

Professional Perspective

How the DMCA Applies to NFTs

Stuart Levi, MacKinzie Neal & Anita Oh, Skadden

**Bloomberg
Law**

[Read Professional Perspectives](#) | [Become a Contributor](#)

Reproduced with permission. Published May 2022. Copyright © 2022 The Bureau of National Affairs, Inc.
800.372.1033. For further use, please contact permissions@bloombergindustry.com

How the DMCA Applies to NFTs

Contributed by *Stuart Levi, MacKinzie Neal & Anita Oh, Skadden*

May 2022

The world of non-fungible tokens is replete with acronyms; however, one of the most important for rightsholders and NFT marketplaces is the DMCA—the Digital Millennium Copyright Act.

This 1998 act, which went into effect in 2000, protects online service providers from secondary liability for copyright infringement arising from works posted by their users, provided that the service provider implements certain steps required by the statute.

In this article, we examine some of the unique issues that arise in applying a copyright law that was written for “centralized” platforms to the decentralized ecosystem of blockchains and NFTs.

Background to NFTs

NFTs are immutable, digital certificates of ownership that are stored on a blockchain. Although NFTs are typically associated with digital works to signify ownership of art, music, and videos, they may also be associated with real-world, tangible items.

Importantly, for purposes of applying the DMCA, while an NFT is stored on a blockchain, the digital work with which it is associated is almost always stored off-chain, such as on a proprietary server or a decentralized file system. This is because most blockchains require participants pay a fee known as a “gas fee,” for storing or transferring files. Such gas fees can be cost-prohibitive for the large files that comprise most digital works associated with an NFT. Thus, NFTs typically include a metadata field with a pointer or link to the off-chain resource where the digital work associated with the NFT is stored.

A common misconception is that an NFT can always serve as a certificate of authenticity. In reality, while an NFT allows one to trace the provenance of a work back to the blockchain wallet address from which it was created or “minted,” unless one can independently verify the owner of that original address, it can be difficult to know whether an underlying work is properly licensed from the owner of the underlying intellectual property or whether the work is an infringing copy. As a result, NFTs have created numerous opportunities for infringers to mint NFTs associated with works for which they have no rights.

The situation is often exacerbated by the fact that certain marketplaces allow anyone to mint an NFT for free, only requiring payment of the applicable fees when the NFT is sold. Thus, a malicious actor could mint infringing NFTs without incurring any minting costs until an unsuspecting buyer purchases the NFT. This incentivizes infringing activity since the infringer only incurs costs if the infringement is financially successful, i.e., through the sale of the infringing NFT. In January 2022, OpenSea, which permits such free minting, disclosed on Twitter that 80% of the NFTs minted in this manner were associated with “plagiarized works, fake collections, and spam.”

Background to the DMCA

The DMCA was enacted well before the evolution of blockchain technology in response to a growing concern from internet service providers and websites that they could be held secondarily liable for copyright infringement because of infringing content their users might post. Since in most cases these service providers could not vet the vast amounts of content being posted by their users, they argued they should not be liable for infringing content.

The DMCA, which was codified into Section 512 of the Copyright Act, includes a safe harbor for service providers that host, store, or otherwise make infringing material available at the direction of a user if the service provider does not have actual knowledge that the material is infringing; it was not aware of facts or circumstances from which the infringing activity is apparent; or upon notification of a claimed infringement, it acts expeditiously to remove, or disable access to, the material. [17 U.S.C. 512\(c\)](#).

Section 512 sets forth the information a copyright holder must provide to satisfy the “notification of a claimed infringement” requirement, what has come to be known as a “DMCA takedown notice.” This section also specifies the process through which the initial poster can provide a “counter notification” to rebut the DMCA takedown notice and ensure content is re-enabled if it is found that poster actually had legitimate rights to the work.

Application of the DMCA to NFTs

At a baseline level, the application of the DMCA to NFT marketplaces is straightforward. NFT marketplaces can take advantage of the DMCA safe harbor by describing how a copyright owner can submit a DMCA takedown notice, and then implementing that process, including by allowing the individual or entity listing an NFT to provide a counter notification through which they can assert their own rights.

The purchaser experience in these cases may not be ideal, especially if they paid a substantial sum for their NFT. There are numerous examples of purchasers seeking to view their NFT, only to find it has been “delisted” for violating the site's terms of service as an infringing work and is no longer accessible through the site.

These purchasers will be reminded that, pursuant to the site's terms, their purchase was at their own risk and that they alone were responsible for verifying the identity, legitimacy, and authenticity of NFTs they purchase—a step that few purchasers may take. Such purchasers typically cannot recover the amount they paid to purchase the NFT, although some marketplaces will refund any service fees that were paid.

Importantly, the DMCA safe harbor protection does not apply if a service provider has taken an active role in what users of the service can post. This includes not only curating what is posted, but also can extend to providing detailed instructions regarding issues of layout, appearance, and content, or monitoring the mix of content on the site. See, e.g., *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002). In contrast, accessibility-enhancing activities such as processes to reformat posted or perform some technological change do not vitiate DMCA protection. See, e.g., *Mavrix Photographs, LLC v. LiveJournal, Inc.*, No. 14-56596 (9th Cir. 2017). NFT marketplaces need to be careful that their additional services and functionality do not put them in a position where the marketplaces are considered to have taken an active role in what users can post, such that DMCA protection is no longer available.

The unique nature of NFTs raises a number of interesting considerations when applying the DMCA. In most non-blockchain contexts, sending a DMCA takedown to a platform provider is all that is required for a copyright holder to protect its rights on that platform. That is because a work is usually displayed and stored by, or on behalf of, the same provider, and removal of the work by the service provider does not leave any loose ends. The same cannot be said for NFTs.

First, when an NFT marketplace honors a DMCA takedown request, it has merely prevented the work associated with the NFT from being displayed for sale on the marketplace. However, if the NFT was already minted, the platform may not be able to destroy or “burn” the NFT itself or recover it from the then-current owner. That is because one of the distinguishing features of blockchains is that once a record exists on-chain, it is, for all practical purposes, immutable, meaning it cannot be deleted or changed. Moreover, once an NFT is associated with a wallet controlled by the NFT owner, the marketplace has no ability to access that NFT or, in many cases, even have the means to contact the owner.

The one exception would be where the smart contract gives the NFT issuer the administrative right to change the then-current owner of the NFT. This would allow the administrator to change the wallet address associated with the NFT to a wallet controlled by the issuer or to a null wallet address that is not owned by any user and has no access key, known as a “burn wallet” or “black hole” wallet address. This renders the NFT inaccessible and unusable, though it will still technically exist on the blockchain.

From the perspective of the marketplace, the inability to burn the NFT may not be problematic for DMCA purposes. The DMCA only addresses the obligation to take down the infringing work; there is no requirement to destroy ancillary records relating to that work.

An NFT marketplace would have a strong argument that the NFT is just such a record, and therefore not covered by the requirements of the DMCA. While the Copyright Act empowers a court, as part of a final judgment or decree, to destroy “articles by means of which [infringing] copies... may be reproduced,” the NFT itself does not provide such capability since it merely acts as a pointer to where the work can be found. [17 U.S.C. § 503\(b\)](#).

An NFT marketplace may also have the technical ability to burn an NFT in situations where the NFT marketplace operates as a “walled garden,” where all NFTs are associated with the marketplace's digital wallet on-chain, while the then-current owner of each NFT is recorded in an off-chain ledger. Such marketplaces could transfer an NFT associated with an infringing work to a burn wallet. Nonetheless, as analyzed above, the fact that these marketplaces may have the technical capability to burn an NFT in certain circumstances likely does not translate into an obligation to do so under the DMCA.

The fact that a marketplace no longer displays an infringing work as available for sale may not be sufficient for some copyright owners if the NFT still exists and still “points” to where the infringing work can be found. This is because even if the work cannot be posted for sale on the marketplace, the owner of the NFT may still be able to see a display of the infringing work through their digital wallet. Whether that capability exists depends, in part, on the type of wallet the user has and the software that wallet uses to retrieve and display the digital work.

In addition, rightsholders may be concerned that the NFT and the associated work could be displayed on future marketplaces before the rightsholder has the chance to send a DMCA takedown notice. The rights holder may therefore simply want the infringing work associated with the NFT to be taken down from wherever it is stored. This leads to the second complicating factor with applying the DMCA to NFTs.

The digital work associated with an NFT may be stored in a variety of different ways. In some cases, the marketplace maintains these works on its own proprietary services or may store them on the servers of a cloud provider. In these cases, the marketplace could take the additional step of removing the infringing work from the storage system it owns or controls.

Whether it has the legal obligation to do so under the DMCA if it no longer displays the work is less clear, because the DMCA only requires that a service provider “remove, or disable access to” the infringing material. [17 U.S.C. 512\(c\)](#). Disabling access to the infringing work by removing it from being listed on the marketplace may satisfy the DMCA without the additional step of removing the work from its servers.

However, in keeping with the decentralized ethos of Web3, many digital works associated with NFTs are themselves stored on decentralized file systems. In general, in such systems, a work is duplicated across numerous file servers and assigned a content identifier. When someone searches for that content, they are searching for a cryptographic hash of what that content is, not for a location of where that content can be found. Thus, the metadata in an NFT will point to a digital work on these systems using a content identifier, or CID, and not a location identifier.

Decentralized file systems are an important alternative to many centralized storage systems since they eliminate a single point of failure. However, the inherent appeal of a decentralized network adds a layer of complication for copyright owners. There is no practical way for a copyright owner to track down each server where an infringing work might be stored and get it taken down, especially since works are often split into smaller files that can be spread across multiple storage nodes. Moreover, operators of storage nodes on a decentralized platform are often compensated by the amount of data they store, and penalized if their storage capacity decreases, creating a disincentive for them to remove content.

One possible option is for copyright owners to contact the “gateways” that serve as a bridge between web applications and some decentralized file systems. These gateways often include their own DMCA takedown procedures and allow copyright owners to request that the gateway block or otherwise make the infringing material unavailable. As more gateways proliferate, a rightsholder would need to fight a multi-front battle to make an infringing work inaccessible.

Conclusion

NFT marketplaces can enjoy important protection from secondary liability for copyright infringement through the DMCA, provided they develop and implement the policies and procedures required under the DMCA and do not curate their collection or provide the types of tools that take them out of DMCA protection. Rightsholders should take advantage of the DMCA takedown procedures, but remain mindful of the practical limitations of having the NFT itself, and possibly the digital work, taken down.