Proskauer

# Will NFT Piracy Compel Changes to the Digital Millennium Copyright Act?

**Blockchain and the Law Blog** on **March 16, 2022**

So you bought an NFT. You now own what is effectively an immutable electronic deed meant to record ownership of an asset, often a digital artwork. You probably paid for the NFT upfront—and if the artist is popular, you may have paid a substantial sum. This is one factor that has made the NFT market so attractive for artists working in digital mediums, many of whom struggle to effectively monetize their work. Like traditional art gallery sales, NFT sales allow creators to reap substantial profits from one-time instantaneous transactions, offering a lucrative alternative to gradually generating revenue through licensing, merchandizing, or streaming (though many NFTs also allow an artist to reap a percentage of future downstream sales, too).

But while NFTs have created a new outlet for many artists, the technology has also been a boon to digital content thieves. Pirates can mint knockoff NFTs with nothing more than a digital file and some cryptocurrency, then sell those knockoffs to unsuspecting collectors. Forged art is as old as art itself, but because they feature exact copies of their stolen works, knockoff NFTs are often indistinguishable from their genuine counterparts. Moreover, unlike other online infringers (think purveyors of illegal streams or unauthorized t-shirts), an NFT pirate only needs one unwitting buyer to take the "one-of-a-kind" virtual bait before disappearing with the oft-substantial payment into anonymity, meaning the entire scam can happen in hours or even minutes. Amidst the resulting piracy boom, it falls to creators to protect both their fans and their IP by scanning platforms for infringing NFT sale listings and issue takedown requests. But even when they succeed in getting a sale listing removed, the knockoff NFT itself remains immutably on its blockchain and the infringing content usually remains elsewhere on the web.

Undoubtedly, digital creators will fight to protect their work. The question is, are current copyright protection procedures—specifically, those under the DMCA—up to the task?

***The DMCA***

When President Bill Clinton signed the Digital Millennium Copyright Act ("DMCA") into law in 1998, the basic structure of copyright protection on Web 2.0 was born. Among other things, the DMCA created a series of safe harbors for online service and storage providers whose systems might be used to transmit potentially infringing material. To qualify for the DMCA safe harbors, most online service providers introduced "Notice-and-Takedown" systems, usually automated webforms, through which copyright owners could flag infringing user posts for removal. Though this has been critical to the growth of the internet as we know it, some content owners and commentators have expressed frustration with the Notice-and-Takedown system, advocating for, among other things, a "notice-and-stay-down" system to stop the reposting of copyrighted material already flagged and removed on a site. In 2020, the US Copyright Office released its own views on reform, issuing a report that called the system "unbalanced" and suggested ways that Congress could amend the existing takedown system, such as by requiring platforms to publish written repeat infringer policies. The burden placed on rights holders to flag infringing content is a hotly-debated issue, and with the recent boom in NFT art sales, this problem and the associated stakes have increased dramatically.

***Streaming Under the DMCA***

Though the DMCA was born years before mass streaming was technologically viable, Notice-and-Takedown adapted to the streaming world surprisingly well. With streaming, most content generates value indirectly and gradually, such as by driving website traffic and associated ad or subscription revenue. Digital piracy has evolved since the early days of the internet, from peer-to-peer file sharing to the current battles against stream-ripping services and pirated streaming sites. Under the DMCA, a copyright owner whose content has been pirated can, in theory, issue a takedown request and cut off an illegal (revenue) stream. The sooner the owner finds the unauthorized content and acts, the sooner the stream is cut off, but there is no point at which the owner will discover the content "too late" to issue a takedown (though don't forget the Copyright Act's three-year statute of limitations for bringing an infringement action). However, many content owners have found that fighting piracy can be like a game of whack-a-mole: Once one pirate link is taken down, a replacement pops up. Though by no means the perfect response to digital piracy, the DMCA has offered some means of protection for content creators, particularly since the advent of automated tools to send mass takedown requests.

***NFTs Under the DMCA***

NFTs have upset the DMCA apple cart in multiple ways. As discussed above, NFTs (unlike streams) can provide upfront lump-sum profits from one-off sales. This means that victims of piracy are now finding themselves under pressure to not just find and remove pirate listings, but to do this quickly, before a sale is consummated.

Complicating matters further, most art NFTs do not include an actual copy of the content, but instead merely point to a copy somewhere off-chain on the internet (*e.g.*, on a server). For a content creator who discovers a counterfeit NFT of his or her art, this means that Notice-and-Takedown is mostly limited to targeting and removing that NFT's marketplace listing (that is, the specific Web 2.0 page at which the NFT is offered for sale and the associated art is displayed)—but leaving the technically non-infringing token itself undisturbed on its blockchain, continuing to point anyone who accesses it to the off-chain unauthorized copy of the art.

Fortunately for artists, for now, leaving the token undisturbed on a blockchain is not a significant practical concern. This is because software programs that allow a user to view an NFT that he or she owns (*i.e.*, virtual wallets) do not directly communicate with the blockchain on which the NFT is stored. Instead, virtual wallets rely on intermediary software programs called APIs (application programming interfaces) to display NFT art—and these APIs are generally provided by the same companies that run the NFT marketplaces. That means that if an NFT marketplace removes an NFT sale listing, it can generally also prevent the NFT and its art from being displayed in a user's virtual wallet. Thus, at time of writing, issuing a DMCA takedown request to an NFT marketplace can be a relatively effective protective step for piracy victims. But if more companies (*i.e.*, companies other than those that run the NFT marketplaces) begin offering API access to blockchains, removing an NFT sale listing would not always necessarily prevent the NFT from still displaying in virtual wallets. In other words, content owners' inability to target tokens themselves could become a bigger problem.

There is a potential way to circumvent this problem: For NFTs that link to a copy of an artwork somewhere on the sever-based internet (the vast majority), the copyright owner can seek to torpedo the value of the NFT by sending a Notice-and-Takedown request to remove the content at its original location. This would lead to a "dead link" in the NFT, destroying its value the same way a land deed would be worthless if the island it described sunk into the sea. But this approach is complicated by the fact that NFTs increasingly use an alternative to traditional location addressing (*i.e.*, linking) called "content addressing." Content addressing works by assigning a unique hash to a piece of content, which applies to all copies of the content on a decentralized network no matter where on the network it is hosted. By decentralizing content in this way, content addressing avoids the vulnerability inherent in relying on a single server or single URL. This means that for a rights holder to stop a content-addressed knockoff NFT from displaying his or her content, a rights holder would need to find and request takedown of every infringing copy of that content in the decentralized network. Alternatively, a rights holder could use Notice-and-Takedown to target the services that allow users of the server-based internet to access content-addressed material, known as "gateways." But the problem here is similar: There is an ever-growing number of gateways that provide access to hashed content. An aggrieved rights holder, then, could end up playing a game of whack-a-mole that parallels the struggle with illegal streams described above.

Unfortunately for content creators, whether or not they are able to stop a knockoff token from displaying their art may often ultimately be irrelevant to the goal of stopping such tokens from propagating in the first place. This is because successfully eliminating a fake NFT does not mean much to a pirate who has already "flipped" the forgery—and made off with the plunder.

***Potential for Change***

In recent years, Congress has shown some bipartisan willingness to address perceived shortcomings with existing DMCA procedures. In 2020, Senator Thom Tillis released a discussion draft of his Digital Copyright Act, which would significantly reform the DMCA. At the time, Notice-and-Takedown seemed potentially ripe for change, but the COVID-19 pandemic stalled the reform effort. In 2022 and beyond, Congress may return to the question of updating the DMCA takedown regime in light of NFT piracy—not to mention the issues that may arise in the impending metaverse, Web 3.0 and beyond.

For now, though, sellers, buyers and platforms have little choice but to operate within the existing legal framework. For rights holders, this means becoming familiar with popular NFT marketplaces' notice-and-takedown systems, and what to do when an infringing listing is discovered. Rights holders seeking to sell legitimate NFTs could also consider certain blockchain-based minting and certification services that verify artists' identities and issue certificates of authenticity for minted NFTs. Similarly, marketplaces can continue to protect themselves from liability by meeting the DMCA's numerous safe harbor requirements, such as designating agents to receive takedown requests, terminating the accounts of repeat infringers, and cooperating with standard technical measures used by copyright owners to identify and protect their works. Though not required for safe harbor, some marketplaces are more proactive than others regarding piracy by implementing seller verification procedures, displaying "confidence scores" about each particular NFT for sale, and by scanning their inventory (and other platforms) for duplications or suspicious listings. Lastly, platforms can encourage buyers to perform their own basic due diligence before completing a sale to avoid ending up with worthless tokens. It is common for the terms of service for NFT platforms to contain certain disclaimers that indicate that the buyer bears full responsibility for verifying the identity and legitimacy of digital assets offered for sale on the platform.

Buyers should remember that verifying ownership of an NFT is not the same as verifying that the NFT is authentic (*i.e.*, authorized by the owner of the copyrighted work) or that no duplicate or similar NFTs have been or will be minted. Generally, a buyer's online sleuthing would include confirming that an account listing an NFT for sale is genuinely associated with an established artist or creator, either through checking the creator's own webpages (or contacting him or her on social media), or perhaps by using certain data analytics sites that can display the history of an NFT on the Ethereum blockchain. By taking these and other precautionary steps, the NFT community can protect copyright interests as well as enhance the reliability of, and thus confidence in, its digital market.

View Original

**Related Professionals**

- **David A. Munkittrick**
  Partner

- **Peter J. Cramer**
  Associate