Crowell

Retail in the Metaverse and Beyond

Insights for corporate counsel and retail executives

Unlocking the Potential of Your Brand

Retailers are leveraging the metaverse to transform the shopping experience, drive customer engagement and loyalty, and unlock new business opportunities. In this collection of Crowell & Moring's latest insights and analyses, we delve into the legal challenges that retailers face as they move into virtual and augmented reality, from ownership of digital assets to data privacy concerns.

And we are just getting started. Today's concerns about the intellectual property implications of creating and selling virtual goods, or the potential liabilities of hosting user-generated content, will turn into concerns yet to be imagined. Will your digital avatar have its own set of rights to publicity? Can someone be injured in a virtual store? Will we even call it the "metaverse" once this digital realm is more integrated into our day-to-day lives? It is our hope that these articles will help retail executives and their corporate counsel protect their companies' digital assets, leverage the metaverse to grow their businesses, and, ultimately, spot what legal issue is next around the (virtual) corner.

Preetha Chakrabarti
Partner
Advertising and Brand Protection
Co-leader, Crowell's Metaverse Working Group
Co-editor, Retail in the Metaverse and Beyond

Dalton Hughes
Associate
Intellectual Property
Co-editor, Retail in the Metaverse and Beyond

Step Inside

Three Key Challenges for Companies Entering the Metaverse

Brands, ownership, and jurisdiction for retailers

Preetha Chakrabarti, Emily Kappers

The term "metaverse" was coined by science fiction novelist Neal Stephenson in his 1992 dystopian thriller, "Snow Crash." Stephenson's metaverse allowed users to create almost limitless avatars and experience a new, virtual world firsthand, accessible through virtual reality goggles or "terminals." Thirty years later, what was once science fiction is now reality. Immersive and interactive 3D digital worlds housed on a variety of virtual platforms are gaining in both prevalence and popularity—accessible through virtual or augmented reality goggles, smartphones, and computer screens. Each virtual platform, or metaverse, functions as its own world, with unique rules, currency, and user experiences.

Collectively, these platforms make up the metaverse as we conceive of it today, with the ultimate goal of allowing users to move seamlessly across worlds, maintaining their avatars' purchases and collected experiences as they go. The metaverse relies on blockchain and cryptocurrency, both highly trusted but decentralized technologies, and user input to accomplish this goal. This reliance on decentralized ownership and access, when coupled with users' ability to craft a fantastical persona and reality for themselves, presents a gold mine of fresh opportunities for companies to reach and interact with current and new consumer bases. It also presents a host of novel legal issues companies must contend with as the metaverse continues to take shape. This article explores three key legal challenges metaverse visitors or users will encounter as this new world expands, evolves, and further integrates with daily life.

1. Brands in the metaverse

The metaverse mimics daily life: It's a virtual platform for users to socialize, play, shop, and otherwise interact with others from the comfort of their own physical homes. This enhanced version of reality demands replication of many places, products, and activities found in the physical world. And in many respects, the presence of physical-world brands in the metaverse provides the necessary bridge between reality and VR. Recognizing this need, many brands already have or are considering a leap into the metaverse. However, as brands grow omnipresent in this new reality, ownership and enforcement of brands becomes tantamount. Brand owners should craft legal strategies, including trademark filings and policing and enforcement policies, to both build and enforce their brands in this new frontier.

Brand owners are currently entering the metaverse in droves. Retail giants like Nike, Gap, Adidas, Burberry, and Louis Vuitton, to name a few, are setting up virtual shops; fast food giants like Wendy's, Chipotle, and Taco Bell are offering interactive virtual restaurants and minting NFTs[1] with aplomb; and even historically conservative brands like HSBC and JP Morgan are getting on board with offerings on The Sandbox and Decentraland, respectively. The successful launches of Nike's recent CryptoKicks campaign, Wendy's Wendysverse on Meta's Horizon Worlds, and JP Morgan's Onyx Lounge, so named after its Ethereum-based suite of services, are early signals that brands are here to stay in this new space.

[1] Brands are using NFTs to drive customer engagement. Fast food giant Taco Bell was early to leverage NFTs, launching a series of 25 taco-themed NFTs in early March 2021 whose initial profits were earmarked for Taco Bell's Live Mas Scholarship. The series sold out in under an hour, further increasing consumer demand. A recent resale of one of Taco Bell's taco-themed NFTs netted over $180,000. Later that same year, in November 2021, McDonald's launched a sweepstakes for a chance to win one of 10 limited-edition McRib NFTs in honor of the McRib sandwich's 40th anniversary. The sweepstakes coincided with the return of the McRib to McDonald's restaurants.

Beyond staking an early claim in this new world, brands are seeking new and innovative ways to interact with consumers. Epic Games, an interactive entertainment company known for games like Fortnite, recently announced a partnership between itself and WPP, the world's largest advertising company, to create "custom brand experiences" accessible in the metaverse. Likewise, Nike's now yearlong partnership with Roblox, an online gaming platform, allowed it to enter the metaverse with its very own Nikeland—a virtual world inspired by Nike's real-world Oregon headquarters where users can compete in real and fanciful games (parkour dodgeball, anyone?), deck themselves out in Nike gear, and build their own games within the bounds of Nikeland. The customizable and unique nature of the metaverse allows many brand owners to craft novel interactions like these between users' avatars and their products, and it is likely to become more commonplace as the metaverse (and its users) continue to grow and evolve over the next decade.

Despite many early, authentic adopters, the metaverse abounds with enterprising third parties looking to capitalize on brand cachet and this largely unexplored (and unclaimed) frontier. Fashion brands especially are experiencing a significant uptick in bad faith trademark filings targeted toward the metaverse. And these brands' well-known marks are ripe targets for inclusion on copycat and counterfeit virtual outfits ("skins"), NFTs, and more. Recent litigation, like that filed by Hermès[2] and Nike[3] over the unauthorized use of trademarks and trade dress, indicate the metaverse is not just a new frontier for users but also a new forum for litigators.

New trademark filings for the metaverse

With the growing ubiquity of the metaverse, brands should consider how they are carving out space in the virtual realm. Is a brand erecting a virtual store, selling a virtual product or experience, or minting an NFT? And where does the brand plan to expand in the next five years? Does the brand even plan to enter the metaverse? After asking and answering these baseline questions, brand owners should consider conducting a critical review of their current portfolios to identify holes in their coverage.

In most cases, brand owners should seek trademark registrations for any goods or services they plan to offer in the virtual world, with the understanding that, at least in the United States, actual use of a mark with these goods or services is required before a registration will be issued. While standardized specifications of goods and services remain in flux (and are largely dependent on U.S. Patent and Trademark Office preference), most filings directed to the metaverse focus on downloadable virtual goods in Class 9; retail store services for virtual goods or entertainment services in Class 35; financial services in Class 36; and online, non-downloadable virtual goods in Class 42. Brand owners are also seeking protection for various entertainment services in Class 41 and restaurant services in Class 43 that they plan to launch in this new VR.

As part of any coverage assessment, brand owners should at least consider trademark filings in the core countries they currently or plan to operate in and in any countries known for counterfeiting or trademark squatting. Keeping in mind that the United States' "use prior to registration" requirement is generally the exception, not the norm,[4] brand owners may also consider seeking protection for their metaverse offerings globally, although this strategy comes with significant startup and maintenance costs. It remains to be seen how brand owners' registered rights will be enforced in the borderless metaverse. And a more conservative filing strategy as we wait and see is to protect at least a brand's primary mark in as many jurisdictions as possible.

At the other end of the spectrum, brands that are not planning an entrance into the metaverse may wish to rely on their current trademark rights for physical-world goods and services. It is an open question as to how trademark offices and courts will translate brands' rights and registrations for physical goods and services to these same offerings in the virtual realm. In certain instances, trademark rights and registrations for physical goods or services may be found to translate to these same virtual goods or services. However, at least thus far, these instances are largely applicable to very well-known or famous brands,[5] and most brand owners would do well to seek protection in both the physical and virtual worlds, even if these applications are merely defensive.

Despite many early, authentic adopters, the metaverse abounds with enterprising third parties looking to capitalize on brand cachet and this largely unexplored (and unclaimed) frontier.

[2] Hermès filed a trademark infringement suit against Los Angeles-based designer Mason Rothschild for creating and selling faux fur digital renditions of the luxury Hermès Birkin handbags and using a collection of 100 NFTs, titled "MetaBirkins," to authenticate the digital images. Rothschild filed a motion to dismiss the suit, arguing the digital images are "art" and entitled to First Amendment protection. Rothschild's motion to dismiss was denied, and on Feb. 8, 2023, a Manhattan federal jury found that Rothschild's "MetaBirkins" infringed and diluted the Hermès trademarks for its globally renowned Birkin bags. The jury further found that Rothschild cybersquatted on the MetaBirkins.com domain name. This outcome signals that trademark infringement in the virtual world has consequences—just as it would in the real world. The case is Hermès International and Hermès of Paris, Inc. v. Mason Rothschild, 22-cv-00384-JSR (S.D.N.Y.).

[3] Nike filed suit against StockX, an online marketplace that primarily resells sneakers, for creating and selling NFTs featuring Nike sneakers. StockX responded that its NFTs were tied directly to a physical Nike shoes, and the complained-of NFTs were merely used to authenticate the shoes it sold. Nike sought leave to amend its complaint, arguing it recently bought sneakers StockX verified as authentic in a bid to add counterfeiting and false advertising claims to its lawsuit. Most recently, and in support of its arguments, Nike submitted a letter to the court describing StockX's sale of 38 purportedly counterfeit Nike sneakers to a collector, following Nike's determination that the sneakers were fakes. The case is ongoing and is Nike, Inc. v. StockX LLC, No. 1:22-cv-00983-VEC (S.D.N.Y.).

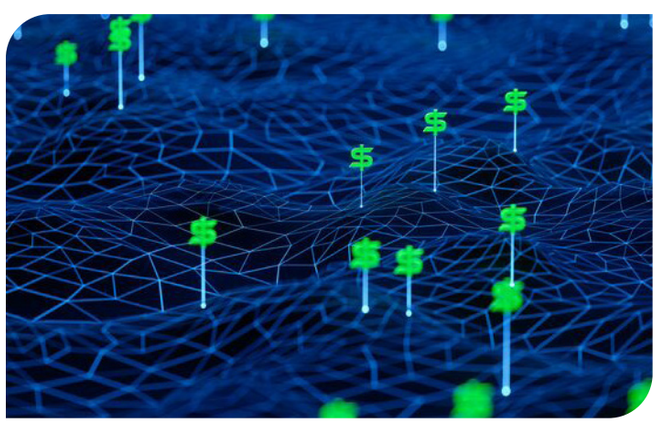
[4] Although, most countries do have nonuse cancellation procedures if a challenger can prove a trademark has not been used with its registered goods or services for a continuous period of time. While it varies country by country, a registration can usually be challenged after three to five years of continuous nonuse.

[5] In late 2021, U.S. trademark applications to register the marks PRADA and GUCCI with metaverse-oriented goods and services were filed by two third-party individuals who were affiliated with neither Prada S.p.A. nor Guccio Gucci S.p.A. The U.S. Patent and Trademark Office refused both registrations, in part due to a likelihood of confusion with Prada and Gucci's registered, and by most respects famous, trademarks for physical-world offerings.

Brand enforcement: the metaverse is a land of opportunity … for infringement

The metaverse is expansive and continues to evolve at a rapid pace. At the time of this article's writing, over 500 companies are building the metaverse in some way. The potential for infringement of brand owners' rights therefore abound and the onus to police and enforce their rights is placed directly on brand owners' shoulders.

Creating a cohesive enforcement strategy in the metaverse presents significant challenges, and the applicability of more-traditional enforcement methods in this new landscape is fairly untested. By its nature, the metaverse is decentralized, and most blockchain-based virtual platforms do not sit on a single server. This severely complicates enforcement efforts and removes many of the traditional enforcement tools brand owners utilize in the physical world. Nevertheless, building a well-defined enforcement strategy, which may include variations on the tools brand owners are already familiar with, will better equip brand owners to identify and protect their rights in this new frontier.



Monitoring programs

Brand owners should implement monitoring programs to identify unauthorized use of their marks in the metaverse. Adopting a monthly or bimonthly internal monitoring routine[6] of (1) major public blockchain transactions, (2) metaverse discussion boards, and (3) major virtual platforms, like Decentraland, The Sandbox, or Roblox—paying special attention to avatar skins, accessories, and other assets and user-created worlds—will help identify potential infringements. Educating monitors on what to look for and how to operate on these platforms is key. For example, monitors should be well versed in a brand's core trademarks, trade dress, goods, and/or services; able to navigate between virtual platforms, discussion boards, and NFT marketplaces; and capable of tracking and reviewing blockchain transactions.

The metaverse is still in its infancy, and formal third-party monitoring services are not yet fully equipped to provide services in this virtual landscape. But they are on the horizon. Many new companies are building technology to assist with enforcement efforts in this ever-evolving and decentralized space. This new technology is calculated to identify and challenge unauthorized use of brand owners' rights, and for certain offerings like NFTs, this technology is already available and gaining popularity.

Takedown notices

Like monitoring programs, takedown notices, in some instances, are viable enforcement tools in the metaverse. Takedown notices offer brand owners an efficient and inexpensive option to enforce their rights and demand the immediate removal of unauthorized or otherwise infringing content. These notices work hand in hand with an effective monitoring program. Brand owners must be aware of unauthorized uses of their marks before they can request the content's removal.

The efficacy of takedown notices in the metaverse is still platform specific, however. Many NFT marketplaces, like OpenSea or even Sotheby's metaverse, provide in their help centers access to Digital Millennium Copyright Act and takedown notice forms for both trademark and copyright infringement. In many cases, however, review of these notices is subject to marketplace employees' discretion. Moreover, many virtual platforms currently lack takedown procedures or leave the review of alleged infringements up to the vote of a decentralized portion of the platform's users or content creators. Again, the metaverse remains in its infancy, and brand owners can expect use of both the DMCA safe harbor provisions for platform hosts and the availability of takedown notices to become more commonplace as these platforms evolve.

Cease and desist letters and litigation

Brand owners may also look to more tried-and-true methods of enforcement, like escalating efforts with cease and desist letters and litigation. The decentralized nature of the metaverse will likely prove to be an initial impediment to both actions, making it difficult to identify an infringer let alone send a letter to or serve a complaint on them. Further, the metaverse is built for social interaction and the sharing of information. While sending an assertive cease and desist letter may prove satisfying in the moment, brand owners should keep in mind they are addressing tech-savvy and largely anonymous parties who can easily share communications to a large, global audience with a few keystrokes. As we have already seen from various letters being shared on social media and in comedy shows, cease and desist letters can go beyond their purpose of getting a behavior to stop and either garner laughs and further appreciation for a brand (see Netflix's infamous 2017 "Stranger Things" letter) or be a brand's undoing.

Partnerships and licensing agreements

Brand owners may also consider entering into partnerships—like Nike and Roblox's Nikeland endeavor or the recent collaboration between Fortnite and WPP—or other licensing agreements with various virtual platforms. While undoubtedly less traditional than the foregoing enforcement strategies, official partnerships and licensing agreements between brands and virtual platforms in the metaverse will allow brand owners further control over their rights in these environments. These partnerships will also provide brand owners easier entrance into the metaverse.

2. 'Real' property ownership in the metaverse

Property in the metaverse is no new frontier to experienced users. Second Life, largely considered one of the first true "metaverses" in a 3D format, began selling virtual land in 2003. Today's pricing for a 65,000-square-meter parcel on a premier island on Second Life costs $349 dollars, with a $229 monthly maintenance fee[7]. Nowadays, the new frontiers are 2D and 3D metaverses offering cryptocurrency bidding for virtual lands, with many premium Decentraland parcels hovering around 250 ether, or $324,000, at the time this article was written.

[6] Memorializing all identified infringements with a date and time stamp and URL address is integral to any monitoring program and helpful in enforcement efforts against these infringements.

[7] Second Life island pricing is standardized by world region: Private Pricing (https://secondlife.com/land/private-pricing).

The application of law and legal jurisdictions continues to be a sticky and evolving consideration for the metaverse.

One of the most important considerations for property ownership in the metaverse is taxation. Charges can vary based on the physical location of the purchaser, the location of the seller, or the country where the server for a website is hosted. Some metaverses will deduct taxes and add land-based value-added taxation on top of a land purchase,[8] while others will place the full burden of tax deductions on the buyer.[9] Additionally, crypto-based metaverse platforms like Decentraland, Solana, and The Sandbox treat land as NFTs, which implicates token tax reporting issues. EVE and Second Life, however, use a virtual land tax to avoid NFT speculation and fluctuation in their metaverses and take a hard stance against NFT usage for land in general.

Contractual land purchase agreements currently mimic physical land purchases, and mortgage agreements popping up for metaverse worlds appear to contain the same legal recuperation procedures. For Ethereum-use metaverses like Decentraland, Cryptovoxels, and Somnium, upstarts like TerraZero Technologies are offering mortgages for virtual property based on ones for real physical land. In these contracts, users and brands should be wary of the implication of frequent changes to platforms' terms of service, as minor changes to land use terms could affect value much quicker than, say, a slow change to a city's municipal code.

3. Jurisdiction and enforcement of laws

The application of law and legal jurisdictions continues to be a sticky and evolving consideration for the metaverse. Some jurisdictions have begun to hash out regulations and policies for metaverse worlds, VR, and augmented reality—like the European Union Virtual and Augmented Reality Industrial Coalition—to formalize and centralize tax and infrastructure requirements. But that still leaves the question of what laws from where apply to an individual's or a business's use and actions in the metaverse. Video game worlds with usage of fiat currency and celebrity likenesses may offer insights into how they would apply to a metaverse. Many lawsuits have been filed against Fortnite and Epic Games for unauthorized use of intellectual property, namely dances that characters can emote.

These lawsuits have initiated claims of copyright infringement under federal U.S. law in the Central District of California, as the plaintiff was located from and harmed in that venue, while Fortnite was also offered for sale there.[10] For NFT-related lawsuits, courts currently appear to favor jurisdiction of where the asset owner is domiciled.[11] Relatedly, in-metaverse promotions and loot boxes are being banned in certain countries, like Spain, which requires companies active in the metaverse to carefully assess any promotional offerings for metaverse assets that are accessible to users worldwide.

An additional layer of challenges appears when a metaverse is accessed by VR, or even AR. With new technologies quickly taking off for VR headsets, like eye tracking, facial recognition, and haptic feedback, enterprises in the metaverse must be cognizant of user-to-user interactions and what limitations are disappearing in comparison to real-life interactions. Even though metaverse platforms like Meta's Horizon Worlds have robust terms of service to protect themselves, user-to-user interactions are nearly infinite and can lead to negligence by all parties.

U.S. courts, however, have thus far not opted to apply a legal duty of care to virtual world designers, even when it results in physical harm. For example, in one case from 2011, Google was found not liable for injuries the defendant suffered after being hit by a car after Google Maps showed that a street was empty on its virtual map.[12]

On the other hand, user-to-user interactions in the metaverse can lead to trouble for users or land owners, even though a metaverse platform owner is potentially protected through terms and conditions. Assault on a virtual body part with a virtual attack, with no damage physically to a real human, is likely not actionable.[13] However, interactions that trigger immediate assault to eyes or ears may be, as it is the main way of interacting with a metaverse and can quickly cause harm before a user can take off a headset or close a laptop. For example, a brand creating a world with robust flashing lights without a warning or opt-out feature could be held liable for an epileptic attack. Some criminal precedent is already there, as an alleged cyberstalker was arrested by the FBI in 2017 for sending images over Twitter to a known epileptic user that resulted in the user having a seizure.[14]

[8] Linden Lab Official: Value Added Tax (VAT) Frequently Asked Questions – Second Life Wiki.

[9] Decentraland's terms state: "You are solely responsible for determining what, if any, Taxes apply to your LAND parcel related transactions, and any other transaction conducted by you. The Foundation does not, and will not, have any insight into or control over any transactions conducted by you in Decentraland, and thus is not responsible for determining the Taxes that apply to your transactions entered through the Tools or otherwise involving any LAND parcel, or any other related transaction, and is not to act as a withholding Tax agent in any circumstances whatsoever." Decentraland.

[10] See, e.g., Alfonso Ribeiro v. Epic Games, Inc., CDCA 2:18-cv-10412 (2018).

[11] See, e.g., Fetch.AI Lrd & Anor v. Persons Unknown Category A & Ors, [2021] EWHC 2254 (Comm.), July 15, 2021.

[12] See Rosenberg v. Harwood, No. 100916536, 2011 WL 3153314 (D. Utah May 27, 2011).

[13] For more on recent developments in virtual torts, see Nicole J. Ligon, "Virtual Assault," 5 U. Ill. L. Rev. 1203 (2022).

[14] Maryland Man Arrested for Cyberstalking | OPA | Department of Justice.

Preetha Chakrabarti
Partner, New York
Advertising and Brand Protection

Emily Kappers
Counsel, Chicago
Advertising and Brand Protection

Copyright in the Metaverse: What Advertisers Need to Know

Sari Depreeuw, David Ervin, Kyle Pham

The landscape for advertisers and marketers has been shifting in an exciting direction. Over the past decade, industries have firmly embraced multichannel communication and brand building, creating a strategy based on a mix of traditional media and social media, with the persona of the "influencer" as the modern incarnation of brand communication. However, early adopters are on to the next, new universe for connecting with a different, wider, and younger audience around their brands: the metaverse.

Major brands, including luxury brands and celebrities, have made their first steps into virtual environments, with famous examples such as Travis Scott's concert in Fortnite (attended by over 12 million Fortnite players, according to Epic Games, and still available on YouTube), the creation of stores or gardens, or Balenciaga's presentation of its Fall 2021 collection.

As with every new technology that opens a whole new world of experiences, the more widespread accessibility of the metaverse raises legal questions related to the protection of privacy and personal data, consumer protection (minors in particular), hate speech, and the physical and psychological integrity of players. The metaverse also provides novel creative opportunities, as the human imagination is no longer limited by physical constraints. In this article, we will explore some of the copyright issues advertisers may want to consider when venturing into the metaverse.

The metaverse, a natural extension of the physical world?

The first and most obvious step for an advertiser may be to bring their existing portfolio, often carefully built up over many years, to the metaverse. Louis Vuitton, for example, created a game (Louis the Game) to celebrate its 200th birthday in which users collect NFTs and are taken through the key moments of the brand's history.

Music labels, festival organizers, and fashion houses with large catalogs of historic material may be eager to explore the opportunities offered by the metaverse to present their older work to newer generations and keep their legacies alive. However, these exciting new exploitations, especially in combination with artificial intelligence-powered technologies to virtualize living or deceased artists, should be preceded by a careful verification of the rights of all creators involved. The authors (composers, song writers, directors), the performers, and the producers may have licensed their exploitation rights under copyright or related rights, but these licenses may not cover these new forms of exploitation. Similarly, the digital reconstruction of a real-life flagship store may be hindered by the copyright the architect may have on their design.

The authors… may have licensed their exploitation rights under copyright or related rights, but these licenses may not cover these new forms of exploitation.

Especially when the contracts date back to an era when the metaverse was not more than a faint idea in the minds of sci-fi writers, local copyright laws may not allow the transfer or licensing of rights beyond the forms of exploitation existing at the time of the contract. In those cases, the advertiser may not use their real-life world catalogues in their new virtual environment until they have acquired the permission to do so (possibly in exchange for additional remuneration).

In addition, the protection of the image and likeness of celebrities may raise some obstacles to their transformation into avatars and projection of adapted video recordings in an unanticipated virtual world. The question of who "owns" what in this ecosystem of creation shall be an important one to consider across jurisdictions.

Avatar-generated content

The metaverse's focus on "avatar-generated" content cultivates a new environment and a new window for human creativity. Younger players in particular will quickly find the tools they need to express their identities by carefully picking the attributes of their avatars and making videos and music performed by their avatars in a 3D environment. In this way, they will be able to share their creative urges with an audience they may not be able to reach in the brick-and-mortar world.

While the conditions for protection under copyright may not be the same everywhere, it is safe to assume that many of these fantasy-induced creations meet the threshold for protection. Who may be considered the author, by contrast, may not be so straightforward.

Many European countries consider the (human) individual as the author and therefore the initial holder of moral and economic rights, but this may be different in the U.S. where legal entities may vest the copyright in a company or other legal entity. Advertisers working with influencers or other creative minds benefit from clear contractual provisions confirming the transfer of copyright (and related rights, such as performers' or producers' rights) for all territories and all jurisdictions.

Platforms

When advertisers decide to take their business to existing virtual worlds, the extent to which they can still exert control over their assets is governed not only by the laws of the real world but also by the contractual terms of the provider of the virtual world.

Those terms illustrate the different approaches the platforms are adopting to the use and reuse of content produced by the users (including advertisers).

Platforms, such as The Sandbox, Roblox, or Meta (in relation to Horizon), impose upon the users an irrevocable, worldwide, royalty-free license to use the protected user content for the purpose of including that content in the virtual world. In addition, Meta requires users to accept a ditto license for the purpose of marketing and advertising Meta's Horizon Worlds.

These terms should catch advertisers' attention: The description of the authorized purposes is often vague (to the platform's advantage), but, more importantly, the irrevocable and perpetual nature of the licenses granted to both the platform and its users make it impossible for the advertiser to control the (commercial) use of their content, even after they decide to leave any given virtual world.

Decentraland, by contrast, takes another approach and specifically states that neither the foundation nor the decentralized autonomous organization behind Decentraland acquires any intellectual property rights over the user's content. Similarly, no IP rights underlying the NFTs are transferred to Decentraland's foundation or the DAO—but it is required that the transfer of an NFT entail the transfer of the IP rights underlying the NFT to the purchaser.

This variation in platform ownership and license term scope regarding underlying copyrights in virtual assets and works can have a significant impact on advertisers, their specific promotional campaigns in the metaverse, and future commercial rights to those assets and works. A number of initial questions require careful attention. For example, is the advertiser willing to limit use and commercial exploitation of its assets and works on the initial metaverse platform or does the advertiser need the flexibility to move the assets and works to other platforms? Does the advertiser have the underlying rights and permissions necessary to grant broad use rights to the platform and its users? Selecting a metaverse platform therefore becomes a threshold issue for advertisers to consider before launching a program in the metaverse.

Where is the NFT in all this?

While the metaverse cannot be reduced to the issue of NFTs, these popular tokens may play an important role in the strategy of any brand in the metaverse. NFTs are unique tokens stored on the blockchain that may be used to certify authenticity and ownership of the associated digital asset or creative work, and they provide a transparent mechanism through which the value of those digital assets or works can be documented and transferred.

Creations in the metaverse do not need to be NFTs. However, it may be useful for brands to mint NFTs of their creations (and make sure no one else does) if they want to sell unique (and therefore scarce) digital representations of their music, videos, photos, fashion accessories, or other works. While the sole minting of an NFT arguably does not entail any acts protected under copyright, players will barely show any interest in buying and selling NFTs if the musical performance, video clip, image, or accessory is not associated with the NFT.

Selecting a metaverse platform, therefore, becomes a threshold issue for advertisers to consider before launching a program in the metaverse.

Advertisers should monitor the main NFT platforms and the existing instances of the metaverse for counterfeits of their catalogue or repertoire.

Realistically, the right holders will have to authorize the offer of NFTs to which their works, performances, or recordings are linked. If the existing contracts do not cover this particular form of exploitation, the distributor should make sure that they negotiate a contractual extension of the existing license.

When an established brand issues NFTs of their catalog of existing creations or new work, it will inspire trust for the public, so the NFT can function as a guarantee of provenance. Considering that anyone can mint any digital file—regardless of content, quality, or legitimacy—the buyer will be able to rely on the reputation of the issuer to assess the quality of the NFT and the veracity of the license associated to it.

Inversely, advertisers should monitor the main NFT platforms and the existing instances of the metaverse for counterfeits of their catalog or repertoire. While the limits of acceptable use such as creative expressions and transformative use may be blurry at this time (awaiting the decision in the Hermes Int'l v. Rothschild MetaBirkins case), advertisers are wise to adopt an IP strategy for the metaverse. Informed by the scope of applicable metaverse platforms terms, such an IP strategy should cover copyright and related rights, as well as trademarks and image rights of the artists with whom they may be working—provided they do indeed hold the rights to these new forms of exploitation.

Major metaverse takeaways

It is clear that the future of the metaverse also involves a future of lengthy discussion and legal ruminations regarding IP rights that will impact how advertisers engage in this new virtual world. As we all navigate this exciting innovation, it may be helpful to remember the following:

- Metaverse rights will differ from country to country, following differences in copyright doctrines.
- Advertisers who wish to develop a presence in one or more of the virtual worlds, expanding on the exploitation of their existing portfolios, should ascertain that they have acquired all relevant IP rights (in particular, copyright, related rights (performers', producers' rights) and trademarks rights) and image or publicity rights.
- As to the virtual world's native creations, real-world copyright rights may vest in the authors and may be transferred to the advertiser (under contract, under any legal presumption, or other assignment mechanism).
- The terms of use of the platform providers may, however, impose usage rights on the existing or native creations (including "perpetual", "irrevocable," or even "exclusive" licenses), which the advertiser may not wish to accept.
- Advertisers who engage in experiments with NFTs should have a clear understanding of the legal implications of such offerings, the warranties offered to the NFT buyer as to the object of the NFTs, and the relation to the licensed content.

Sari Depreeuw
Partner, Brussels
Advertising and Brand Protection

David Ervin
Partner, Washington, D.C.
Advertising and Brand Protection

Kyle Pham
Associate, Washington, D.C.
Advertising and Brand Protection

Privacy and Cybersecurity for Retailers in the Metaverse

What privacy and cybersecurity issues should retailers consider before entering the metaverse

Kristin Madigan, Jacob Canter, Alexis Ward

Imagine a customer walking into a clothing store. She browses the racks, selects a few items, and asks the sales associate for a dressing room. She walks into the dressing room and tries on the clothes. Then she heads to the counter, pays for some of the items, and leaves.

We take for granted—because it's so obvious—how much information is transferred from the customer to the company in this very normal situation: her height, weight, clothing preferences, credit card number, and bank account information. If the sales associate is discerning, the company might also learn why she prefers some clothes over others or what other shops she frequents.

What happens when the customer is in the United States, the racks of clothes are in France, the dressing room is in the United Kingdom, and the counter to pay is in Japan? Sounds crazy! But in the metaverse, it actually is possible.

The metaverse is a digital world seamlessly integrated into the physical world. In the most ambitious visions of the metaverse, people around the globe use digital avatars to work and socialize together in a virtual cyberspace. This active commercial environment could make the metaverse a valuable location to access potential customers, and retailers could also make the metaverse a more desirable place to visit.

However, the metaverse also brings risk. In nearly every jurisdiction across the globe, consumer privacy laws regulate the collection and use of customers' personal information obtained over the internet. Complying with these laws in a traditional setting can already be complex. This article identifies some of the most pressing issues that could arise for retailers in the digital future of the metaverse.

Which data privacy laws apply in the metaverse?

A California retailer in the metaverse may host virtual customers from Virginia, France, and China all at the same time. In this example, the California retailer would not only be responsible for complying with California privacy laws, it also must comply with the privacy laws of Virginia, the European Union, and China.

Each one of a retailer's virtual visitors may be protected by one or more regional privacy law regimes, and retailers are responsible for complying with them all. This creates challenges. Retailers must take reasonable steps to determine each customer's location, determine whether that location has additional or different laws related to the use and collection of personal information, and, if so, comply with those laws, which sometimes may require making business changes to how information is collected, stored, and used. On top of these practical challenges, retailers will need to address how these privacy regulations interact and how they can comply with the several different and possibly conflicting regimes at once. Major online platforms deal with challenges like this regularly, but the metaverse makes this a problem for much smaller retailers for the first time.

How to handle international data exchanges in the metaverse

One of the key benefits of the metaverse is that retailers aren't limited by physical boundaries. A Belgian citizen could visit the store of a U.S.-based retailer without leaving home. However, this simple interaction necessarily includes the transfer and exchange of data across international borders.

Body movements, the smallest glances, changes in vocal tone, heart rate, proximity to other avatars—all of this information is theoretically collectible in the metaverse.

Retailers processing this type of international transaction will need to be aware of international data transfer and data localization laws. In the metaverse, as in today's digital space, international data transfer laws will govern exchanges of information across borders, while data localization laws will dictate where the information can be stored. Retailers must be aware of these laws and take steps to remain in compliance.

For example, a straightforward way to stay within the law for transfers to and from the EU is to rely on standard contractual clauses. SCCs are model contractual clauses preapproved by the European Commission to ensure adequate data protection during international exchanges of information. Also, retailers in the U.S. and the EU may soon be able to participate in the EU-U.S. Data Privacy Framework, which would, if agreed upon, provide a framework for the transfer of data between the EU and the U.S. in compliance with the EU's General Data Protection Regulation. The framework was implemented by an October 2020 executive order and is being considered by the EU.

How to comply with data privacy laws in the metaverse

Some of the most basic elements of modern U.S. privacy law—such as providing notice and obtaining consent for the collection and use of personal information—become surprisingly complex in the metaverse.

It's not too complicated to make a privacy policy reasonably accessible on a website. In most situations, all the company has to do is have a hyperlink on its homepage that links to the policy. However, there are no "homepages" in the metaverse. It's not even obvious when a metaverse avatar moves from one retailer's online space to another's. But in jurisdictions that require conspicuous notification of privacy policies, this complexity must be sorted out.

Consent is even more challenging. When and how is consent obtained? What would be equivalent to a pop-up bubble prior to entering a website? Perhaps a floating orb? Or a new avatar that seeks the consent? If express written consent is required to collect any data, then companies must get creative to ensure they don't inadvertently collect data prior to obtaining consent. In a space where every step potentially implicates the collection of personal information, there are significant risks to not proactively preparing to comply with the laws.

How to maintain data governance and cybersecurity

The metaverse could substantially change how we interact in digital spaces, and the amount of collectible information may increase in size just as much. Body movements, the smallest glances, changes in vocal tone, heart rate, proximity to other avatars—all of this information is theoretically collectible in the metaverse. This creates real opportunities and real risk for both consumers and retailers that are promising to protect that same information through privacy policies.

Retailers will need to place an even greater emphasis on data governance and cybersecurity to deal with the increasing amount of information and interaction. An increase in personal and sensitive information coupled with an increase in possible access points may incentivize bad actors to target retailers in the virtual space. Therefore, retailers will need to be vigilant and consistent in their data management and security practices to stave off these threats.

While the future of the metaverse is still unknown, retailers should be aware of the privacy concerns it may bring. The global nature of the metaverse will challenge retailers to comply with a multitude of privacy regimes, while the novel structure of the metaverse will require them to collect and secure data in new ways. Retailers that are able to adapt to these privacy challenges may discover new opportunities in the metaverse.

This article first appeared online at *Total Retail* on Oct. 20, 2022. It can be accessed at https://www.mytotalretail.com/article/privacy-and-cybersecurity-for-retailers-in-the-metaverse/.

Kristin Madigan
Partner, San Francisco
Privacy and Cybersecurity

Jacob Canter
Associate, San Francisco
Privacy and Cybersecurity

Alexis Ward
Associate, Los Angeles
Privacy and Cybersecurity

Cases Show Real-World Laws Likely Apply in Metaverse

In the brave new world of the metaverse, unprecedented legal issues may arise and, in some cases, have already arisen

Jason Stiehl, Jacob Canter, Preetha Chakrabarti, Deborah Yellin

Endless articles, commentary, and blog entries have been rattling the cage about the brave new world of the metaverse and the unprecedented legal issues that may arise and, in some cases, that have already arisen.

But how brave and new are these legal issues? Open minds and creativity will, of course, be essential in tackling them, but like most things in the law, the metaverse is simply a newly packaged set of facts that largely fits within our established precedent. It is a new arena for people to transact, collaborate, and create.

The term "metaverse" originated 30 years ago in "Snow Crash," a novel by Neal Stephenson. The novel sets out important imagery to help understand why the metaverse isn't really that different from existing legal issues:

When Hiro goes into the metaverse and looks down the Street and sees buildings and electric signs stretching off into the darkness, disappearing over the curve of the globe, he is actually staring at the graphic representations— the user interfaces—of a myriad different pieces of software that have been engineered by major corporations. In order to place these things on the Street, they have had to get approval from the Global Multimedia Protocol Group, have had to buy frontage on the Street, get zoning approval, obtain permits, bribe inspectors, the whole bit.

Following Stephenson's imagery, you can picture the metaverse as Main Street. You can open a store, advertise goods, share and exchange ideas, and engage in any form of real-world commerce you can imagine—only virtually.

Here you do not necessarily move linearly like you would in the real world. You can transport yourself instantly down a side street, visit a friend in a different location, attend a virtual conference, or simply unplug and disappear.

These multifaceted webs of interactions and engagement will force lawyers to apply current laws in an arguably more holistic, 3D way.

For one, the metaverse is global; choice of law (jurisdictional law, contract law, etc.), content standards, and other laws and regulations will have to accommodate this conundrum. Also consider a concert in the metaverse: Law in play will not just consider the artist performing, the rights to the music, and the venue. One must also consider the virtual engine underpinning the production, licenses, and contracts to any input from virtual contributors, and even digital dance choreography.

Precedent is everywhere

But fear not: This is neither the first attempt at a virtual world nor the first effort to create a litany of litigation over the very issues that are percolating in the metaverse. Video games like Second Life, a 3D virtual world full of content created by its users, and Fortnite, an online video game where players cannot only fight, but meet up, watch a concert, and build an island, are early versions of metaverses.

Second Life is famous for its free-market economy. Players of Second Life, called "residents," can buy and sell goods with Second Life currency, which can be exchanged for real currency. Since the appearance of Second Life, created by Linden Research Inc. in the 2000s, it has become widely accepted that laws applicable in real life are also applicable to online life, including, as discussed below, in the areas of intellectual property and real property.

> … Like most things in the law, the metaverse is simply a newly packaged set of facts that largely fits within our established precedent.

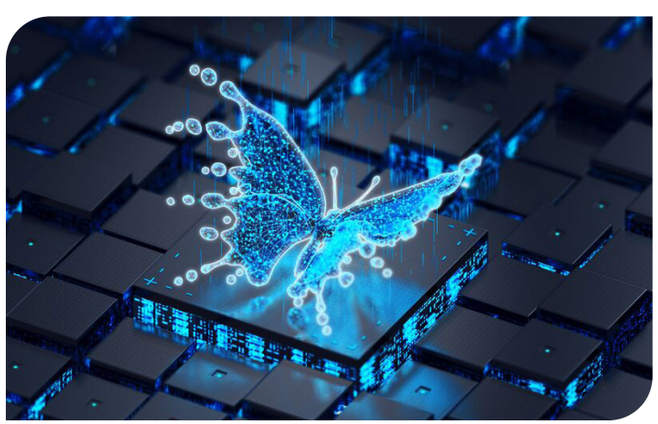
Battles over virtual and real property

Perhaps one of the most active areas, not surprisingly, was in the space of IP. The Second Life metaverse generated a handful of cases involving copyright, trademark, and counterfeiting issues. Like in most metaverses, the users own the copyright to the content they create. The result was real-life battles over artificial concepts.

For example, in 2010, two breeders of metaverse animals—Amaretto Ranch, which bred virtual horses, and Ozimals, which bred virtual bunnies—became ensnared in three years of litigation over whether the online animals violated the Digital Millennium Copyright Act, spawning additional claims of defamation, libel, and unfair competition. The lawsuit also successfully enjoined Linden Labs from taking down any of the content.[1]

Similar cases raised the issue of what obligations the metaverse owner had to police its virtual world.

For example, in *Taser International v. Linden Research Inc.*, Taser became aware of several uses with Second Life of its trademarked word "taser," including advertisements for similar nonlethal virtual weapons.[2] Taser filed litigation against Linden, and within days, it appears that Linden successfully identified the infringing user(s). By the week's end, no instances of "taser" could be found.



The possibility of a trademark action causing a word to disappear from an entire metaverse community is thus well grounded in existing precedent. The consequences of such an action, however, are much less clear.

A more creative dispute spawned from an artist's use of the phrase "SL"—for Second Life—in his online art. Minsky, a real-world artist, opened a virtual art gallery and then published a real-world book describing the "SLART" that had been created online. Having secured trademark protection for "SLART," he discovered that another artist was using the phrase "SLART Garden" and had developed a community called "SLartists of Second Life."

Minsky first looked to Linden to enforce his IP rights before engaging in litigation. Instead, Linden refused, Minsky filed suit, and Linden countersued and attempted to remove Minsky for infringing their mark, SL. Ultimately, the parties settled out of court, and Minsky continued to utilize his SLART mark in Second Life.[3]

Finally, *Eros LLC v. Linden Research, Inc.* is an example of counterfeiting in the metaverse.[4]

Eros marketed various erotic items and skins within Second Life and claimed that its digital products had been counterfeited by Second Life residents. Linden responded that it was nothing more than a marketplace and was effectively a manager of digital rights.

Eros countered that Linden provided the platform and access for the opportunity to pirate the materials and, as the operator of the most widely used currency exchange, profited from the counterfeited goods. Eros brought a class action on behalf of similarly situated victims of infringement on Second Life. Ultimately, the matter was settled out of court on an individual basis.

Each of these cases provides insight into future applications of existing laws to the metaverse, as well the obligations, if any, of the metaverse owners to monitor and police the content and infringing scenarios online. The cases also speak to the likelihood that the DMCA will not provide the same shield to metaverse operators that has been recently enjoyed by more social media platforms.

The scenarios further reflect that in a digital world IP disputes necessarily become disputes that have real-property characteristics.

Much like IP in the metaverse, disputes have come up regarding the purchase of "real" property.

In one such dispute, users filed a class action against Linden on behalf of users who had their virtual property "seized" by Linden for various reasons and not returned. The users analogized the purchase of virtual property as akin to that of real property and argued that Linden's reclaiming of the property resulted in a fraudulent misrepresentation and conversion of their property.

Ultimately, the court certified the class of individuals and the matter settled for 43 million Linden dollars—worth about $172,000 at the time.[5]

In a similar matter, the plaintiff, Bragg, claimed that he was induced into investing in virtual land by representations made by Linden and Rosedale in press releases, interviews, and through the Second Life website. He also paid Linden real money as a tax on his land.

Bragg both purchased land and crafted digital fireworks to sell to other avatars for profit. Linden had seized Bragg's land, claiming he had purchased it through "exploit" and ultimately froze Bragg's Second Life account. The matter ultimately was arbitrated based on the terms of use.[6]

Both of these cases reflect that courts have looked at property rights similarly as those rights that exist in the real world and have applied common law torts, such as conversion, to allow for the recovery of the value lost for the property purchased.

[1] See Amaretto Ranch Breedables, LLC v. Ozimals, Inc., Case No. 10-cv-05696 (N.D. Cal).

[2] Taser International v. Linden Research Inc. (D. Az. 2009).

[3] See Minsky v. Linden Research Inc., Case No. 08-cv-819 (N.D.N.Y.).

[4] Eros LLC v. Linden Research, Inc. (N.D. Cal. 2009).

[5] See Evans v. Linden Research, Inc., Case No. 11-cv-01078 (N.D. Cal.).

[6] See Bragg v. Linden Research, Inc., Case No. 06-cv-04925 (E.D. Pa. 2007).

Some areas remain untested

Surprisingly, there does not appear to be any precedent in the virtual world for these claims, despite much offline documenting of issues. Current metaverse operators appear to be incredibly proactive and have taken efforts to protect users in virtual worlds from things such as digital sexual harassment: nonconsensual touching, verbal harassment, and simulations of sexual assault.

And as more aspects of life enter the metaverse and the technology becomes more immersive, it is possible that notions of bodily integrity—and what it means to violate bodily integrity—will similarly develop.

The metaverse platforms are trying to develop technological solutions to combat bodily assaults. For example, in February, Meta added a feature called "personal boundary" that can be used to stop other avatars from getting too close—but that is unlikely to disrupt all attacks.

Likewise, though it never reached the attention of the courts, there was plenty of interest in the tax implications of Second Life's many virtual transactions. Some academics proposed treating revenue earned in Second Life as taxable income because it could be exchanged for fiat.

The IRS similarly remarked in 2007 that redeeming Linden currency for money, goods, or services would have tax consequences. Congress, in 2006, considered preparing a study of virtual world tax issues through its Joint Economic Committee, but the study never materialized. And starting in 2013, Second Life began issuing Form 1099-Ks to users who received proceeds over $20,000 from the exchange of Lindens.

Past is precedent, even in a new world. But the present is already being written.

For example, in *Hermès Int'l v. Rothschild*, the plaintiff alleged that its Birkin brand was being infringed by the online MetaBirkin NFTs.[7] The case went to trial, and on Feb. 8, 2023, a Manhattan federal jury found that Los Angeles designer Mason Rothschild's "MetaBirkin" NFTs infringe and dilute the Hermès trademarks for its globally renowned Birkin bags and that Rothschild cybersquatted on the MetaBirkins.com domain name. Rothschild must now pay $110,000 of net profits for trademark infringement and dilution and $23,000 in statutory damages for cybersquatting.

And in *Doe v. Roblox*, the court allowed the plaintiff's allegations of fraudulent commercial practices to survive dismissal despite the defendant arguing that the claims were barred by Section 230 of the Communications Decency Act.[8]

Companies should look carefully at these past cases, as they provide, even in untested areas, strong guidance as to what the likely outcomes will be for operation in the metaverse.

An expectation exists that activities in the metaverse will be policed—and enforced—much like they would be in the physical world, and compliance with the formalities of normal commercial interactions, even when "playing" in the metaverse, will apply.

A strong understanding of the past will make sure you are protected today.

This article was originally published by Portfolio Media (*Law360*). The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Past is precedent, even in a new world. But the present is already being written.

[7] Hermes Int'l v. Rothschild (S.D.N.Y. 2022).

[8] Doe v. Roblox, (N.D. Cal 2022).

Jason Stiehl
Partner, Chicago
Advertising and Brand Protection

Jacob Canter
Associate, San Francisco
Privacy and Cybersecurity

Preetha Chakrabarti
Partner, New York
Advertising and Brand Protection

Deborah Yellin
Partner, Washington, D.C.
Intellectual Property

A Walk Through the Metaverse for Corporate Counsel

Let's walk through the metaverse, step by virtual step, and explore some of the legal questions that arise along the way

Andrew Avsec, Dalton Hughes

If your company isn't on the metaverse yet, don't wait for it. Because your customers are already there.

From department stores to restaurant chains, brands are engaging with customers on the metaverse to drive them to their "real life" stores, and in the process, creating new revenue streams. And with these new worlds (or universes) come new legal questions, especially for a brand's intellectual property.

In this article, we're going to walk with you through the metaverse, step by virtual step, and explore some of the legal questions that arise along the way.

First step: We pick a metaverse. There are many metaverses, even if the term is used interchangeably.

There are blockchain-based metaverses like Decentraland and The Sandbox, non-VR experiences like Roblox and Second Life, and social virtual reality universes like Horizon Worlds, Altspace, and VRChat. The metaverse can be accessed by technology in or out of VR (meaning the 3D headset), but VR adds an extra layer of immersion by allowing you to interact directly with the virtual world and others in real time.

Our walk focuses on a VR metaverse—Horizon Worlds, Facebook's (now Meta) VR social metaverse.

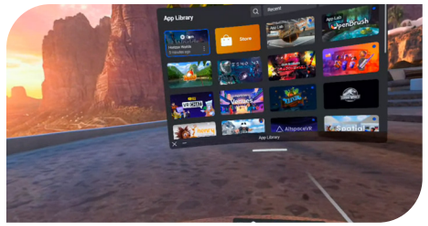
Next, we set up the gear. We are accessing Horizon Worlds with a Meta Quest 2 VR headset (formerly known as Facebook's Oculus Quest 2).

In the box, we find two handgrip controllers, a VR headset, and Meta's safety instructions. The instructions warn us of concerns like bumping into walls and flashing images.

We find a space sufficiently free of obstructions and then set invisible boundaries in our physical rooms, so that when we step outside of it, the virtual world ends. The view on our headsets change from virtual to real, and we can see whatever couch or table we might bump into.

For most of us, the first immersive experience can be disorienting. We are greeted with a beautiful home environment and an app library menu that allows us to access experiences.

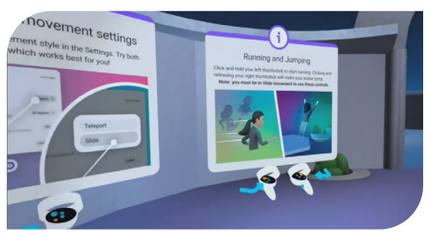
After selecting Horizon Worlds in the application library of the Quest 2, the Horizon loading screen pops up.



Now it's time to create a character.

Virtual hands appear! Check out Dalton's avatar, which will represent him in Horizon Worlds and will be what other users see.

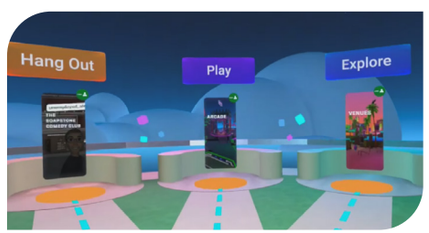
We learn how to move in the metaverse and interact with digital objects. It varies by headset, but with the Quest 2, we learn how to jump, run, teleport, and even throw a paper plane with the controllers!



Horizon Worlds, Meta's Metaverse, has three main categories of experiences:

- Hang Out is for static worlds to interact with other users.
- Play is for playing video games by yourself or others in VR.
- Explore is for interactive experiences, like a concert or visiting a mountaintop, alone or with friends or strangers.

There are thousands of these experiences, and the objects and environments within are built by Meta, companies, or individuals. Platforms do their best to moderate, but proceed with caution. Just like in the real world, these are interactions with real people, and you could potentially hear or see anything.



We decide to hop into Hang Out first. There are advertisements for live and recorded events, and content creators can work with brands to sponsor live events or even perform in spaces created by brands to host these events. We select a comedy club world!

The world settings can be set by the moderator of the virtual experience in an attempt to curtail inappropriate content and protect their creations. This notice lets users know that we will be interacting with real individuals and that purchases can be made here.

Tip for in-house counsel: Consider what you would include in a disclaimer in the virtual world. These disclaimers are a mix of use of a product along with use of a public space. Consider safety implications for how your world could impact users. Sights, sounds, and other health impacts could arise. For example, if a content creator uses strobe-effect lighting that could trigger seizures, whose responsibility is it to warn the user as they enter your world?

Walking toward the comedy club, we see advertisements for virtual jobs (that pay real money) to host or produce comedy productions at the club. Here, you can be paid as a host or producer of live comedy shows in the metaverse. The goal, of course, is to curate a quality experience for scheduled shows at the club.

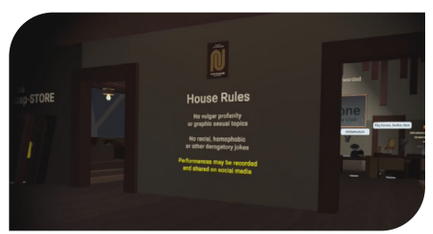
Tip for in-house counsel: Even aside from staffing a metaverse world, retailers may one day hire in the metaverse as well. HR departments could use the metaverse to advertise open positions and conduct interviews for jobs in real life. Expect to see novel employment law issues (like to what extent you can control how your employees' avatars appear).

Currently, the club is hosting an open mic, and we appreciate why employees are necessary. While someone is at the mic talking, the audience members are mingling and speaking to each other, often with little respect for the comedian. If this were a scheduled showtime, it would be necessary to have a virtual enforcer so that the audience could enjoy the show.

In this show, two people perform a joint stand-up set. All the names in white (appearing above the avatars) are real people experiencing this VR world with us at the same time. As you can see on the wall in this image, the audience clapped 150 times, so it was definitely a good show!

Tip for in-house counsel: Brands should plan—depending on the engagement they expect in their virtual world—to have real employees answer questions and keep the virtual world safe and hospitable for their customers. Consider the legal issues associated with unchecked, unruly patrons. Should brands designate employees to monitor such behavior, just as they do in brick-and-mortar stores?

The club does post rules to help moderate the live online experience. They prohibit the use of vulgar language and include an IP notice that you are free to record this space. Remember that, just like in real life, others can hear you and see your movements.



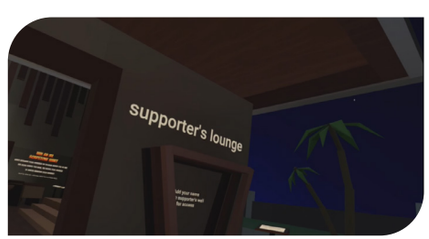
Tip for in-house counsel: The first thing we appreciate is how much content is already in the metaverse. As much as the metaverse provides opportunities for new avenues of creativity and opportunity, it also provides a new forum for infringement. Horizon Worlds is owned by Meta, which has spent many years developing an IP infringement reporting tool. Accordingly, Horizon Worlds already has a takedown mechanism. Most virtual worlds have some reporting mechanism, but there are mixed reports on how effective they are.

The development and availability of significant content has important IP implications:

- Your company may be developing significant IP in launching its presence in the metaverse.
  - Assess what IP you are generating and how best to protect it, including through copyright and trademark registrations.
  - In the metaverse, assets can be altered and modified easily by consumers and placed in locations that you may not be considering in real life. (For example, wearing a logo like a tattoo on your virtual avatar!)
  - Develop clear house rules and post them prominently. Use monitors to help enforce those rules.
- Your company may be interacting with third parties (new vendors, new partners, new influencers, etc.).
  - Consider strategic decisions when drafting contracts to license your brand out on what terms apply to VR versus real-life use of something like your logo.
- The opportunities for third parties to infringe your IP also abound.
  - It is difficult to restrict audio-visual recording of anything in the metaverse like you may be able to at a live performance physically, as the medium naturally streams to a headset or screen and could be recorded in live time on a computer.
  - Consider setting up a monitoring team or using a vendor that monitors the metaverse for IP infringements.
- Avoid IP infringement. It is important that your employees and vendors developing content and working in the metaverse receive training on copyright and trademark laws. These employees may not have been in areas of the business to receive such training in the past.

Back outside of the club, there are premium experiences that we can use real currency to purchase. As is common in the metaverse, there is an opportunity to purchase both virtual products and real products.

By paying a fee, we can access a supporter's lounge to gain access to premium shows by comedians not accessible by someone just stopping by for an open mic, like we just did.



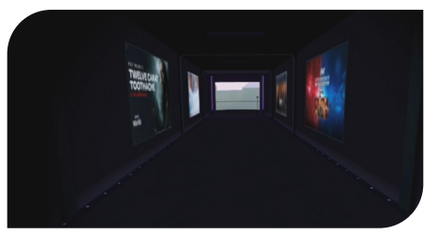
The other side of the entrance is the clothing store for the club.

Here, there are two different assets available for purchase—virtual goods to dress up an avatar and physical shirts that would be shipped to a customer's house after purchase.

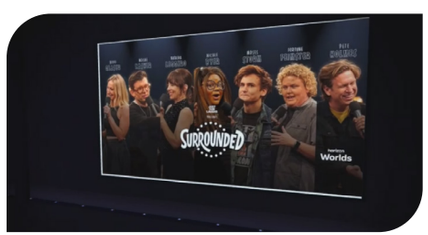
Tip for in-house counsel: While the world is virtual, it typically functions much like the real world and interacts with the real world. Early NFT and metaverse cases have focused on "fair use" principles to justify the use of others' brands.

Make no mistake: Virtual clothing and physical clothing can be bought in the same venues in the metaverse. While virtual clothing may not provide warmth, it is purchased for the same reasons (aesthetics, cachet, style, and brand reputation) that consumers consider when purchasing real clothing. From a trademark law perspective, the "likelihood of confusion" analysis in the metaverse will and should often track the real world. Brands should advise their employees that the metaverse does not change the IP rules.

Next, we check out an Explore world. We selected a Horizon Venue recorded experience of Billie Eilish playing at the Governors Ball Music Festival. After we load up the experience, we enter a hallway similar to that leading to a movie theater, with some advertisements on the wall.



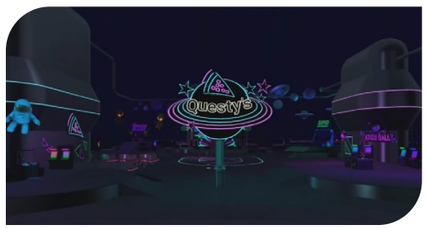
We encounter two ads while walking up to the concert stage: one for a VR comedy show similar to the environment we are going to attend now and the other for a non-VR movie.



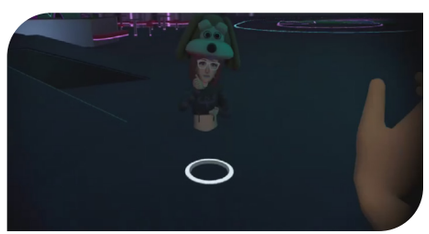
Wow! When we leave the tunnel, we land in the front row of the concert (which is recorded and playing on a loop). Visitors here are able to move around the stage to get different views. There are other experiences like this that can be experienced or purchased; for example, a live NBA basketball game from the front row. These are 3D experiences where you can walk around the audience and stage.

Tip for in-house counsel: Do existing contracts and agreements with advertising agencies and influencers address activities in the metaverse? Consider these issues as your company expands activities into the metaverse.

Next stop, a Play experience. The Play door at the Horizon Worlds' intro area took us to Questy's, a retro arcade experience.



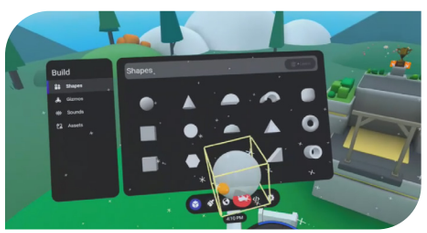
Walking around Questy's, we talk to another user in the metaverse, who wears a hilariously big dog hat. She was another Quest 2 user, from England, and we spoke over voice chat about how it was our first time here. She recommended playing the whack-a-mole game and we went our separate ways.



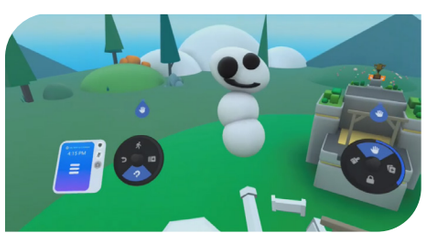
Tip for in-house counsel: The metaverse is inherently international. In the metaverse, you can encounter people from all over the world, though some experiences list suggested languages for conversing. Even if a virtual world is created in one country, consider how easily accessible it is for foreign users to access a world, like other online websites.

Laws and consumer expectations, including the protection of personal information, vary from jurisdiction to jurisdiction. Which country's laws govern? Where are disputes adjudicated? Review your metaverse provider's policy, and to the extent you have control over these issues, include this information clearly in your house rules.

Now that we have visited the main categories of Horizon Worlds' user experiences, we open up Horizon Worlds' Create mode to try creating a digital asset. Depending on the certain metaverse's policies, these objects may be freely shared, used, or sent in the metaverse you're in or even sold as a virtual item to others in some worlds. Payment is similar to real-life purchases and can be made with fiat currency, crypto, or, in some cases, with fictional in-game currencies.



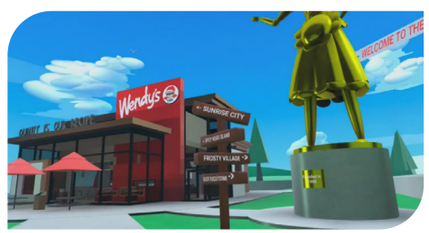
We tried to build a snowman—in an apparent summer landscape. I'm not sure if you can call him a snowman, but the little art project turned out all right to us!



Tip for in-house counsel: Companies must consider what they own and do not own in developing assets and materials in the metaverse. Not all platforms have the same rules. In some, virtual land must be rented or purchased.

How do brands in real life utilize their design, trade dress, logos, and other IP in the metaverse? Recently, Wendy's Restaurants opened up a VR experience, so we loaded it up.

This metaverse world contains a fully built, 1:1 scale Wendy's we can enter. The restaurant and branding look very familiar and similar to a real Wendy's, although you will note that Wendy is wearing a VR headset!



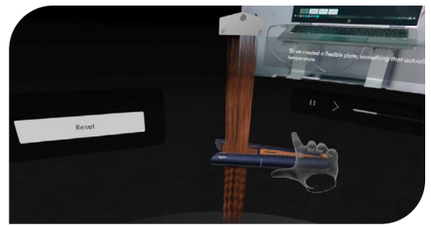
Entering the Wendy's provides the impression of a real building's dimensions and approximates the design of real Wendy's in real life.

The self-order terminals sprung to life when we approach them. But instead of ordering virtual food, visitors are able to download a coupon for free real food as a thank-you for visiting their virtual world.

Tip for in-house counsel: Consider what disclosures and disclaimers are provided with promotional items provided in the real world and whether any modifications need to be made. Do technical restrictions need to be added, such as how many coupons can be downloaded by a single user?

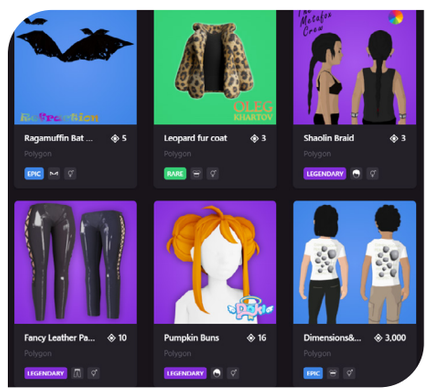
Though some brands like Wendy's create a virtual environment to give users a unique virtual experience, other brands will use the metaverse to showcase products and mimic real-life functionality for user testing. Dyson has developed a beautiful Meta Quest application to allow consumers to learn about and test-drive their new hair care technology. Though their application is stand alone and not in a metaverse, it reveals a way that brands can implement their real products in a virtual environment for metaverse use.

Selecting the straightener starts a video about the new technology and allows us to test it ourselves in their showroom on virtual hair, which responds just like real hair!



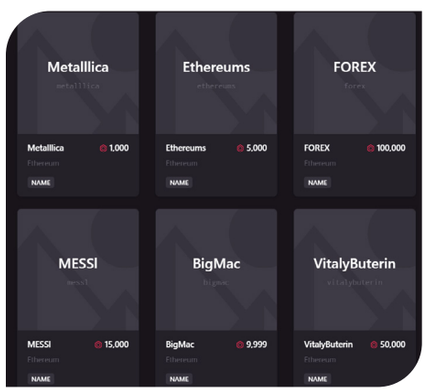
Tip for in-house counsel: Consider whether virtual displays provide a realistic representation of your product's experience. If products do not perform in the real world as effectively as they do in the virtual world, you can expect consumers and competitors to consider what legal remedies they may have. Disclosures that products may perform differently in real life may not be sufficient in all circumstances.

As we conclude our tour, we explore marketplaces to outfit our avatar in other universes. These examples are user-created (i.e., nonbrand digital assets to purchase for avatars) from other metaverse platforms that we find online, without our VR goggles.



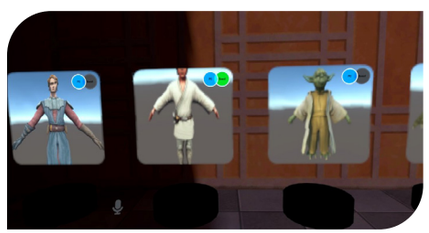
In addition to purchasing articles of clothing and accessories, we can purchase avatar names. Decentraland names are one example, used for our virtual avatar and as a unique identifier in Ethereum to make it easier to send payments. This has led to a practice that is analogous to cybersquatting on domain names during the early dot-com boom.

As we can see below in this screenshot taken from Decentraland's marketplace, names have been claimed that are identical or similar to well-known brands, companies, and individuals listed for purchase to claim in this metaverse. In the example below, BigMac is listed for 9,999 MANA, which is currently trading for approximately $6,300.



VRChat is another independent metaverse, not based on crypto, that has endless possibilities for user world and avatar creation. VRChat is an older, more mod-able and complex metaverse that can be accessed in VR or on a computer and is known for its creative and talented user base that designs and models worlds and avatars for anyone to use.

Because of this, VRChat is one of the most active metaverses, along with publicly traded Roblox, which has similar user-creation abilities. This scope of creation, however, inevitably implicates gray-area use of IP without permission.



For example, here is a user-created world where we can select an avatar to use anywhere in VRChat, showing some well-known movie characters. Once in an avatar, the avatar can virtually say and do anything with it in this metaverse, no doubt running afoul of many brands' preferred uses for their IP.

Tip for in-house counsel: Policing your trademarks and other IP in the metaverse will require resources to identify infringements and remove unauthorized uses of your brands. This might include the following:

- Assign a person or team to periodically shop or search for counterfeit or infringing items in the metaverse and on NFT marketplaces.
- Watch the trademark register. Bad faith actors often file trademark applications believing incorrectly that the use of another's brand in the metaverse gives them trademark rights.
- Monitor customer complaints. Customer reports often identify brand misuse in the metaverse. Train your customer relations teams to look for abuse of your trademarks in the metaverse.
- Consider using a brand protection vendor that searches certain NFT marketplaces for potential trademark infringements.

The metaverse offers retailers opportunities for creation and co-creation. Brands will do well to remember the unexpected challenges that came with the rise of social media, which allowed them to communicate with prospective customers and fans more directly than they had ever before. Consumers complained publicly—and complained louder if their complaints were removed. Brands could go viral with the good and the bad.

The metaverse is the next evolution of two-way communication with consumers in that it allows for that communication to take place in an immersive environment. Users will become co-creators of the worlds they visit. We're just starting to learn what that could mean for brands, but we know they will need best practices in place to keep pace with the changes.

Andrew Avsec
Partner, Chicago
Advertising and Brand Protection

Dalton Hughes
Associate, Chicago
Intellectual Property

AI, IP, and the Metaverse

Adapting traditional IP principles to AI and the metaverse

William Frankel, Dalton Hughes

Artificial intelligence and the metaverse are two of the most rapidly evolving technologies today, testing the boundaries of intellectual property law. While the swift expansion of AI in all industry sectors can be thrilling, it also presents challenges in terms of protecting and encouraging artistic and scientific endeavors. A principal challenge for authors, creators, and corporations is how to protect creative endeavors from the threat of consumption and reproduction by AI engines, while at the same time realizing the promise of AI-conceived and -developed creative and technological advances. This fundamental IP conundrum also arises in the evolving metaverse.

AI for human interaction is technology that enables computers to perform mental tasks that would typically require human intelligence, such as understanding natural language phrases, recognizing images, and suggesting next steps for a decision. At its core, AI is a computer algorithm that has been programmed to mimic the natural intelligence of human beings, such as learning, reasoning, and making decisions.

Today, AI has evolved beyond machine learning (using examples of input and expected output to train a system to make decisions without being programmed how to do so, e.g., email spam filtering, machine translation, text and image recognition) to deep learning based on deep neural networks that can analyze new data sets—best described as "deep supervised machine learning."

The metaverse is a natural canvas for AI, a digital world where users can interact and work in a virtual environment. The metaverse is commonly understood to mean an interactive virtual space where users can interact with each other and the virtual world around them in real time, either in a 2D, 3D, or virtual reality space. Examples of metaverses include Meta's Quest VR application Horizon Worlds, cryptocurrency and NFT-built Decentraland, and the 3D virtual game Second Life.

AI and the metaverse

The combination of AI and the metaverse provides the opportunity for many new, exciting experiences, things that once were the domain of science fiction. AI can be used to generate realistic virtual landscapes, buildings, and characters that can adapt to the actions of users in the metaverse. One can envision a 3D transformation of such technology resulting in a simulated environment like the holodeck featured in the "Star Trek" series. We continue to see new applications for these innovations. Examples include DALL-E and Midjourney, which create art from simple or complex text descriptions; Stability AI, an approachable coding program for deploying machine learning models; and Deviant Art's DreamUP, a platform for artists to create AI images based on their and others' artistic styles.

The expansion of conversational chatbots also suggests applications that likely are heading to the metaverse. Currently, ChatGPT, OpenAI's chatbot for consumer and professional use, is rapidly expanding in popularity and in its uses. (ChatGPT: Optimizing Language Models for Dialogue). OpenAI boasts that ChatGPT is meant to interact with humans in a conversational way, with memory-based functionality to provide the opportunity to conduct full conversations with the AI, attempting to provide the user correct factual information.

A principal challenge for authors, creators, and corporations is how to protect creative endeavors from the threat of consumption and reproduction by AI engines...

The AI is able to generate code for programmers, write complex articles, answer questions about the world, respond to search requests posed as plain-English questions, and draft arguments for legal motions. One can readily envision the use of conversational chatbots like ChatGPT in the metaverse, which features highly interactive and vibrant environments.

Another AI application, Character.AI, is experimenting with simulated character conversations for personal entertainment use, making up scenarios and facts for role-playing interactions with new or well-known characters. Released in September 2022, the application allows users to interact with familiar characters in a free-form chat. The characters include fictional entities like Wonder Woman, historical figures like Albert Einstein, and famous living individuals like President Joe Biden or entertainer Billie Eilish.

Use of these figures could potentially implicate IP rights of the person, including the right of publicity, which protects against unauthorized commercial use of an individual's name or likeness. Not only will we be able to create our own virtual worlds in the metaverse, but once there we will be able to converse and interact with any number of virtual characters or real persons through their online avatars.

AI also will enable more efficient and effective ways of "living" and working in the metaverse. AI can be used to automate repetitive tasks, such as scheduling meetings or organizing documents, or for consumers to contact self-help chatbots for product support with a layer of interaction beyond just a chat box.

For example, the application One Law is an AI program for law firms to onboard new clients and acts as a legal assistant for administrative tasks. The platform uses a generated human character, named Amelia, that can respond with actual speech and movements, which replicates interactions in the metaverse. Another project that utilizes similar technology is BOT Libre, an open-source AI platform for the metaverse that enables businesses to provide information on products or VR users to conduct virtual conferences or classroom lessons.

Legal considerations

Like most cutting-edge technologies when they first hit the scene, AI is presenting new legal challenges for businesses across all industries, not to mention for IP and other lawyers addressing this area. To what extent is AI protectable by the conventional tools in the IP toolbox, such as patents, copyrights, and trademarks? Who owns IP in AI creations?

Government agencies already have been tasked with reviewing applications for copyright registration and patents when AI is a co-author or the sole author of a copyrightable work, or the co-inventor or sole inventor of a patentable invention. Tech companies have been active in patenting new technologies to incorporate into the metaverse while utilizing AI. For example, Apple obtained a patent for "Specifying Effects for Entering or Exiting a Computer-Generated Reality Environment" (U.S. Patent No. 11,222,454 (issued Jan. 11, 2022)). This patent incorporates AI into a VR or augmented reality metaverse experience for users. They can then naturally transition between VR and AR metaverse experiences while wearing a headset for a more seamless, interactive experience.

What happens when the inventor is an AI engine itself? Computer scientist Stephen Thaler applied for two patents invented by a system called DABUS, or "Device for the Autonomous Bootstrapping of Unified Sentience." The inventions that DABUS created were a fractal drink container that can change shape for better gripping of the container and a flickering light that better catches someone's attention in emergency circumstances. Both were rejected by the U.S. Patent and Trademark Office.

Though patent applications for AI technology are possible, U.S. courts have ruled that inventions created by AI alone cannot be patented because the inventor must be a natural person. The U.S. Court of Appeals for the Federal Circuit ruled that the DABUS technology is not an "individual" under the Patent Act and AI inventorship is at odds with the plain language and intention of the Constitution. (*Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022)).

Though patent applications for AI technology are possible, U.S. Courts have ruled that inventions created by AI alone cannot be patented...

Copyright protection presents its own challenges for AI-inspired creative endeavors. The U.S. Copyright Office has refused to register a claim for copyright if it determines that the work was not created by a human being. Here, too, Thaler has sought to register copyright in works created by his DABUS technology.

In 2014, DABUS reviewed thousands of photographs and generated an original work of art that it named "A Recent Entrance to Paradise." Thaler sought to register the work with the Copyright Office in 2018. He could have asserted that he was the human author and that DABUS was an assisting instrumentality, but he instead intentionally represented that "A Recent Entrance to Paradise" was autonomously created by AI without human intervention.

Despite multiple requests for reconsideration, the Copyright Office refused registration on the basis that the work "lacks the human authorship necessary to support a copyright claim." On Feb. 14, 2022, the Copyright Review Board rejected Thaler's argument that the human authorship requirement was unconstitutional and unsupported by case law. The Copyright Office has since clarified that applicants must identify and disclaim an AI-led element in their applications. On Jan. 10, 2023, Thaler filed sued against the Copyright Office to challenge its refusal to register AI-created works.

Relatedly, copyright claims may impact NFT use in the metaverse. One court recently held that the Bored Ape Yacht Club NFT terms and conditions grant purchasers a license to use the NFT commercially but do not transfer ownership in the subject NFT art, and that use of the NFT art by others may constitute copyright infringement. (*Yuga Labs, Inc. v. Ripps*, No. CV 22-4355-JFW (JEMx), 2022 LEXIS 234124 (C.D. Cal. Jan. 18, 2023)).

... It will become increasingly important to protect the personal information and data of users, and public figures will have to protect their image from being exploited.

It also is possible for trademark rights to be implicated and infringed with AI in the metaverse. A federal jury found a Los Angeles designer liable for trademark infringement for the creation of "MetaBirkins" bags for use in virtual worlds. (*Hermès et al. v. Rothschild*, No. 1:22-cv-00384, Dkt. 144 (S.D.N.Y. Feb. 8, 2023)). These virtual accessories were sold as NFTs. Hermes International successfully argued the virtual bags infringed their trademark rights in their physical Birkin bag designs and the Birkin brand name, and that use of the NFTs amounted to cybersquatting on the Hermes name and trademarks in the metaverse.

This result is a strong win for fashion brands that plan to produce and sell similar items to their tangible goods as virtual avatar accessories or NFTs. Even though the MetaBirkins utilized original designs, the close association and stylistic comparison with the Hermès-branded products were found to constitute infringement—a result that could apply to both human- and AI-created works depending on relatability and the degree of connection with the physical brand.

Another challenge is the issue of privacy rights in the metaverse. As the metaverse becomes more prevalent, it will become increasingly important to protect the personal information and data of users, and public figures will have to protect their image from being exploited. New York has attempted to get a head start on protecting these rights, as well as protecting citizens from confusing representations of public figures. (S. No. 5959-D, 2019-2020 Sess. (N.Y. May 16, 2019)).

The statute bans virtual avatars during election periods (mostly due to the concern of deepfakes—highly realistic, AI-generated videos that appear to be the actual figure speaking), requires mandatory disclaimers for certain avatars, and creates additional causes of action for nonconsensual pornography. Additionally, such laws are anticipated in an effort to curtail the misuse of AI in virtual spaces. In a recent class action filed against companies utilizing AI art generators, the plaintiffs make the novel argument that an artist's right of publicity is violated when an AI art generator can respond to prompts requesting output images "in the style of" that artist. (*Andersen et al. v. Stability AI LTD et al.*, No. 3:23-cv-00201, Dkt. 1 (N.D. Cal. Jan. 13, 2023)).

Looking ahead, the use of AI in the metaverse is all but sure to revolutionize the way we interact with customers, work, and each other. And the law of IP will grapple with the thorny questions that arise with such new and disruptive technologies. We recommend that companies and brands do their best to stay on top of developments in these rapidly evolving technology spaces as they enter the metaverse. They also should be mindful of the fundamental issues and challenges related to IP ownership, enforcement, and privacy in the worlds of AI and the metaverse.

William Frankel
Partner, Chicago
Intellectual Property

Dalton Hughes
Associate, Chicago
Intellectual Property

ESG in the Metaverse: An Opportunity to Rethink Sustainability

Can the metaverse serve as an opportunity to wipe the slate clean and start over?

Preetha Chakrabarti, Helen Ogunyanwo, Felicia Isaac, Tiffany Aguiar

At times, the real world can feel too set in its ways to change. Can the metaverse serve as an opportunity to wipe the slate clean and start over? If so, what would you consider? How would you create it with environmental, social, and governance principles in mind?

This article explores how the metaverse might allow companies and people a chance to answer these types of questions today.

Environmental sustainability in the metaverse

The metaverse's ease of access and use (i.e., plugging in a gaming system or turning on a laptop) can make its environmental impact seem minimal to consumers. To the experts behind the scenes, however, the metaverse's environmental impact is enormous.

To truly understand the scope of the metaverse's environmental footprint, we must untangle the coils of fiber-optic cables, look up to cellular towers, and feel the heat emanating from computer servers and data centers. We must look to the electricity, water, air, heat, metals, minerals, and rare earth elements that support and bear the burden of the metaverse. Assessing these individual elements helps uncover the metaverse's potentially enormous environmental impact.

Lawmakers and regulators have long recognized the importance of increased environmental awareness in private industry. The Environmental Protection Agency, since its inception in 1970, has been challenged with striking a balance between environmental protection, society's needs, and economic development. The modern world of technology only intensifies that challenge by introducing concepts like NFTs, virtual twinning platforms, cloud computing, and multiplayer gaming—all important components within the metaverse.

The metaverse's promise to create a world where individuals are always connected to their digital twins will undoubtedly upend efforts to increase environmental protection. As the metaverse expands, so does its carbon footprint.

Metaverse emissions

The cloud alone has a greater carbon footprint than the airline industry, and Intel predicted that the metaverse needs at least a 1,000 times increase in computing power along with improved and additional infrastructure. How can the industry build a sustainable future when its current infrastructure and operation are seemingly unsustainable?

Within the metaverse's current infrastructure, virtual twinning platforms utilize massive amounts of energy and electricity to re-create the nearly infinite diversity of the real world. The American Council for an Energy-Efficient Economy estimated in 2012 that it takes 5.12kWh of electricity per gigabyte of transferred data. The Department of Energy estimates that the average U.S. power plant expends 0.855 pounds of carbon dioxide for a single kWh generated. Already-existing gaming systems, for example—played by more than 2 billion people worldwide—generate an ecological plight that will undoubtedly be compounded in the metaverse, with high-end gamers contributing as much as 2,000 pounds of carbon emissions into the atmosphere each year.

While twinning platforms and gaming have been the subject of ecocriticism, arguably, no metaverse component has been more heavily criticized than NFTs. NFTs are minted (or converted) by blockchain technology, paid for with cryptocurrency, and have become the predominant means for conveying digital art and virtual land. On average, the current blockchain transaction consumes 60% more energy than 100,000 credit card transactions; and an average Bitcoin transaction consumes 14 times more energy.

Current efforts to decarbonize technology

Most large technology companies have expressed strong commitments to eliminating carbon emissions. Some companies are already meeting 100% of their electricity needs through renewable energy power purchase agreements. Others have announced robust sustainability goals centered around reduced carbon emissions.

Gaming and technology companies within the metaverse have also committed to carbon footprint reduction. For example, Ethereum, a blockchain technology company, advertises itself as a "green blockchain" and recently upgraded its systems to reduce energy consumption. NFT companies are taking steps to reduce the number of blockchain transactions. And the Playing for the Planet Alliance has made commitments that include integrating green activations in games, reducing emissions, and supporting the global environmental agenda through initiatives to plant millions of trees and reduce plastic in their products.

Challenges to an environmentally sustainable metaverse

Despite efforts to increase and promote sustainability within the virtual metaverse, the physical world presents many challenges. Regulatory uncertainty in the U.S. and abroad, greenwashing, and conflict materials all pose significant challenges to environmental sustainability.

Regulatory uncertainty in global climate policy

As environmental responsibility and sustainability take center stage, private industry finds itself in a conundrum—which regulation takes precedence?

Data localization requirements, requiring customer data to be processed and stored on in-country infrastructure, may persuade companies to overlook sustainability goals and instead keep their less-efficient data centers.

Localization requirements could force companies to site their data centers in markets where renewable energy is difficult to procure or where operating conditions (e.g., heat, humidity, grid intermittency) create reduced efficiencies or rely on carbon-intensive backup generation.

U.S. antitrust laws may hinder competitors from working collaboratively on sustainability. Collaboration often offers solutions that are unavailable to individual companies because they lack the necessary capital or real estate.

Yet Federal Trade Commission Chair Lina Khan recently responded to a question at a Senate hearing by asserting that there is no ESG exemption to antitrust laws. A coalition, including 19 state attorneys general, sent a letter to an investment company in August 2022 expressing concern that "coordinated conduct with other financial institutions to impose net zero raises antitrust concerns." These concerns add to the tangled web of regulations that the metaverse will need to consider and address.

Greenwashing

Greenwashing occurs when an entity makes an unsubstantiated claim about environmental sustainability, intending to convince consumers that something is more environmentally protective than it is. Greenwashing often occurs through selective disclosure or symbolic actions:

- "Selective disclosure" means that a company highlights its potential environmental benefits, while excluding the disclosure of its negative attributes.
- "Symbolic actions" means that a company makes a gesture, like using green packaging, without actually engaging in environmental sustainability efforts.

Enforcement actions and civil suits alleging greenwashing are increasing both domestically and abroad. For years, the FTC has been policing corporate greenwashing, and the commission is poised to update their guidance on environmental claims—the Green Guides—later this year. The Securities and Exchange Commission recently launched the Climate and ESG Task Force "to identify potential violations including material gaps or misstatements in issuers' disclosure of climate risks under existing rules." And the Department of Justice has announced that DOJ will consider "all prior misconduct" for companies facing investigation, substantially increasing the risks for companies making sustainability claims.

This increase in enforcement—during a potentially transformative time within the metaverse—requires any sustainability claims within the metaverse to be genuine, specific, and contextual. For example, claims that purchases within the metaverse benefit the environment because it doesn't require physical production must be presented within the context that considers the emissions necessary to power the metaverse.

Conflict materials

The technology and infrastructure for the metaverse depend on significant supplies of certain metals and minerals. Conflict minerals such as tin, tantalum, tungsten, gold, and cobalt are key components in IT products, yet they are connected to armed conflicts and human rights abuses such as forced labor and child labor, violence, and widespread environmental degradation.

A report by the International Institute for Sustainable Development analyzes the supply chains for these metals and minerals. According to the report, the mineral excavation process uses toxic substances, which exposes workers who aren't provided protective equipment and negatively impacts soil, water, and human health. The risk to human rights and the environment have prompted governments to regulate through illegal mining laws, which the metaverse must navigate as its demand for minerals increases.

"Despite efforts to increase and promote sustainability within the virtual metaverse, the physical world presents many challenges."

Sustainable benefits within the metaverse

The challenges facing the metaverse and its heavy dependence on energy and electricity are not the end of the metaverse's sustainability story—the metaverse offers several environmental benefits.

Virtual reality offers consumers the opportunity to reduce emissions by substituting physical goods with virtual goods and real-world presence with digital interactions. It is feasible that customers could adjust their budgets for certain physical products to more sustainable virtual products.

The metaverse offers significant environmental benefits for industries like fast fashion and online markets, which can contribute to overproduction and overconsumption. A sizable portion of online sales were returned in the U.S. resulting in returns that double transportation miles, packaging, and stocking—all challenges the metaverse has the potential to reduce.

Whether going to work, the Seven Wonders of the World, or to a retail store to purchase products, the metaverse aims to offer these experiences without travel and the associated global emissions. In 2021, air travel accounted for over 2% of global emissions. We have since learned that many business meetings can be conducted virtually. The metaverse promises to enhance these experiences by re-creating many of the same benefits as in-person meetings without the emissions of travel.

Perhaps the most important environmental benefit of the metaverse is its ability to leverage technology to improve the identification and implementation of carbon-reduction plans. Digital twin platforms provide a panoramic view of the physical world that allows for optimization of sustainability efforts. Digital twins also make it possible to make predictions about environmental impacts.

Whether the metaverse lives up to its promise to create a world where individuals are always connected to their digital twins or falls short due to infrastructure and other hurdles, its impact on climate change, and particularly carbon emissions, is a concern.

The metaverse has already found its way into the U.S. court system, and its presence will likely grow as it grapples with the seemingly infinite environmental challenges that lie ahead. The legal community will continue to be instrumental in navigating these issues.

Social responsibility in the metaverse

The metaverse presents an opportunity for companies to create a different, better approach to accessibility, diversity, inclusion, and equity. But what does that look like, and what are the potential benefits and costs?

Advantages: Increased connection, community, and education

- Companies are increasing interactions with stakeholders on a more personal level and with fewer limitations on time and distance.
- Companies have the opportunity to create a more accessible, inclusive, and equitable metaverse since more people report feeling included in the metaverse than in real life.
- Institutions can provide medically safer COVID-19-free interactions.
- Educational institutions can provide immersive educational opportunities such as a surgeon practicing on virtual patients or primary school students virtually traveling to ancient Rome to experience history.

Challenges: Structural limitations

Modeling software and 3D graphics, networking and communication protocols, and artificial intelligence and machine learning algorithms continue to be subject to various limitations, privacy laws, and technical issues. For example, 3D graphics and modeling software may not be able to create highly detailed and realistic virtual environments that capture diverse and different backgrounds and experiences from the physical world. Indeed, biases embedded in AI and machine learning are already well documented and cannot be ignored.

The metaverse has already found its way into the U.S. court system, and its presence will likely grow...

Since the metaverse is still in its early stages, companies have the potential to create an improved, more accessible world. However, companies may want to consider the following policies and practices:

- Companies should consider creating and enforcing practices related to responsible technology and data collection in order to mitigate potential legal risks of data accumulation about the behavior of their users and their demographics (e.g., income group, age, gender, and skin color).
- Companies should consider creating incident response plans for data security breaches and revising data processing agreements with third-party vendors/service providers.
- Companies engaged in the metaverse should consider the accessibility of their products. For instance, using the metaverse is expensive, and electricity bills, bandwidth equipment, and micro transactions in the metaverse can be considered cost-prohibitive and pose as barriers to inclusivity.

The metaverse requires a significant amount of data to be transmitted between users and devices in real time in order to create a seamless and immersive experience, which can be a challenge in areas with limited or unreliable internet connectivity.

Governance—minding company operations in the metaverse

The final pillar of ESG, governance, has garnered less attention than the E and S. Still, it is important to understand because poor corporate governance has played a part in some large corporate scandals. The G relates to the rules and procedures that an entity, like a corporation, implements to guide decisions and determine rights and responsibilities among various stakeholders inside and outside the organization.

The metaverse provides companies with the opportunity to increase stakeholder transparency by engaging with them in an immersive virtual space.

Investors and consumers have shown more interest in a company's governance factors to better evaluate how decisions are being made about environmental and social factors. In response to increased interest and the importance of consistent governance policies in the physical world and in the metaverse, some companies are adding C-suite-level metaverse officers to oversee the company's metaverse expansion and impact.

In addition, the metaverse provides companies with the opportunity to increase stakeholder transparency by engaging with them in an immersive virtual space . For instance, a company could allow stakeholders to visit its metaverse processing center to see how the center impacts its community. With the increased attention on supply-level transparency, a company could provide detailed virtual experiences into the life cycle of a product or service.

The metaverse is undoubtably providing more opportunities for companies to communicate governance-related topics to its customers—an opportunity that should be heeded to ensure consistent messaging between the metaverse and the physical world.

Conclusion

Given the increased focus on ESG issues, companies should heed their ESG impact in the real world and the metaverse. Now is the time: Companies can take advantage of the nascent and malleable nature of the metaverse to help drive what the metaverse can do for them and their customers.

Published March 6, 2023. Copyright 2023 by Bloomberg Industry Group Inc., 800-372-1033. "ESG in the Metaverse: An Opportunity to Rethink Sustainability," https://www.bloomberglaw.com/external/document/XD81F1N4000000/esg-professional-perspective-esg-in-the-metaverse-an-opportunity.

Preetha Chakrabarti
Partner, New York
Advertising and Brand Protection

Helen Ogunyanwo
Counsel, Washington, D.C.
Advertising and Brand Protection

Felicia Isaac
Associate, Washington, D.C.
Environment and Natural Resources

Tiffany Aguiar
Associate, Orange County
Advertising and Brand Protection

Will Web3 and the Metaverse Give Rise to Brand Guidelines 3.0?

First, came e-commerce. Then social media and influencers. Now it's all about the metaverse.

Jonathan Brown, Preetha Chakrabarti, Suzanne Trivette

Emerging technology leads to evolving brand guidelines. With the rise of e-commerce, trademarks were being copied and exploited in ways they had never been before, and guidelines began to emerge for internal and external teams online. Next, brands had to adapt to social media. The Federal Trade Commission began to against influencers, and brands had to carefully monitor what claims influencers were making. Brands also had to attentively manage how their own employees were interacting with social media.

And the metaverse is next. While brands have only recently begun entering this new space, many have already made a substantial investment, and some have already experienced intellectual property infringement. Developing guidelines to specifically address the metaverse will be critical moving forward. What should go in your brand guidelines 3.0? This article offers some suggestions and guidance.

Enforcement

A novel aspect of the metaverse is the ease with which virtual elements can be copied and pasted and move between the 2D and 3D worlds. Brands will need to carefully check for infringing uses of their IP, even in areas (and industries) in which they normally wouldn't have to be vigilant. For example, Hermès would likely not have expected digital creator Mason Rothschild to turn its iconic leather Birkin bag into a faux fur-covered NFT, sometimes selling for more than a physical purse, before Hermès itself entered the metaverse. While some companies have already begun enforcing their rights in the metaverse, such as Hermès and Nike, the potential for infringement is rampant. Companies will need to carefully ensure that they are monitoring metaverse platforms for infringement and swiftly acting against it.

Expansion of rights

Not only will brands need to proactively protect their IP in the metaverse, but they will need to think strategically about how they wish to expand their rights. Several companies have already begun staking out IP rights in the metaverse.

For example, a number of fast food businesses have applied for metaverse-related trademark registration in classes such as 9, 35, 41, and 43. These applications contemplate the opening of virtual restaurants where consumers could order within the metaverse and have physical food delivered. Fashion brands such as Nike have also expanded metaverse-related trademark applications to include the sale of physical goods through virtual ones. These examples indicate that the brands that have applied for new trademark registrations do not necessarily believe their existing IP rights cover certain conduct in the metaverse. Thus, brands will want to carefully review their existing IP protections, consider ways they already cover uses in the metaverse, and consider broadening their IP rights along with any metaverse-related expansion.

This expansion of rights should be done in conversation with sales, marketing, and licensing teams that are often on the front line of trademark usage.

Brands will need to carefully check for infringing uses of their IP, even in areas (and industries) in which they normally wouldn't have to be vigilant.

Careful claims

Virtual influencers are influencers just the same in the eyes of regulators, and brands will need to carefully consider what claims are being made in the metaverse. For example, in April 2022, TruthInAdvertising.org sent a complaint letter to the FTC concerning metaverse platform Roblox and the potential that consumers were being deceived by hidden advertising. One of the potentially deceptive forms of advertising on the Roblox platform was through avatar influencers who were not disclosing their "material connections" to the brands at issue.

This example should serve as an important reminder that even if an influencer that is attracting consumers comes in the form of a bot or an individual using an avatar, this influencer must still disclose any material connections to the brand at issue. The TruthInAdvertising complaint also brought to light other metaverse-specific advertising concerns that brands should consider, such as the fact that it is not permissible to artificially inflate "likes" for services on a metaverse platform, that games combining advertising and gaming should carefully clarify the advertising portion, and that any sponsored content should be clearly disclosed.

Right of publicity

Another primary legal concern in the metaverse relates to the right of publicity. Individuals, including celebrities, influencers, and ordinary people, all enjoy a protected right to certain of their own identifiable characteristics, such as their name, image, voice, signature, etc. A company seeking to promote a brand in the metaverse must be careful not to do so in a way that evokes an affiliation with an identifiable characteristic of one's persona, unless there is a formal agreement in place to allow use of the persona.

For example, a company should not create a metaverse avatar that resembles a real person. As companies think strategically about collaborating with third parties for various metaverse initiatives, the right of publicity guidelines outlined below can serve as a foundation on which to build and implement robust right of publicity metaverse brand protection guidelines. Individuals seeking to partner with the company must enter into a formal, written agreement in order for their name/image/likeness to be used in association with the brand. This includes, but is not limited to, use of the brand in connection with an avatar, virtual property, virtual events, virtual sponsorships, etc.

1. All NIL agreements must contain a release of applicable legal claims, including, but not limited to, claims for copyright or trademark infringement, infringement of moral rights, libel, defamation, invasion of any rights of privacy (including intrusion, false light, public disclosure of private facts, and misappropriation of NIL), violation of rights of publicity, physical or emotional injury or distress, or any similar claim or cause of action in tort, contract, or any other legal theory.
2. Individuals with whom the company collaborates are not permitted to create social media accounts (such as Facebook fan pages, Twitter accounts, etc.) that include company trademarks, nor are they permitted to post content incorporating company trademarks without prior written consent.
3. All promotions incorporating company brands and marks are to be controlled exclusively by the company.

NFTs

Issuance of unique NFTs is emerging as an opportunity for companies to create new ways to engage consumers and foster brand excitement and loyalty. However, companies should consider the ownership rights being conveyed upon a sale of an NFT before releasing NFTs into the marketplace. Generally, an NFT issuer will want to retain control over the digital work they have created and limit any transfer of rights to the purchaser. The NFT guidelines below are a good starting point for brands looking to mint NFTs to consider.

1. Without a license arrangement with the company, everything about a third-party NFT (including developer name, NFT name, NFT image, and other NFT properties) must be unique to the third party and free of the company's brand assets.
2. The company's brand assets are not permitted to be used in a manner that implies the company developed, endorsed, is affiliated with, or is otherwise connected with a third party's NFT. Furthermore, the company's logos, designs, and icons can never be used in connection with a third party's NFT and can only be used in third-party advertisements with a license agreement in place.
3. Copyrights in NFTs minted by the company must be retained by the company and not assigned/transferred.
4. NFTs minted by the company must include imbedded authentication (i.e., a unique watermark or other identifier to verify authenticity).
5. All company-minted NFTs must be released via an Ethereum Name Service domain name.

Digital assets as securities

A common question with respect to digital assets, and in particular NFTs, is whether they qualify as regulated financial products. If an NFT provides its holder the right to income streams or to a share in an underlying portfolio of investment assets, then the NFT potentially becomes a regulated financial product. For example, an NFT that gives its holders rights to a share of royalties generated by underlying music catalogs may be considered a security, thereby triggering a number of financial regulatory compliance requirements. As such, companies that issue NFTs must be cognizant as to whether their NFT offerings may qualify as securities. The guidelines below may help companies structure their digital asset offerings in a manner that avoids such offerings from becoming a regulated product.

1. Company-issued NFTs must be issued by a decentralized autonomous organization or other protocol that is fully decentralized (i.e., centralized control is not exercised by any particular person).
2. Company-issued NFTs must never be described as "investments."
3. Company-issued NFTs must never convey a form of payment to the purchaser.
4. Company-issued NFTs must be sold to a single purchaser such that the purchaser owns the entire NFT.

An abridged version of this article appeared in *MediaPost's* "Marketing Insider" on Feb. 16, 2023, and can be found at https://www.mediapost.com/publications/article/382621/will-web3-and-the-metaverse-give-rise-to-brand-gui.html.

Jonathan Brown
Associate, Chicago
Advertising and Brand Protection

Preetha Chakrabarti
Partner, New York
Advertising and Brand Protection

Suzanne Trivette
Associate, New York
Advertising and Brand Protection

Privacy and Cybersecurity Considerations for Artificial Intelligence in the Metaverse

Protecting customers and companies in the brave new world of AI

Garylene (Gage) Javier, Christiana State

Technology is advancing at a rapid pace, and at the forefront of this evolution is artificial intelligence and the metaverse. AI systems have access to vast amounts of personal data, and the metaverse offers a new platform for social interaction and commerce. As the use of AI becomes increasingly ubiquitous and the metaverse continues to evolve, organizations should contemplate the implications posed by the use of AI in the metaverse, including:

1. Data privacy concerns,
2. Algorithmic and automated decision-making bias,
3. Cybersecurity threats, and
4. Regulation.

What is artificial intelligence?

AI, broadly, is the simulation of human intelligence processes by machines, especially computer systems.[1] AI developers use algorithms and statistical models to "train" the AI system to generate conclusions. This requires the ingestion of significant volumes of data collected from various sources and incorporated into the instruction of the AI system. The "training" results in the ability for AI to execute tasks such as recognizing images, understanding natural language, making decisions, and playing games.

There are different types of AI,[2] including:

- Reactive AI (reacts to the environment but has no memory and is not self-aware);
- Limited-memory AI (ability to absorb learning data and improve over time);
- Theory-of-mind AI (machines would have the capability to understand and remember emotions and adjust behavior based on those emotions); and
- Self-aware AI (aware of emotions and mental states of others, but also their own).

As of today, the most used andxdeveloped AI are reactive and limited-memory AI, while others have not yet been effectively developed.

What is the metaverse?

The "metaverse" is not one place. Rather, the term refers to a virtual world or a shared virtual space where physical and virtual reality converge and allow users to, among other things, socialize, experience new forms of entertainment, and engage in commerce. Developers can create their own versions of this interactive and immersive technology environment in which users can engage virtually using devices such as VR headsets.

Data privacy

Privacy issues should be contemplated throughout each phase of the use of AI in the metaverse. This includes the AI training phase, use within the metaverse, and ongoing updates to the AI system.

AI training phase

When developers initially train the AI system, they rely on large data sets to perform specific tasks or make decisions based on data inputs. These data sets generally represent the issue the AI system is meant to solve, and as the system goes through the iterative process of testing the output for accuracy, developers

[1] https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

[2] https://builtin.com/artificial-intelligence/types-of-artificial-intelligence.

adjust the algorithms (weights) to more precisely analyze the data set to subsequently produce the desired outcome. The use of large data sets raises issues of data ownership, appropriate disclosures, and the protection of personally identifiable information.

Data can be sourced from worldwide data collections and processed for training and validating machine learning models and user studies. Such collections of information may be gathered from third-party data brokers or the data owners themselves. Organizations using these data sets inherently must rely on the representation that their data sources acquired the appropriate permissions from data owners for data use, sale, or sharing.

These data sets may include PII; however, several state privacy laws require that notices be provided at collection, giving individuals the ability to understand, for instance, why their information is being collected, how it is used, and whether it is shared with other entities. For example, the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020, which was the first comprehensive privacy legislation in the United States, provides: "A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of ... [t]he categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared."[3] Unless the organization developing AI acquires data directly from known data owners, it is challenging to ensure that proper privacy disclosures were issued at the time the data was collected.

Accordingly, AI developers should consider the origin of their data sets and assess whether they are reasonably confident that the appropriate disclosures were provided at the onset of collection and, subsequently, whether incorporation of the data into the training and machine learning process is appropriate. In addition, depending on the nature of the data and the uses for such data, it is sometimes necessary to actually obtain consent from the individuals before using such data for machine learning model training.

Data use in the metaverse

The metaverse provides individuals a platform to engage in commerce and immersive experiences such as gaming within the virtual space. As world building often uses AI and user avatars, AI may be used to interpret an avatar's or user's actions in order to progress through the environment. Such behaviors are often captured by hardware such as VR headsets and handheld gaming devices. Information from these devices can include, among other things, device ID numbers, geolocation, biometric data, environmental data, and behavioral data. In instances where organizations develop a virtual presence, such as a retail store within a metaverse platform, the in-person shopping experience is replicated in the virtual space. Here, natural language recognition AI could be leveraged, and text or voice data is ingested to train the AI system to develop more realistic customer interactions.

In both examples, data may be transferred from the user hardware to the retailer or game developer as well as the organization whose metaverse platform in which the game or virtual store is created. In these scenarios, safeguards should be put in place to ensure transparency related to the sharing of user data. In fact, state privacy laws like the CCPA require that businesses must provide consumers with the right to know what personal information is sold and shared and to whom.[4] To mitigate risk, organizations should be transparent with their users on how their data is being leveraged for AI within the metaverse.

Updates to the AI system

The effectiveness of an AI system is reliant on its ability to determine outcomes and make decisions based on the most current available information. Accordingly, data sets must regularly be refreshed. However, there are certain instances where this constant collection and use of information for the purpose of updating an AI system may encounter compliance issues with privacy laws.

One scenario involves scientific analysis or research. For instance, research into predictive analytics for user behavior analysis, machine learning for avatar personalization, or natural language processing for conversational AI agents may involve data sets that could incorporate personal information. Here, some privacy laws like the CCPA impose certain rules regarding information used for research purposes. Particularly:

"Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be: (1) compatible with the business purpose for which the personal information was collected ... (2) subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business ... (7) used solely for research purposes that are compatible with the context in which the personal information was collected."[5]

To mitigate risk, organizations should be transparent with its users on how their data is being leveraged for AI within the metaverse.

[3] Cal. Civ. Code § 1798.100(a)(1).

[4] Cal. Civ. Code § 1798.115.

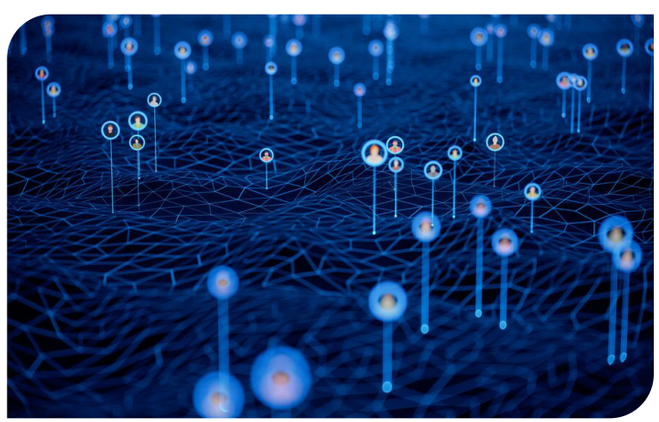
[5] Cal. Civ. Code § 1798.140(ab).

The inner workings of AI systems in the metaverse can be opaque, making it difficult for users to understand how decisions are being made and what data is being used.

Given the immense amounts of data ingested by AI training and sourced internationally, complying with requirements such as those of the CCPA may be challenging. To train AI in compliance with legal requirements for certain scientific research projects may entail using data specifically obtained and labeled as research data. Such a process would involve giving individuals notifications and obtaining specific consents that are specifically tailored for a given research project.

Algorithmic and automated decision-making bias

The use of AI in the metaverse may inherently create user profiles on which certain decisions may be based. Organizations leveraging AI in this space would need to be mindful that profiles created by unverified and widely sourced information are not used to generate decisions that may negatively impact or be biased toward a certain consumer or demographic, particularly if the decision making is automated. This may be problematic where AI algorithms used in the metaverse may perpetuate biases based on the data they were trained on, leading to discriminatory outcomes and experiences for certain users. The inner workings of AI systems in the metaverse can be opaque, making it difficult for users to understand how decisions are being made and what data is being used.



States have expanded consumer rights to include giving consumers certain rights in connection with automated decision making, particularly if it produces a legal effect or significantly affects the individual. Under the CCPA, certain information used to build consumer profiles must be disclosed and may be subject to a right of opt-out for automated decisions. Additionally, the CPRA added a new definition of "profiling," giving consumers opt-out rights with respect to businesses' use of "automated decision-making technology," which includes profiling consumers based on their "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[6]

In addition, organizations that use AI to make automated decisions about consumers face another challenge—explaining how the AI works. This is a very difficult task given the "black box" nature of predictive AI algorithms. The CPRA charges the California Privacy Protection Agency with adopting regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology,"[7] including providing meaningful information about the logic of the decision and the likely outcome with respect to the consumer. While such guidance has yet to be issued, organizations contemplating the use of AI in the metaverse should bear in mind the potential rights of consumers that state privacy laws may impose and consider how the AI system may be able to practically produce supporting evidence of its automated decision regarding a metaverse consumer.

Cybersecurity threats

The metaverse is susceptible to various cybersecurity threats such as hacking, malware, and data breaches that put user data at risk. Users' personal data can be collected, shared, and exploited by metaverse operators, AI algorithms, and other users, creating the risk of identity theft, fraud, and privacy violations.

Security breaches may pose a challenge to organizations leveraging AI in the metaverse because such incidents may require data breach notifications.

Security breaches may pose a challenge to organizations leveraging AI in the metaverse because such incidents may require data breach notifications, depending on the scope and type of data impacted. As summarized by the International Association of Privacy Professionals, "U.S. data breach notification laws vary across all 50 states and U.S. territories. Each law must be applied to every factual scenario to determine if a notification requirement is triggered."[8] Given that PII may be gathered in large volumes in order to train AI systems, the impacted population may be quite significant.

Furthermore, how AI may be used by various organizations in the metaverse is still unknown. Should security incidents occur, certain industries may require compliance with specific data breach notification obligations. For example, the Office of the Comptroller of the Currency within the Department of the Treasury, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corp. issued a final rule that requires a banking organization to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," and under certain circumstances, notify each affected banking organization customer.[9] The practical exercise of identifying impacted consumers may be challenging given that the volume of consumers could be significant.

[6] Cal. Civ. Code § 1798.140(z).

[7] Cal. Civ. Code § 1798.185(a)(16).

[8] https://iapp.org/resources/article/state-data-breach-notification-chart/.

[9] https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

Given the potentially vast scope of the use of AI in the metaverse and how its use may cross borders, different countries and regions will have different approaches to its regulation.

To mitigate cybersecurity threats, a combination of technical and nontechnical measures may be helpful, including (i) ensuring that personal data used to train and operate AI systems is properly secured and protected from unauthorized access, theft, and misuse; (ii) providing increased human oversight and intervention to help detect and address cybersecurity threats associated with AI systems in the metaverse; and (iii) conducting regular security audits.

In January 2023, the National Institute of Standards and Technology released the NIST AI Risk Management Framework[10] to better manage the risks to individuals, organizations, and society associated with AI. Organizations looking to leverage AI in the metaverse should consider reviewing the AI RMF for recommendations on how to address, document, and manage AI risks and potential negative impacts effectively in order to establish more trustworthy AI systems.

Regulation

The use of AI in the metaverse raises questions about jurisdiction, liability and accountability, and the need for clear, comprehensive regulation. Given the potentially vast scope of the use of AI in the metaverse and how its use may cross borders, different countries and regions will have different approaches to its regulation.

In the United States alone, numerous pieces of legislation related to AI were introduced and enacted, having been prompted by concerns about potential misuse or unintended consequences of AI.[11] Recently, U.S. Rep. Ted Lieu used AI to draft the first AI-written bill for Congress,[12] signaling that AI is a current national issue. The development of AI in the metaverse is also likely to involve a range of stakeholders, including technology companies, governments, academic institutions, and public interest organizations. Regulation may also be influenced by broader international trends and agreements, such as the United Nations' discussions on responsible uses of AI[13] and the development of a global regulatory framework for AI.[14] The regulatory proposal aims to "provide AI developers, deployers and users with clear requirements and obligations regarding specific uses of AI. At the same time, the proposal seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises."[15] As it stands, existing regulatory frameworks such as the CCPA, the CPRA, and the European Union's General Data Protection Regulation[16] covering technology and data privacy may be used to regulate AI in the metaverse in the interim.

Conclusion

The convergence of AI and the metaverse opens up incredible possibilities for advancement in innovation, social engagement, education, and global connectivity. However, with such progress, we must also consider the privacy and cybersecurity implications in order to mitigate risk and take thoughtful and deliberate steps toward protecting individuals and organizations in the metaverse while leveraging AI.

This article originally appeared on Competition Policy International on March 16, 2023: https://www.competitionpolicyinternational.com/complex-technologies-converge-privacy-and-cybersecurity-considerations-for-artificial-intelligence-in-the-metaverse/.

[10] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[11] https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence.

[12] https://www.msnbc.com/the-reidout/reidout-blog/ted-lieu-chatgpt-ai-bill-congress-rcna67944.

[13] https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence.

[14] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[15] Id.

[16] https://gdpr-info.eu/.

Garylene (Gage) Javier
Associate, Washington, D.C.
Privacy and Cybersecurity

Christiana State
Senior Counsel, San Francisco
Privacy and Cybersecurity

Expanding the Runway: Fashion and the Metaverse

The risks and opportunities facing the next frontier in fashion

Suzanne Trivette, Risa Rahman, Emily Kappers, Preetha Chakrabarti

Through the metaverse, the global fashion marketplace is experiencing unprecedented digital transformation that will fundamentally reimagine and expand how consumers experience fashion. The power of the metaverse does not end in its untapped monetary valuation (estimated at $800 billion over the next 10 years); it also provides a digital platform that creates new ways for global companies to connect with their consumers. With all that this medium has to offer, it is no surprise that major fashion brands are tuning in and entering the metaverse in droves.

At the same time, the metaverse presents risks for unauthorized brand exploitation and intellectual property infringement. As fashion brands seek to expand their presence in the metaverse, they should increasingly think about how to protect their IP from infringement in the virtual world while staking out a claim to newly available virtual real estate and accompanying IP rights.

Opportunities

Virtual fashion shows

Along with other industries, fashion brands are creating virtual experiences for consumers in the metaverse that expand their offerings in the physical world. For example, brands are beginning to advertise to consumers across the globe using innovative immersive experiences and virtual promotional events, as well as allowing consumers to buy products and services using digital wallets. Legacy powerhouses and new entrants alike are already creating virtual fashion experiences to showcase their collections and expand their brand recognition:

- Fendi partnered with online game Honor of Kings in November 2020 to launch a limited-edition collection of wearable virtual items, including a handbag, a jacket, and shoes.
- Balenciaga collaborated with online game Afterworld: The Age of Tomorrow in December 2020 to showcase its Autumn 2021 collection. Set in a dystopian future, the game featured virtual models wearing the collection and allowed players to interact with their virtual cityscape, including by entering virtual stores.
- In April 2021, Louis Vuitton showcased its Autumn/Winter 2021 collection through a virtual experience called “Louis Vuitton Walk in the Park.” The experience allowed users to navigate through a virtual park to view the collection in an immersive experience using 360-degree technology.
- In May 2021, Gucci collaborated with digital fashion platform Roblox to create the “Gucci Garden Experience.” The experience, which showcased Gucci’s Aria collection, was set in a virtual garden, featuring virtual models wearing the designs and interactive elements like mini-games and virtual stores.

As technology continues to evolve, we can expect to see more fashion brands embrace the metaverse to showcase their collections.

Digital designs

In addition to hosting virtual events, fashion houses are exploring new ways to create digital clothing for users’ avatars to wear within the metaverse. While some brands are creating virtual replicas of their physical designs, others are taking greater creative liberties to craft designs that would be physically impossible or impractical in the real world.

Brands are also innovating through the use of NFTs as currency for the purchase of their digital clothing. For example, in 2020, digital fashion brand The Fabricant sold a virtual dress for $9,500 using an NFT. Gucci sold a digital sneaker using an NFT

in 2019. Both items were wearable in virtual environments, and the buyers could use their NFTs to prove ownership.

One of the benefits of using NFTs as currency for virtual fashion clothing is that it creates a sense of ownership and exclusivity, just like owning a physical piece of clothing would. Because of their unique and trackable nature, NFTs also allow for easy buying and selling of digital fashion items within the metaverse.

Challenges

Trademark implications

As the fashion industry continues to explore the metaverse as a new platform to showcase designs, there are important trademark infringement implications to consider. The courts are beginning to assess trademark infringement issues as applied to virtual goods and services. This is particularly true in the wake of the *Hermès Int'l v. Rothschild* "MetaBirkins" dispute, which set an important precedent for trademark infringement in the metaverse and highlights the challenges in enforcing trademark rights in virtual environments.

Last year, Hermès filed a trademark infringement suit against Los Angeles-based designer Mason Rothschild for creating and selling faux-fur digital renditions of the luxury Hermès Birkin handbags and using a collection of 100 NFTs, titled "MetaBirkins," to authenticate the digital images. On 8 February

2023, a Manhattan federal jury found that Rothschild's "MetaBirkin" NFTs infringed and diluted the Hermès trademarks for its Birkin bags, and that Rothschild cybersquatted on the 'metabirkins.com' domain name. Rothschild was ordered to pay $110,000 for trademark infringement and dilution, and $23,000 in statutory damages for cybersquatting.

This verdict shows that virtual trademark infringement has consequences just as it would in the physical world. In the initial stages of the lawsuit, Rothschild argued that the MetaBirkin NFTs were non-infringing because they were "art" and, therefore, received First Amendment protection. However, this argument ultimately did not succeed. The court instead found that Rothschild was unfairly profiting off a false association with the Birkin name.

Despite this promising outcome for trademark protection in the metaverse, digital items can be swiftly replicated and distributed, which can make it challenging to enforce trademark rights. For example, a user like Rothschild can easily create a virtual replica of a luxury brand's logo or design and use it within a virtual environment without permission, potentially causing confusion among consumers about the origin of the goods. This can be especially problematic for luxury brands, which rely heavily on their brand image and reputation to maintain their market position. In such an environment where goods can be effortlessly replicated without authorization, it may also be more difficult to maintain the distinctiveness of a trademark, potentially leading to dilution over time.

The issue of NFT authentication for virtual fashion items on sale in the metaverse has already found its place in two courts.

The *Hermès Int'l v. Rothschild* court speculated that First Amendment protection may not be extended to such situations. Instead, the courts may recognize digitally wearable clothing items (and other products and services) connected to NFTs as protectable commodities, which may provide more comfort to brands concerned about rampant infringement.

Additionally, in 2021, Nike filed a lawsuit against online resale platform StockX. Nike alleged that StockX was 'minting' NFTs that prominently use Nike's trademarks. As discussed further in this article, Nike had already filed several metaverse-related trademark applications. This example demonstrates how brands may wish to preemptively obtain trademark protection in the metaverse to prepare for similar instances of unauthorized use.

As the metaverse continues to develop, it is important that brands remain aware of evolving legal frameworks to address trademark protection in virtual environments.

One of the benefits of using NFTs as currency for virtual fashion clothing is that it creates a sense of ownership and exclusivity, just like owning a physical piece of clothing would.

Copyright implications

Historically, copyright protection for fashion designs has been thin. According to the two-prong Star Athletica test, the aesthetic elements of a useful article (e.g., a piece of clothing) are copyrightable only if:

- The element can be perceived as a 2D or 3D work of art separate from the useful article; and
- The element would qualify as a protectable pictorial, graphic or sculptural work on its own or fixed in another medium if imagined separately from the useful article.

In the physical world, fashion design is limited by physical realities such as fabric, gravity and cost. Additionally, fashion designs must generally be functional and wearable. But in the metaverse, users interact using virtual personalized avatars that are not limited by the laws of physics or functionality. This will allow fashion brands to explore over-the-top fantastical fashion designs that may even be physically impossible.

Given fashion in the metaverse is tailored for an avatar and not a living person, a fashion brand's creative choices will likely be aesthetic rather than functional. Perhaps this will even result in a new standard for what constitutes a 'useful article' and what can be imagined separately within the meaning of Star Athletica.

Sculptural designs are often difficult to create and can be cost prohibitive in the physical world. Brands in the metaverse do not face this problem. Fashion designer Zuzanna Blasco has already created a jellyfish dress using AI technology.

The fashion industry is likely to experience a significant increase in similarly over-the-top, fantastical virtual wearable designs that are more easily viewed as sculptural and pictorial within the meaning of Star Athletica. If Star Athletica remains the standard, the fashion industry may begin to experience more copyright protection for virtual wearable clothing compared to physical clothing.

Hermès v Rothschild also addressed how an NFT linked to virtually wearable clothing may be considered a commodity rather than art. Because virtually wearable clothing is non-physical, it may not be evaluated under Star Athletica at all. Instead, it is possible that brands could receive copyright protection for virtual fashion akin to that for software or a work of graphic art. Virtual designs do not have the same functional characteristics as physical clothing, bringing virtual fashion closer to, for example, a painting of a person wearing a dress than a wearable textile that is necessary for human needs such as cover and warmth.

There may also be even more of a need for copyright protection for virtual fashion, which can be easily replicated and distributed, making it more difficult to distinguish between original designs and copies.

The Star Athletica test could ultimately help to determine the eligibility of virtual fashion designs for copyright protection. However, the test does not necessarily or seamlessly apply to digital fashion items. Instead, it is likely that new legal frameworks will need to be developed to address the copyright issues that arise for fashion design in the metaverse.

Accessibility

In addition to concerns over copyright and trademark protection, the metaverse also raises a novel issue for brands: exclusivity.

For many legacy fashion powerhouses, the value of a brand lies in its exclusivity. Access to products and stores as well as fashion week and other marketing events is and was historically limited. This can impact consumers who may not live near a physical location and lack the opportunity to shop in a luxury store. Brands may also generally limit online purchases or restrict them to consumers who have already bought products in-store. Many fashion week events are reserved for buyers and the press, and even those open to the public require an often-expensive ticket.

The metaverse changes this, creating a level of access that was never previously possible for many consumers. While this opens sales up to a broader set of consumers, creating a new avenue of trade for brands, it also may impact the exclusive nature of luxury fashion powerhouses. Because of this, it is possible that brands will have to re-think the nature of exclusivity, possibly even re-defining it.

The accessibility that the metaverse brings also includes the unprecedented integration of the physical and virtual world. The metaverse fundamentally imagines the two becoming seamlessly connected, allowing consumers to move between them with ease. Fashion brands may even provide the option for consumers to buy a product in the physical world that allows them to attend a virtual event or buy a virtual product or service for their online avatar (e.g., a ticket to a virtual concert).

On the flip side, consumers may be able to buy something online (e.g., an accessory for an avatar), that allows them to buy something similar or gives them a discount in the physical world. Additionally, consumers may be able to shop in online stores and purchase goods that are physically delivered to them in real life.

All of these transactions not only invoke concerns of maintaining exclusivity, but potentially change the definition of customer service, as well as raising a host of concerns such as consumer complaints or product liability issues.

In a similar vein, the metaverse turns the concept of quality control on its head. Many fashion brands use quality control provisions in their vendor and partnership contracts. But what is quality control in the metaverse? Is it high resolution pixels for virtually wearable clothing, fast data transmission rates, a high-resolution shopping experience free of bugs or lags, customization or other personalized options, or something else? Brands will now have to carefully consider how they wish to define quality control as they are designing virtual stores and goods and before entering into agreements with programmers, partners, or others.

How to...

Mitigate risks arising from collaborations

Not only is it easy for users to create and distribute virtual versions of branded items without permission, the widespread exposure from collaborations with other brands or designers in the metaverse can also lead to increased unauthorized use of a brand's IP. Collaborating with other brands or designers in the metaverse can result in a loss of control over a brand's image, potentially leading to consumer confusion about the brand's image or values and to eventual brand dilution.

To protect themselves from these risks, fashion brands should develop brand guidelines for collaborations in the metaverse. These guidelines should include clear policies on the use of the brand's IP (e.g., logos and designs), as well as guidelines for the use of the brand's trademarks in virtual environments.

Brand guidelines should also establish expectations for the quality and integrity of collaborations, ensuring that the brand's values and mission are upheld.

To protect themselves from these risks, fashion brands should develop brand guidelines for collaborations in the metaverse.

Fashion brands can also consider using technologies such as blockchain to protect their IP in the metaverse. Blockchain allows for the secure and transparent tracking of digital assets, making it more difficult for unauthorized users to replicate or distribute virtual versions of branded items without permission. With blockchain technology, fashion brands can protect their IP and maintain greater control over their brand image in the metaverse.

Register metaverse-related goods and services

In 2021, many fashion brands preemptively filed metaverse-related intent-to-use trademark applications in anticipation of expanding their products and services to the metaverse. Since the fashion industry is in the initial stages of implementing metaverse technologies, these intent-to-use trademark applications provide an interim safeguard for brands even if they have not yet expanded into the metaverse, but intend to. In most jurisdictions, the first applicant to file a trademark application will own rights in the trademark. Therefore, even if a fashion brand has not expanded its designs or virtual experiences into the metaverse, an intent-to-use application filing date will establish a priority date, even if actual use occurs later.

The fashion brands that have sought metaverse-related trademark protection have applied for protection in connection with:

- "Downloadable virtual goods" (Class 9);
- "Retail store services featuring virtual goods" (Class 35);
- "Entertainment services, namely providing online, non-downloadable virtual [products and services] for use in virtual environments" (Class 41);
- "Online non-downloadable virtual goods and NFTs" (Class 42); and
- "Financial services, including digital tokens" (Class 36).

For example, Nike filed several metaverse-related intent-to-use US applications for its most famous marks, including the Nike name, the swoosh logo, JUST DO IT and the Jordan marks in Classes 9, 35 and 41.

However, brands cannot merely file intent-to-use applications without specifying how they plan to use their marks in the metaverse. In October 2021, USPTO examining attorney Barbara Rutland issued several office actions requesting that Nike clarify its timeline in connection with its "indefinite" identification of goods and services for use in the metaverse. Rutland found that the "precise nature of the goods and services is unclear" and that Nike should provide "clarifying wording" to overcome the rejection.

On the other hand, Converse had three metaverse-related US trademark applications allowed in November 2021 without receiving any office actions, indicating that the USPTO found them sufficiently specific.

Fashion brands should also consider filing trade dress applications for any virtual fashion environments that they plan to implement. A trade dress registration protects the overall grouping of interacting elements of a store. Many companies are beginning to create twin environments to their physical locations. As fashion brands work with graphic designers and software engineers building out their virtual fashion experience, an intent-to-use application could be considered for that virtual environment.

Fashion brands should also consider filing trade dress applications for any virtual fashion environments that they plan to implement.

Detect and enforce against infringing use

Many examples of infringement in the metaverse so far involve fashion brands. However, given the limitless nature of the metaverse, it is difficult to detect infringing uses. The metaverse is far more complex than traditional online marketplaces because it is largely decentralized. As a result, users may receive unfettered access. While a decentralized autonomous organization exists to monitor compliance with terms of use and other policies of metaverse platforms, this entity acts in response to users' votes rather than in accordance with legal rules. Ultimately the DAO lacks legal authority to enforce and monitor trademark infringement. As an added layer, virtual personae provide anonymity to users.

As of now, brands may learn of IP infringement through careful tracking of consumer engagement and trademark applications. For example, Hermès learned about Rothchild's infringement through the MetaBirkin NFTs' increasing popularity.

Additionally, bad-faith actors are filing preemptive metaverse trademark applications, just as legitimate brands are. This has already impacted Prada and Gucci. So brands should also monitor IP office databases for new applications filed under Classes 9, 35, 36, 41 and 42 that relate to their known trademarks.

For copyright infringement, brands can rely on existing notice-and-takedown procedures. For example, under the U.S. Digital Millennium Copyright Act, copyright holders and their agents can notify platforms about infringing material and request that this material be removed.

... in the coming years, we anticipate more case law development, trademark office guidance, and IP enforcement as the metaverse itself develops.

Six practical takeaways

The metaverse is a powerful digital platform with the potential to offer imaginative virtual fashion designs and experiences. Like brands, courts and trademark offices across the globe are attuned to these technological changes.

The MetaBirkins case set a promising precedent that trademark infringement in the metaverse will be taken seriously, but in the coming years, we anticipate more case law development, trademark office guidance, and IP enforcement as the metaverse itself develops.

It is difficult to forecast the strength of copyright and trademark protection for fashion in the metaverse – and how these standards may change or apply differently from those in the physical world. But until more case law develops, brands can stay ahead of the game by taking the following measures:

1. Apply for trademark and trade dress protection in accordance with jurisdictional requirements for marks, logos, and virtual fashion environments as soon as possible. Brands that plan to use their trademarks in the metaverse but have not yet started can file intent-to-use applications.
2. Specify exactly how trademarks will be used in the metaverse when applying for a registration.
3. Develop tailored brand guidelines for collaborations and partnerships, carefully delineating how IP will be used.
4. Track and monitor IP office databases for bad-faith applications filed under Classes 9, 35, 36, 41, and 42.
5. Implement blockchain technologies to securely track digital assets.
6. Incorporate quality control provisions into any vendor or partnership agreements on digital platforms.

Eventually, the metaverse may alter how fashion-related IP is conceptualized as well as protected. In the meantime, and even though the metaverse is still in its early stages, it is crucial for brands to take the necessary precautions to protect their new and existing designs.

This article first appeared on World Trademark Review, www.WorldTrademarkReview.com

Suzanne Trivette
Associate, New York
Advertising and Brand Protection

Risa Rahman
Associate, Washington, D.C.
Advertising and Brand Protection

Emily Kappers
Counsel, Chicago
Advertising and Brand Protection

Preetha Chakrabarti
Partner, New York
Advertising and Brand Protection

Brands, How Well-Versed Are You in the Metaverse?

Trademark protections in the digital world

Andrew Avsec, Matteo Mariano, Risa Rahman

With the emergence of the "metaverse," the global marketplace is experiencing unprecedented digital transformation, and brands are tuning in. This type of digital platform provides new opportunities for global companies to connect with their consumers. At the same time, it also offers a new opportunity for unauthorized brand exploitation and infringement. As companies seek to expand their presence in the metaverse, brands have been increasingly interested in how to protect their existing intellectual property from trademark infringement in the virtual world while also obtaining new metaverse-related trademark protection for their own brands.

The metaverse is a powerful digital tool to expand a brand's presence

Currently, there are different types of existing metaverses. The first type of metaverse is centralized, in which particular entities or companies manage the activities of users in a particular metaverse world. This occurs in video games, such as Minecraft or Fortnite, in which the metaverse world is contained within and limited to the world created within the videogame.

On the other hand, there are decentralized, or open, metaverses. In this case, particular entities or companies do not manage the activities of users as they would in a centralized metaverse world. Rather, the functions of the metaverse world are decentralized through the use of blockchain technology. Decentralized autonomous organizations manage decentralized metaverse worlds. In this case, users vote on their own rules for managing the metaverse world and those agreed-upon rules are encoded as a transparent computer program that is controlled by DAO members.

All metaverses are virtual worlds. Users typically interact using personalized avatars that represent their virtual personae. Post-pandemic, industries shifted toward establishing remote on-screen communication and collaboration on a more structural basis. This in turn led to many businesses implementing metaverse use cases as a new method of communication and as a collaborative e-commerce business paradigm that offers products and services without geographical barriers.

In the metaverse, users can come together in an interconnected digital space and perform many activities that could be performed in the real world. For example, users can talk to each other in a virtual park, attend a concert, buy and sell virtual goods (such as clothing and accessories), adopt pets, play games, and even secure jobs. This in turn means that companies may do many of the things they do in the real world. For example, companies may advertise, buy and sell virtual property, provide services, meet customers and prospects, and sell virtual goods. Brands can replicate many real-world social and economic interactions using traditional, state-issued currencies, in-game currencies, cryptocurrencies, and, of course, NFTs. Many companies are minting NFTs and creating digital assets using their well-known trademarks.

Companies have also engaged in fairly routine, traditional business activities, such as by creating virtual meeting spaces and offices that replicate their offices in the real world. To visualize this, consider the following use case. You have a scheduled meeting with key stakeholders located across the world. With the metaverse, you can put on a virtual reality headset that will transport you to a shared virtual conference room with the other stakeholders without leaving the comfort of your own home. In this conference room, you can interact with the other stakeholders, with the use of your respective avatar, just as you would in a conference room in the real world.

With its limitless structure, the metaverse offers countless marketing and commercialization opportunities for brands, especially in the retail industry.

There are many benefits to expanding business presence into the metaverse, including advertising using innovative storytelling immersive experiences, interacting with consumers across the globe without physical barriers, using digital wallets that replicate real-world financial transactions, and offering promotional events and services virtually.

In this respect, the metaverse serves as a new digital marketplace and is providing opportunities for companies to increase scalability and accessibility of their products and services. Currently, metaverse worlds may be 2D or 3D. VR goggles may not be required to engage with some metaverse platforms currently, and many do not support VR yet. However, that is expected to change as the metaverse develops over the next decade. In fact, it is estimated that over the next 10 years, the value of the metaverse will reach $800 billion. There are limitless possibilities with the metaverse, and businesses are looking for opportunities to leverage the metaverse to promote their brands.

Detecting infringements in the metaverse

Just like the metaverse contains real consumers and real businesses, it contains real infringers as well. There are several approaches companies may pursue to identify infringers in the metaverse.

A company may assign a person or team to periodically shop or search for counterfeit or infringing items in the metaverse and on NFT marketplaces such as OpenSea, Rarible, and Mintable.

Companies may also use brand protection vendors, such as Corsearch or Redpoints, which offer services for searching certain NFT marketplaces on which digital items are bought and sold for potential trademark infringements.

As another option, a company may also watch the trademark register. Shockingly, bad faith actors are filing preemptive metaverse trademark applications. For example, recently bad faith trademark applications were filed for Prada and Gucci's trademarks for use in the metaverse.

Finally, customer engagement and reporting are other methods through which brands learn of misuse. Customers may encounter the trademark in the metaverse world and report it. The company may also learn about the infringement through their consumers' active engagement with a popular infringing use of their products and services.

Addressing infringements in the metaverse

The first line of protection in the metaverse is the mechanisms provided in the metaverse itself.

In centralized worlds, the owner offers terms of use or service that require compliance with intellectual property rights and also allows users to submit a report of IP infringement (e.g., Meta's Horizon Worlds) in a process that will be familiar to IP owners. In other centralized platforms, there are notice-and-takedown procedures in place. For example, under the Digital Millennium Copyright Act, copyright holders and their agents can notify a platform about material they believe infringes on their copyrights and can request a service provider remove this material. To comply with the requirements of the DMCA, the service provider must respond expeditiously to valid DMCA notices (e.g., Roblox).

DAOs vote on their own rules. However, the terms of use in decentralized metaverse rules generally include a provision requiring compliance with IP rights (e.g., Decentraland, Star Atlas, Sandbox).

Likewise, digital marketplaces, such as OpenSea, often provide mechanisms for removing infringing digital assets.

If takedown mechanisms are not effective, there are few options short of filing a lawsuit. In the U.S., trademark owners typically file infringement actions in federal district court. Case law still needs to develop that details how to enforce injunctions. Additionally, if a trademark is infringed in the metaverse while only being registered in a certain number of countries, there is no guidance discussing whether a company can enforce their trademark in a country where the user is located, but their trademark is unregistered. Because the metaverse is borderless, this poses complex jurisdictional issues that will likely continue to develop as the metaverse develops.

How have courts analyzed trademark infringement issues in connection with the metaverse?

Earlier last year, Hermès filed a trademark infringement suit against Los Angeles-based designer Mason Rothschild for creating and selling faux fur digital renditions of the luxury Hermès Birkin handbags and using a collection of 100 NFTs, called "MetaBirkins," to authenticate the digital images. In response, Rothschild filed a motion to dismiss Hermès' trademark infringement claim under the Rogers test on the basis that the digital images of the Birkin bags are "art" and therefore receive First Amendment protection. Rothschild argued for First Amendment protection under the Rogers test for his use of the Hermès' Birkin mark because he used "MetaBirkins" as the title of his artwork.

This case also raised issues related to whether NFTs used to authenticate digitally wearable clothing would raise First Amendment issues. In the initial stages of the lawsuit, the court found at the motion to dismiss stage that the digital MetaBirkins images could be interpreted as artwork and entitled to freedom of speech protection, and therefore the use of NFT authentication is irrelevant to the trademark infringement inquiry. However, the court proffered in a hypothetical scenario that such freedom of speech protection may not be similarly extended to certain artworks where the NFTs are used to authenticate digitally wearable clothing items for sale in the metaverse. This shows that courts may recognize digitally wearable clothing items (and other products and services) connected to NFTs as commodities, which provides more protection for companies seeking to expand their brands into the metaverse.

However, although the court recognized Rothschild's images could be interpreted as artwork under the First Amendment, Rothschild's argument did not ultimately succeed. On Feb. 8, 2023, a Manhattan federal jury found that Rothschild's "MetaBirkin" NFTs infringed and diluted the Hermès trademarks for its Birkin bags and that Rothschild cybersquatted on the 'metabirkins.com' domain name. Rothschild was ordered to pay $110,000 for trademark infringement and dilution and $23,000 in statutory damages for cybersquatting.

...even if your company has not expanded its products and services into the metaverse, if you expect that your brand may face infringement in the metaverse, a proactive trademark application is a low-cost tool to secure rights.

This verdict shows that virtual trademark infringement has consequences just as it would in the physical world. Although case law regarding trademark infringement in the metaverse will evolve as the technology itself evolves, for now, this verdict is promising for brand owners that are navigating and deciphering the early stages of the metaverse with their brands.

In 2021, the issue of trademark protection of NFTs had also arisen when Nike filed a lawsuit against an online reselling platform StockX. Nike alleged that StockX is 'minting' NFTs that prominently use Nike's trademarks. The minted NFTs in this suit contained images of Nike sneakers. StockX argued the NFTs were simply a channel for tracking ownership of Nike products in the real world sold on StockX's virtual marketplace, and that its NFTs are simply a method to track ownership of physical Nike products sold on the StockX marketplace and held in StockX's custody. While Nike argued that StockX's Nike-branded NFTs are themselves virtual products and not simply a representation of ownership of physical Nike sneakers.

This raises questions as to ownership of virtual assets, especially as companies begin to venture into the metaverse. For example, Nike argued the public already began conflating the parties' NFT offerings. In one instance, a commentator incorrectly reported that Nike NFTs debuted on StockX's platform and that users can buy NFTs supported by Nike when that was not the case. This case is expected to be a key development for metaverse jurisprudence because it may define the scope of trademark protection for infringing uses of a brand's marks in connection with their NFTs.

Additionally, Nike filed several applications for use of their famous trademarks in the metaverse. Although the metaverse was not explicitly discussed, if Nike expands into the metaverse (as it appears from its preemptive metaverse filings), Nike may have more protection for its NFT-authenticated products and services if case law progresses as it did in the MetaBirkin case.

How can you register your brand and design for metaverse-related goods and services?

In 2021, many companies preemptively applied for metaverse-related intent-to-use trademark applications in anticipation of expanding their products and services to the metaverse. Depending on the jurisdiction, a trademark application's requirements may vary. In the United States, an intent-to-use trademark application (1(b) basis) is one type of trademark application that a trademark applicant can file with the U.S. Patent and Trademark Office to register the trademark before using the mark in commerce. An intent-to-use trademark application in the U.S. will provide trademark protection for your brand's products and services even if your company has not expanded into the metaverse yet, but intends to. However, in order to ultimately secure trademark rights in the United States, the trademark owner must use the trademark on the registered goods.

In most jurisdictions, the first applicant to file the application will own rights in the trademark. Therefore, even if your company has not expanded its products and services into the metaverse, if you expect that your brand may face infringement in the metaverse, a proactive trademark application is a low-cost tool to secure rights.

The companies that have applied for metaverse-related trademark applications have registered their products and services in connection with "downloadable virtual goods" (class 9), "retail store services featuring virtual goods" (class 35), "entertainment services, namely providing on-line, non-downloadable virtual [products and services] for use in virtual environments" (class 41), "on-line non-downloadable virtual goods and NFTs" (class 42), and "financial services, including digital tokens" (class 36). For example, Nike filed a handful of its most famous marks for use in the metaverse. Nike filed several intent-to-use applications with the USPTO for its name, the swoosh logo, "JUST DO IT," and Jordan marks "for use in virtual environments" in connection with classes 9, 35, and 41.

However, in October 2021, USPTO examining attorney Barbara Rutland issued several office actions requesting Nike to clarify its timeline in connection with its "indefinite" identification of goods and services for use in the metaverse. The examining attorney requested that the application states the "precise nature of the goods and services is unclear" and that Nike should provide "clarifying wording" to overcome the rejection.

On the other hand, Converse also filed applications for use in the metaverse, and the USPTO approved publication of three of its metaverse trademark applications registered in early November 2021 without receiving any office actions. The description for Converse's applications for their mark and their All Star Chuck Taylor logo was more specific. For example, the description for one application for use in the metaverse recited "downloadable virtual goods, namely, computer programs featuring footwear, clothing, headwear, eyewear, bags, sports bags, backpacks, sports equipment, art, toys and accessories for use online and in online virtual worlds." Therefore, it is crucial to specify how exactly your company's products and services will be used in the metaverse.

Key considerations for brands expanding into the metaverse

The metaverse is a powerful digital platform with the potential to offer products and services for businesses, and many companies are staying ahead of the game as the metaverse and corresponding case law develop. Like brands, courts and trademark offices across the globe are attuned to these technological changes. In the upcoming years, we anticipate more case law development, trademark office guidance, and metaverse IP enforcement as the metaverse itself develops. Your brand can stay ahead of the game by applying for trademark applications in accordance with your jurisdiction's requirements. In the meantime, we'll see you in the metaverse.

Andrew Avsec
Partner, Chicago
Advertising and Brand Protection

Matteo Mariano
Associate, Brussels
Intellectual Property

Risa Rahman
Associate, Washington, D.C.
Advertising and Brand Protection

For more information, contact:

Preetha Chakrabarti
Partner
+1.212.895.4327 | pchakrabarti@crowell.com

Alexander Urbelis
Senior Counsel
+1.212.895.4254 | aurbelis@crowell.com

590 Madison Ave.
20th Floor
New York, NY 10022

To access an electronic version of this publication, go to crowell.com/metaverse.