, it falls under legal precedent banning speech that intentionally invites violence and malicious actions against others. However, this does require clarification due to the myriad attempts to censor offensive and inflammatory speech. While legally dubious cases such as *Schenck v United States*, *Whitney v. California*, or *Dennis v. United States* invite doubt on the morality of doxxing laws, in America it should be illegal to maliciously divulge personal information about someone with the knowledge and intentions of causing the doxxed victim harm.

The legal precedent that could potentially support anti-doxxing laws in the US is the eponymous litmus test birthed from *Brandenburg v Ohio*, a case originating from a long line of considerations on free speech and the First Amendment of the US Constitution. As Sherman points out,

"*Brandenburg v. Ohio* set a standard for protection of speech that remains in effect today. According to the Supreme Court, speech advocating even extreme ideas may only be proscribed when it is intended to incite imminent lawless activity and is likely to do so"[199]. The Brandenburg test involves three components:

1) the willful intent to speak in a way that invites lawlessness
2) the temporal imminence and imploration of imminent violent
3) the likelihood that the speech will directly influence a reasonable person to act in accordance with the unlawful suggestions.

Regulating doxxing requires consultation with the components of the Brandenburg test and anti-harassment laws. Doxxing is an uncomfortable manifestation of the accessibility of the internet; and it is seemingly the kind of uncouth speech that ought to be protected. However, as we discussed, many instances of doxxing result in direct calls to harassment of the victim, checking off all the boxes of the Brandenburg test.

In the International Sphere

International law presents a difficult challenge as speech laws are highly contested and highly individualized among governments. We need to decide as an international community what our fundamental rights are to data privacy, anonymity, and speech protection. Is it illegal for a private citizen to doxx a state official in another country? Or vice versa? The international community needs a consensus on internet freedom and the freedom from internet harassment in order to create solutions to these growing issues.

---

[199] Michael J. Sherman, "*Brandenburg* v Twitter," *Civil Rights Law Journal* 28, no.2 (2018): 127–172. http://sls.gmu.edu/crlj/wp-content/uploads/sites/16/2019/02/GMC202_crop-1-1.pdf.

Implications

With new technology comes new ways to commit crimes, with new laws come new ways to abuse power, and so on and so forth. As with any consideration for new regulation and legislation, anything created must be done with the utmost care for stability, outcomes, implications, loopholes, and the myriad ways that rules impact our lives.

Additionally, it is one task to assess issues and create laws to combat malintent. It is another task entirely to enforce these regulations and track down those who violate cyber laws. The law is limited by how well it can be executed and enforced. Blockchain/crypto mixers and doxxing hackers cover their digital tracks well, and the constant evolution of covert activities and methods of conducting crime prevent legislation from fully encompassing the scope of cybercrime. The task of cyber legalities must be cautious ambiguity.

A recurring theme in countless articles, assessments, and other documents on cybersecurity is the reverence and caution at restraining the ultimate freedoms and opportunities for connection provided by the internet. Throughout history, the scales seem to have leaned toward either security or liberty. Technology has placed weight on both sides of the scale, none to be taken lightly. As we move ahead in defending ourselves from the limitless potential of the future, we must tread lightly with the knowledge that just as this world wide web connects us to the ends of the universe, so too can it trap us and consume us whole.

Terms of Service and social media outlets that make data readily available to all of the internet need more consumer/user-friendly explanations of what is being broadcast and sold. The intentional esoterism of these documents, which many simply scroll through to the accept button, place users in binding agreements that put them at risk for doxxing and other harmful uses of their information. Education is

a large component of safety, and the public must be educated on the dangers of doxxing and the dubious nature of cryptocurrency.

Conclusion: The Journey Ahead

What makes humans such a strong species is our ability to adapt and to be proactive in the face of a chaotic world. We consider ourselves in control of our existence that we create rules around societies. The nature of law requires stability and equity to produce justice and fair decisions, but the world wide web challenges that rigidness with the ever-evolving avenues to commit cybercrime. We outpace ourselves every day in how to be the very best and at the same time the very worst of ourselves. The ecosystem of economics and the new flavor of criminality brought forth by cryptocurrency asks us to reevaluate how we engage with money. The immortal battle against privacy and speech that must surely be as old as the human language itself, finds insidious homes in the Information Age with doxxing. The hope is that more attention will be focused on the doxxing phenomenon and that Know Your Customer laws will encourage the de-anonymization of crypto transactions. With that, we can make the internet even a fraction safer than before.