Since 2014, the world has been constantly evolving in all facets. How we pay our bills, how we shop, how we invest, what we collect, and what we search for online has been constantly changing. In 2014, the term Non-Fungible Token hereafter referred to as NFT was introduced to the world. With this introduction, an entire new generation of risk and privacy/security compliance issues have emerged. This paper will attempt to explore, elaborate on, and address the privacy and cybersecurity risks surrounding NFTs as well as what NFT owners can actively do on their own to mitigate these risks.

Before any discussion on NFTs can take place, the origins of NFTs as well as the technology behind them must be clarified. An NFT can be defined as "a unit of data, stored on a type of digital ledger called a blockchain, which can be sold and traded." (Wilson, Kathleen Bridget; Karg, Adam; Ghaderi, Hadi (October 2021). "Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity", Business Horizons). Now, when the average individual thinks of a “unit of data,” they most often think of a cell in an excel spreadsheet, or perhaps the file name of something stored on their hard drive. In this instance, this “unit” is so much more. This specific “unit of data” is directly affiliated with a physical or digital asset while also possessing a license which allows for the use of that asset for a specific purpose. (Dean, Sam (March 11, 2021). "$69 million for digital art? The NFT craze, explained", Los Angeles Times.) That specific purpose or future plans of that unit of data is at the discretion of the owner much like any physical tangible asset. This form of economics has the potential to dramatically alter how not only commerce but investing is done globally.

While economics is not the subject of this paper, NFTs and blockchain have an extremely close bond. Blockchain can be defined as a system of recording information in a way that makes it purportedly difficult to change, hack, or cheat the system, or at a high level blockchain is the digital ledger that records transactions and then distributes those transactions across a given network. If we are using tangible more commonly known items, blockchain is the “log” that records all the transactions (NFT buying and selling). This ledger has the potential to not only provide a full listing of an individual’s financial habits and patterns (which would be considered Personally Identifiable Information (PII) as well as Financial Private Information (FPI), but also to potentially disclose an individual’s financial worth and value. From a data privacy perspective, this ledger is the smoking gun when it comes to privacy and security incidents regarding an individual’s financial habits.

Despite this new and exciting method of commerce and assets, there are many unknowns and substantial privacy and security risks associated with blockchain, specifically NFTs. Just because they are new technologies, does not make them immune to privacy and cyber risks. Furthermore, new technologies in the digital realm also often expose pioneers to new cybersecurity and privacy risks. NFTs are no exception. These risks are generally divided into several categories: risks vs inherent to the technology, risks vs the platform/implementation, and common shared cybersecurity risks.

Among a large subset of the user base, there is a misconception that blockchain-based technologies upon which cryptocurrency and NFTs rely are untraceable and that the transactions are effectively anonymous. This has been demonstrably false. In fact, the US Federal Bureau of Investigation (FBI), has transacted with drug dealers with the intention of
obtaining real-world identities (a modern version of “buy and bust”) operations. Furthermore, it has been possible to cluster cryptocurrency addresses in a manner to identify users belonging to the same organization. As NFTs are built on similar technologies, it is highly likely that a similar weakness exists. Further expanding on risks, copyright infringement is another example where a risk is posed regarding NFTs. Unlike more traditional mediums, where methods of determining the veracity of a given work are well-tested, properly verifying the legitimacy of any given NFT is difficult, as NFTs have been created from real works without the consent or involvement of the original creator at all, thus making any resulting NFT fraudulent and worthless.

More ominously, NFTs themselves have been crafted to serve as malicious code delivery systems. NFTs are governed by smart contracts, which implement code intended to enable features such as royalty payments. However, a recent OpenSea vulnerability (now patched) enabled a carefully-constructed NFT to be gifted to a victim and could not be refused. Upon viewing, the code executed malware and transferred the entire contents of the cryptocurrency wallet to the attacker. Given that NFTs are intended to be immutable and unchanging, code updates to mitigate their threat are not possible. Furthermore, this issue is exacerbated by the fact that any transactions involving NFTs also requires paying transaction fees to include “burning” the NFT to remove them from the wallet. Thus, users gifted a malicious NFT cannot update the code to protect themselves and must pay to get rid of them.

In addition to concerns with the underlying NFT technology, there have also been a number of attacks perpetrated against the platforms which process NFTs and the NFT ecosystem as a whole. In January and February 2022, in another OpenSea-related issue, the platform suffered multiple security incidents in which nearly $2 million US were stolen in a phishing attack and a website vulnerability allowed users to purchase NFTs with 1% of the price floor. In general, these platforms suffer the same web-based weaknesses as any other online application. On August 11, 2022, the US Federal Trade Commission (FTC) opened its first probe into the cryptocurrency markets, initiating an investigation into the hack to the BitMart cryptocurrency exchange which resulted in the loss of up to $200 million. The FTC probe is being conducted under the Gramm-Leach-Bliley Act, which requires financial institutions to disclose their information sharing practices. Presumably, BitMart may not have been in compliance with this and other financial regulations which have been enacted specifically to protect consumers. Other crypto exchanges and other crypto-based infrastructure may also be non-compliant and thus pose a greater risk for consumers than more traditional financial institutions.

For that matter, users of NFTs are also not immune to other common cybersecurity concerns shared with other technologies. First and foremost, users must remain vigilant regarding basic operational security practices surrounding the digital wallet. As shown, phishing-based attacks on NFT users are no less effective than in other contexts. In June of 2022, the compromise of a community manager of the Bored Ape Yacht Club, led to a phishing attack against community members and the loss of roughly $360,000. A user which may inadvertently disclose their password during a phishing attack is as vulnerable as any other user utilizing a web-enabled application. Furthermore, users should also be cautioned that the financial structures have not yet been put in place to safeguard users who have had their assets compromised in some fashion. This harkens back to the period of time prior to legal protections for consumers who were victims of identity theft and credit card fraud. Such victims lost their entire fortunes due to malicious criminal activity which are far less impactful today.

Setting the legal risks that will be discussed later aside, participants in the NFT marketplace should consider employing several privacy risk mitigation strategies. Although they may not be
required to adhere to any specific requirements, following several best practices in response to known privacy and security risks will help ensure the safety and security of all parties’ information. It would provide NFT sellers and buyers a degree of assurance even absent regulatory oversight. Basic practices like multifactor authentication, the use of VPNs, only accepting communications from trusted parties, and only conducting transactions on secure networks can go a long way even in rapidly shifting technological landscapes.

Although there is no central repository for storage of information associated with NFT transactions, and the lack of regulatory guidance makes it difficult to know what safeguards and controls should apply to transaction information, buyers and sellers alike should start with considering the basic security posture of devices and systems used for the transaction. If a transaction provider is a relative unknown in the market and cannot demonstrate the security of their systems, that is a warranted red flag.

Transaction provider practices are also an issue with regard to who is able to see a user’s transactions. In several notable incidents, the public Venmo payment exchange feeds of users have revealed transactions the users would have preferred remain private, sometimes with legal consequences. The public visibility of “wallets” associated with NFTs, and cryptocurrency for that matter, makes it possible for anyone to see a user’s activity, and even deposit contents into that wallet. They need only find the wallet’s address. Similar to physical cash in a real wallet, contents can only be removed by spending them.

The legal and regulatory landscape surrounding NFTs is currently sparse. Given the unique nature of NFTs and the means by which purchasers submit payment for them, it is unclear what, if any, existing financial or privacy laws and regulations would apply to them. For example, the Bank Secrecy Act (BSA) plainly applies to transactions between a corporate financial entity and its customers, but it is at best unclear whether sellers of NFTs would be considered financial entities per the direct interpretation of existing financial privacy laws such as Gramm Leach Bliley (GLBA), Dodd Frank, and others. Additionally, given the lack of an applicable federal privacy law, there are no federal or state privacy laws regulating the personal and financial information collected, stored, and maintained as part of an NFT transaction. 2022 saw an unexpected development in federal privacy legislation: introduction of the American Data Privacy and Protection Act (“ADPPA”), which would, for the first time, create a foundational and universally applicable federal privacy framework. While this would be a major step forward for matters related to regulatory authorities as well as federal law, there are several obstacles that prevent this from coming to fruition in the near term. To date, the ADPPA has only advanced as far as passage out of a House committee. The ADPPA was the first all encompassing privacy legislation to pass out of either Congressional chamber and represents a departure from the United States’ historically sector-specific model of privacy regulation. While it will likely pass the full House prior to the 2022 midterm elections, the Senate is unlikely to take up its version of the bill in this Congress. Thus, it is highly likely that while a significant step forward, the ADPPA will be an early topic in the 118th Congress. Despite this major step forward federally, the step has not actually yet been taken, and state privacy laws continue to create a patchwork regulatory model across the country. In the interim, there are more unknowns and unanswered questions than definitive steps forward concerning federal privacy regulation in the United States. This paper will attempt to address those.

The financial transaction issues here also merit consideration, as numerous financial laws and regulations outside of the privacy per se realm might apply. For example, the Fair and Accurate Transactions Act of 2003 (FACT Act) requires “financial institutions” and “creditors” to develop and implement programs to prevent identity theft. Yet, because the law has not yet been
updated to account for both truly peer-to-peer transactions (peer-to-peer transactions currently and almost exclusively route through licensed financial service providers like PayPal, Zelle, and Venmo) and business to business transactions in the NFT context, we cannot say with legal certainty whether NFT market participants would be considered financial institutions or creditors. Yes, it would require an expansive interpretation of those terms. But, it is not impossible. And although legitimate businesses will likely have some privacy and security practices built into their normal operations, the relative ease of entering the NFT marketplace means less-than-compliant entities could do so. Additionally, the Internal Revenue Code requires both individuals and businesses to report instances of receiving $10,000 or more in a year from a single buyer. This requirement could impose tax reporting requirements on NFT sellers, because this statute does expressly include individual persons.

State privacy and data security laws are a rapidly expanding issue, in the sense that numerous states have passed or are in the process of passing their own privacy/data security laws. Much of this rapid pace is driven by the abbreviated legislative sessions used in many states (for example, Georgia’s is only 40 days per year). Newer state privacy laws such as the Virginia Consumer Data Protection Act (VCDPA) either contain outright exemptions for regulated financial entities, or defer to the appropriate federal regulators. The question here is whether sellers of NFTs can avail themselves of these exemptions and deferrals because existing legal definitions of financial institutions do not clearly include or exclude NFTs sellers. At the state level, the State Attorney General would be the designated enforcement entity, however it remains to be seen what direct authority the state AGs would truly have when it comes to the enforcement of privacy and data security regulations regarding NFTs. This question will have to be answered by their respective state legislatures.

In attempting to address all of these concerns, NFT sellers should consider several questions. The first question is that of who is the controller of data that is collected as part of an NFT transaction. Essentially, the controller is the party responsible for determining how the data will be collected, used, and protected. In jurisdictions such as the European Union (EU), controllers (and data protection officers (DPOs)) have additional legislatively defined responsibilities, such as ensuring data subjects can access all information held about them. Crucially, the EU’s definition of a controller includes, “natural persons,” which could reasonably be interpreted as including individuals or entities selling NFTs. Although this may seem like an innocuous distinction, it is notable for individuals because of the responsibilities being deemed a controller would place on them, including determination of the processor responsible for processing personal data on the controller’s behalf. And, in some instances, the global scope of the EU’s regulations, notably the General Data Protection Regulation (GDPR) makes this an area of concern for EU and non-EU persons alike.

US state privacy laws have not yet adopted a broad definition like the EU’s, but certain states have shown a willingness to be aggressive in imposing privacy regulations and perhaps create universally applicable privacy laws like we have not yet seen in the US. While it would be a major departure from the US’ historic norm of sector-specific privacy regulation, the possibility cannot be ruled out. Regardless of the jurisdiction, domestic or international, state or federal, and so on, this is very much a legal gray area with numerous unanswered questions and limited coverage by existing privacy laws. The NFT marketplace as well as the buyers and sellers would benefit immensely from clearly defined legal and regulatory expectations.

In this modern day and age, technology evolves at a daily pace. This rapid evolution makes regulating, mitigating, and securing these new technologies incredibly difficult not only to regulators but to the individuals who are partaking in these new technologies. As covered
previously, there are substantial security risks associated with Blockchain as well as NFTs and other items that can be cataloged in this “digital ledger.” While there are some active measures individuals can take to protect themselves and decrease vulnerabilities, many users are not aware of these measures. Privacy risk is even further from the thought process of most of these individuals, and this is reinforced by the fact that while there are numerous state and federal level financial privacy laws, none of them are targeted towards modern technologies and the exposure that they produce. Currently, the US Congress is moving several pieces of privacy legislation through the appropriate committees, however none of this legislation will provide direction, guidance, or coverage to blockchain and its related mediums. While this is a step forward in the right direction, until more targeted policy is devised Blockchain, crypto, and NFTs will truly be the “Wild West” of the 21st century financial world.

**Glossary of terms:**

**Non Fungible Token** - A non-interchangeable unit of data stored on a blockchain, cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other

**Blockchain** - A distributed database that is shared among the nodes of a computer network

**Personal data (aka personally identifiable information/PII)** - Information which identifies a specific individual (IAPP book terms)

**Processor** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Controller** - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**General Data Privacy Regulation** - European Union’s primary data privacy and data protection regulation.

**Gramm Leach Bliley Act** - also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.

**Fair Accurate Credit Transactions Act** - FACTA (Fair and Accurate Credit Transactions Act) is an amendment to FCRA (Fair Credit Reporting Act ) that was added, primarily, to protect consumers from identity theft. The Act stipulates requirements for information privacy, accuracy and disposal and limits the ways consumer information can be shared.

**Bank Secrecy Act** - The Bank Secrecy Act of 1970, also known as the Currency and Foreign Transactions Reporting Act, is a U.S. law requiring financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.

**Dodd Frank** - A series of federal regulations passed to prevent future financial crises.

**Internal Revenue Code** - The domestic portion of federal statutory tax law in the United States
**Federal Trade Commission** - An independent agency of the United States government whose principal mission is the enforcement of civil U.S. antitrust law and the promotion of consumer protection.

**Consumer Financial Protection Bureau** - An agency of the United States government responsible for consumer protection in the financial sector.

**State Attorney General** - The top law enforcement individual at the state level in the United States.

**Data Protection Officer (DPO)** - An individual ensures, in an independent manner, that the European Commission correctly applies the law protecting individuals' personal data.

**Multi Factor Authentication** - An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

**Phishing** - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

**Whaling** - A highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email.