

Key Privacy Issues To Consider Before Launching An NFT

By **Daniel Goldberg and Zachary Lewis** (June 10, 2022)

So, your brand is ready to launch an NFT collection, and you are moving through your due diligence checklist before greenlighting the drop.[1]

You've considered intellectual property, securities and various technical issues. Your marketing department assures you privacy isn't an issue because NFTs reside in Web3 where everything is open, decentralized and anonymous.[2]

Good to go? Well, not quite.

While NFTs offer the promise of Web3, most of the ecosystem — including the websites where NFTs are bought and sold and the platforms where NFT communities engage — still exists on Web 2.0. As a result, NFT drops rely on a Web 2.5 ecosystem — as we like to call it — where data collection and monetization rule and a plethora of privacy laws, rules and regulations apply.[3]

This article proposes that there are five steps in dropping an NFT collection, and examines the privacy and data protection issues brands must consider through each of these five steps.



Daniel Goldberg

Step 1: Generating Hype

Before dropping an NFT collection, or project, most brands try to build excitement around the drop. A brand typically starts by setting up a website and/or Discord server dedicated to the NFT drop.[4]

The brand then announces the NFT drop using Twitter, and often embeds a URL in its brand profile or tweets that links to the brand's Discord server and/or website.

This process of generating hype inherently involves the collection and processing of personal information. Tweets, comments, IP addresses and other device identifiers constitute or may include personal information under various privacy laws.

Tweets and comments are particularly identifiable, as they relate to specific user accounts. In addition, the URL itself may collect personal information.

As a rule of thumb, a brand is responsible for personal information it collects and processes, whether through its website, Twitter page or Discord server and beyond. In certain situations, a brand is also responsible — at least in part — for data collected and processed by its vendors.

A brand must evaluate its obligations under privacy law, including comprehensive state laws from California, Virginia, Colorado, Utah and now Connecticut.[5][6] Moreover, when using or collecting data through Twitter or Discord, a brand must comply with the relevant platform's terms, community guidelines and privacy policy.

In all instances, a brand must post a privacy policy — usually on its own website and made

Zachary Lewis

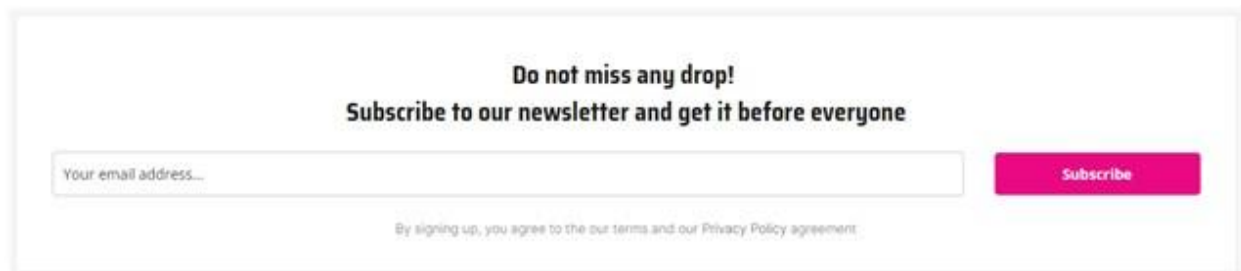
available through its Twitter page or Discord server — that discloses the brand's data practices and explains how users can exercise their data rights.

Where a brand uses its own website to promote an NFT collection, it should consider the functionality of the website. If a brand deploys cookies, pixels or other tracking technologies on the website — or in emails or ads for the website — including for purposes of analytics or targeted advertising, the brand must address privacy obligations relating to data collected through those tracking technologies.

Likewise, if a brand offers an email sign-up through the website, the brand must determine whether email addresses will be used solely for the purpose of sending email updates regarding the NFT project or for broader purposes such as creating hashed audiences for targeted advertising.

Hashed audiences and targeted advertising require additional disclosures and evaluation of user rights, including opt-outs under comprehensive state privacy laws.

Here's an example of an email sign-up on an NFT website:

A screenshot of an email sign-up form. At the top, the text "Do not miss any drop!" is displayed in bold. Below it, the text "Subscribe to our newsletter and get it before everyone" is also in bold. There is a text input field with the placeholder text "Your email address...". To the right of the input field is a pink button labeled "Subscribe". Below the input field and button, there is a small line of text: "By signing up, you agree to the our terms and our Privacy Policy agreement."

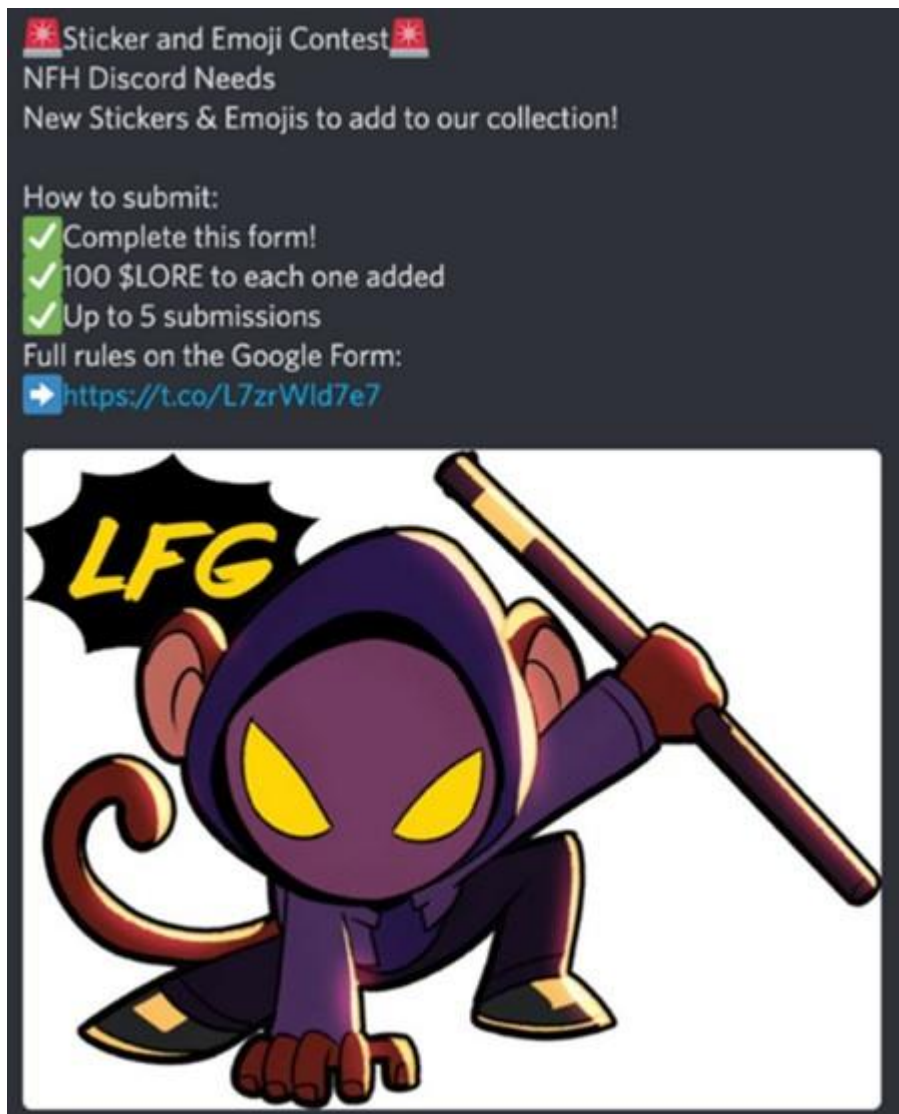
And, of course, if an NFT project is meant to be available or advertised worldwide, a brand must consider global data protection issues, including potential applicability of the European Union's General Data Protection Regulation and related data transfer obligations.[7]

Step 2: Developing a Discord Community

In conjunction with generating hype, brands frequently use Discord to develop a sense of community around their NFT project and engage with users. A brand may open text and voice channels to the public and converse with users on topics related — and unrelated — to the NFT project.

In addition to opening channels, a brand may organize game nights, art or meme contests, loyalty programs, sweepstakes or other events on Discord where, by participating, users can win NFTs, cryptocurrency or the opportunity to add their digital wallet address to a list — often referred to as a whitelist, guestlist or allowlist — granting early access to NFT minting.

Here's an example of a contest advertised on Discord where users must provide a digital wallet address to receive a digital asset prize:



As noted above, a brand is responsible for personal information it collects through its Discord server, and should familiarize itself with Discord's terms, community guidelines and privacy policy. A brand should consider what type of information it solicits from users and how it uses that information.

For example, if a brand processes sensitive information through Discord, like voice, such processing could violate certain biometric laws.[8] Further, if a brand asks users to participate in an event in return for early access to NFT minting or other prizes, the brand may risk triggering financial incentive opt in and disclosure obligations under California privacy law, which is an area of interest for California Attorney General Rob Bonta.[9]

Brands should be extra careful regarding the security of user data collected through Discord. We've heard of Discord moderators soliciting digital wallet addresses as part of an event, storing the addresses within a list on Google Forms or an unsecured spreadsheet, and posting the entire list to their Discord server to let users confirm whether they are on a whitelist.

As digital wallet addresses may constitute personal information under applicable law, posting these lists in the clear on Discord could constitute a security incident and trigger data breach obligations in certain jurisdictions.

Step 3: Setting Up and Maintaining a Digital Wallet

Next, in order to drop an NFT collection or receive any sale proceeds in cryptocurrency, a brand must either set up its own digital wallet or entrust a third party to manage its digital assets. As part of that process, the brand must decide who will open the wallet.

The brand should associate any custodial digital wallet that it opens with a brand account rather than an employee's own account, as the employee may have individual privacy rights under the law.

Importantly, a brand must consider how the wallet's private keys — i.e., the code to the safe — will be protected. While digital wallets are generally considered secure, a wallet is only as secure as the wallet's private keys, also known as a user's seed phrase, secret phrase or recovery phrase.

Any seed phrase stored online, on a computer or in an electronic password manager is susceptible to being stolen. Once a bad actor has access to a brand's seed phrase, it can transfer all the assets in the brand's digital wallet to a new wallet the brand doesn't control. The nature of blockchain technology makes these transactions irreversible.

Brands should be aware of the tactics used by bad actors to gain access to digital wallets. Most attackers rely on phishing schemes where the attacker gains access to an online account that ultimately leads them to a digital wallet. Discord, Twitter and Instagram are particularly vulnerable to attack.

We've seen many instances where an attacker gains access to an NFT issuer's Discord, Twitter or Instagram account tweets or posts an announcement through the account of a new NFT drop along with a malicious link and gains access to the private keys of those users who click on the link — whether through a vulnerability on the user's device or where the user provides their private keys as part of connecting their wallet to the attacker's website in the belief they will receive an NFT.[10][11][12]

We're also aware of at least one instance where an attacker gained access to an iCloud account and discovered the backup data included his seed phrase. These scams have resulted in wallet holders losing millions of dollars in assets, including cryptocurrency. Where a brand falls victim to an attack, the brand could face significant liability as well as damage to its goodwill.[13]


Here is what Bored Ape Yacht Club tweeted after its Instagram account was hacked on April 25, where the hacker allegedly stole nearly \$2.5 million worth of NFTs:



Bored Ape Yacht Club ✓

@BoredApeYC



 There is no mint going on today. It looks like BAYC Instagram was hacked. Do not mint anything, click links, or link your wallet to anything.

9:58 AM · Apr 25, 2022



9.1K



Reply



Share

Accordingly, brands must take appropriate measures to prevent and timely respond to such attacks. Even basic measures such as employee training and limiting access on a need-to-know basis help protect not only the brand, but also potential NFT purchasers who interact with the brand.

Step 4: Dropping the NFT Collection

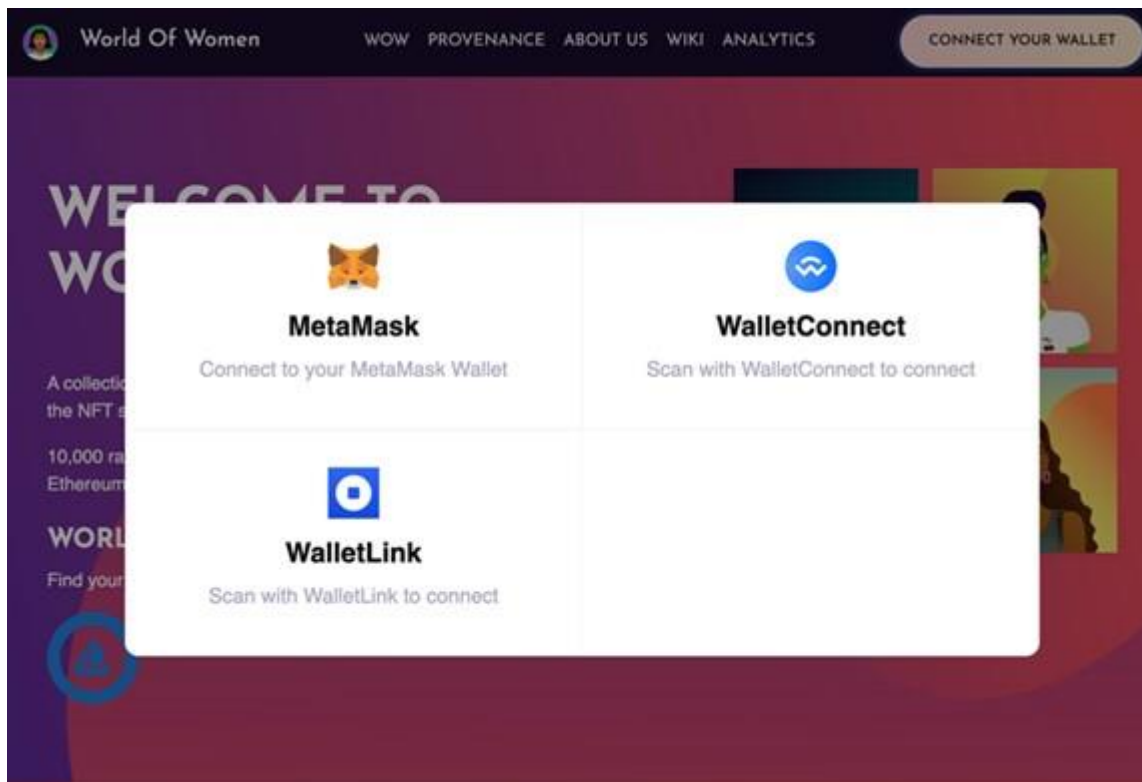
Once everything else is in place, a brand can proceed with dropping its NFT collection.

Most brands choose to sell NFTs through their own websites, often microsites or splash pages, which are designed to be compatible with MetaMask or similar third-party digital wallet extensions. We note that brands can alternatively drop their NFTs directly on marketplaces like OpenSea, which carries its own privacy considerations.

Users simply connect their digital wallets to the website for the opportunity to mint an NFT. When a user purchases a brand's NFT, a public entry is created on the applicable blockchain showing that a user's digital wallet address and the NFT collection's smart contract address — which typically points to the brand's digital wallet address as the deployer — sent cryptocurrency and NFTs to each other.

Brands are responsible for any personal information they collect during this process.

Here's an example of a website with digital wallet integration:



One of the touted benefits of digital wallets is that they are supposed to be anonymous. Each wallet has a unique, random and immutable public address that allows its user to receive cryptocurrencies.

Because these addresses are long strings of alphanumeric characters, some brands may believe that the addresses should not be able to identify a wallet holder, and therefore they do not need to consider privacy and data protection obligations. However, while a digital wallet address alone cannot identify a user, it could become identifiable and subject to privacy law by associating other pieces of information with it.

One possible way to identify the owner of a digital wallet address is through its transaction activity. Blockchains, which are distributed digital ledgers, store and publicly list all transactions and assets associated with each digital wallet and each NFT collection's smart contract address.

Unlike information stored using other technologies, these transaction histories cannot be deleted or modified. Through a quick search, a brand — and third parties — can view all of the transactions and assets associated with a digital wallet, or smart contract address, and find out:

- When the wallet was opened;
- What assets the wallet holds and has held;

- When assets were purchased and sold;
- From whom assets were purchased and to whom assets were sold; and
- Whether any blockchain-based domain names, i.e., customized wallet addresses, are associated with the wallet, e.g., janedoe.eth.

Here's an example of a scan through Etherscan.io showing some transaction activity of a digital wallet:

	0xf43a486d29a550a45e...	Claim Reward	14638440	7 days 21 hrs ago	0x804910a8f18337b106f...	OUT
	0xb9b13abf20dfc92eaf4...	Transfer	14584150	16 days 8 hrs ago	0x804910a8f18337b106f...	OUT
	0x422fe1460973ef0bb84...	Transfer	14292173	61 days 20 hrs ago	Coinbase 4	IN
	0xac1613e5dee9643d1e...	Transfer	13967495	112 days 1 hr ago	0x804910a8f18337b106f...	OUT

Knowing several pieces of transaction activity, or even a single piece of transaction activity associated with outside information, could quickly make a digital wallet address identifiable to a brand.

For example, as recently demonstrated by Jimmy Fallon, a digital wallet address could become identifiable where a brand knows that the digital wallet holds a specific NFT and the brand interacts with a user on Twitter, Discord or LinkedIn using that NFT as an avatar or profile picture.[14]



A digital wallet address could also become identifiable where a brand knows that the digital wallet holds a Proof of Attendance Protocol NFT, which certifies the holder attended a specific event, and the brand also has a list of those individuals who attended that event.

In addition, a digital wallet address could become identifiable based on associating the address with data collected through a brand's website. For example, a brand could collect the IP address of a user who visits the brand's website and associate the IP address with a digital wallet address based on the time of a purchase.

More directly, a brand could require a user to register an account in order to make a purchase and associate the account information with a digital wallet address. Brands that are particularly mindful of anti-money laundering and know-your-customer requirements have even required digital wallet owners to submit personal information such as photos of government-issued IDs to purchase NFTs or use NFTs in their wallet to redeem physical assets.

Based on the above, regulators could consider digital wallet addresses to be personal information under privacy law and expect brands to treat them as such. This has yet to be tested in most jurisdictions. This means brands must provide disclosures and rights around digital wallet addresses, even if the brand cannot delete the immutable information from the blockchain.

We expect some brands may argue that digital wallet addresses are publicly available information and thus exempt from the definition of personal information in certain jurisdictions. However, brands should be careful when relying on this argument.

Even if a digital wallet address itself is publicly available information, if a brand associates a digital wallet address with other information, the resulting combined information could be considered personal information. Earlier this year, Bonta issued an opinion that inferences generated based on publicly available information are subject to the protections under California privacy law.[15]

Step 5: Post-Drop Utility

After a drop, a brand may continue to engage with its users and offer additional utility for NFT holders. For example, a brand may give NFT holders the ability to redeem physical goods or exclusive merchandise, attend invite-only events or meetups, or download or access exclusive content.[16]

To the extent these practices involve the collection or processing of personal information, a brand must continue to evaluate its obligations with respect to such processing.

Final Thoughts

There is a lot to consider when dropping an NFT collection, and privacy and data protection compliance should be a chief consideration. Failure to address privacy and data protection could lead to regulatory scrutiny and enforcement, damage to consumer trust and goodwill, and loss of valuable assets and revenue.

As we move closer to Web3, best practices and laws will evolve, and brands will need to stay up to date and nimble to address their obligations.

Now, the next time your marketing department assures you privacy isn't an issue, you'll be ready to kindly respond that it is.

Daniel M. Goldberg is chair of the privacy and data security group and Zachary Lewis is an associate at Frankfurt Kurnit Klein & Selz PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, 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.

[1] <https://ipandmedialaw.fkks.com/post/102gt4b/a-primer-on-nfts-and-intellectual-property>.

- [2] <https://www.investopedia.com/web-20-web-30-5208698>.
- [3] <https://www.investopedia.com/web-20-web-30-5208698#:~:text=Web%202.0%20is%20the%20current%20version%20of%20the%20web%20with,exponential%20growth%20of%20Web%202.0>.
- [4] <https://advertisinglaw.fkks.com/post/102h4l7/time-to-learn-about-discord-where-social-media-and-the-metaverse-collide>.
- [5] <https://advertisinglaw.fkks.com/post/102hk2a/utah-set-to-join-california-virginia-and-colorado-with-comprehensive-state-priv>.
- [6] <https://advertisinglaw.fkks.com/post/102hnm1/connecticuts-sb-6-poised-to-become-fifth-u-s-comprehensive-privacy-law>.
- [7] <https://advertisinglaw.fkks.com/post/102h7qk/a-new-standard-in-standard-contractual-clauses>.
- [8] <https://advertisinglaw.fkks.com/post/102haa6/facebook-stops-use-of-facial-recognition-technology-amid-risk-of-increased-enforc>.
- [9] <https://advertisinglaw.fkks.com/post/102hhmw/california-attorney-general-warning-letters-provide-insight-into-ccpa-enforcement>.
- [10] <https://indianexpress.com/article/technology/crypto/heres-how-a-hacker-stole-800000-worth-nfts-through-discord-7826954/>.
- [11] <https://www.benzinga.com/markets/cryptocurrency/22/03/26404067/bored-apes-other-nfts-are-stolen-in-major-twitter-phishing-hack>.
- [12] <https://www.coindesk.com/tech/2022/04/25/at-least-13m-in-nfts-stolen-after-bored-ape-yacht-club-instagram-discord-hacked/>.
- [13] <https://screenrant.com/apple-icloud-crypto-scam-seed-phrase-650k/>.
- [14] <https://news.knowyourmeme.com/news/crypto-wallet-supposedly-belonging-to-jimmy-fallon-bought-trump-nft-and-lets-go-brandon-crypto-coins>.
- [15] <https://advertisinglaw.fkks.com/post/102hkl7/california-ag-issues-written-opinion-on-internally-generated-inferences>.
- [16] <https://www.theverge.com/22824387/bored-ape-yacht-club-nft-party-new-york>.