UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
(West Palm Beach Division)

CASE NO.:

NEAL MAGENHEIM and ANGELA NEIL,
on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

NIKE, INC., *an Oregon corporation*,

Defendant.
_____/

CLASS ACTION COMPLAINT

Plaintiffs, NEAL MAGENHEIM and ANGELA NEIL (collectively, the "Plaintiffs"), brings this class action lawsuit against Defendant, NIKE, INC. ("Defendant"), on behalf of themselves, and all others similarly situated, and allege:

NATURE OF THE ACTION

1. This case involves a pressing problem. Americans cannot maintain privacy when large corporations, data brokers, and marketers are incessantly invading private web browsers located on private computers, without consent, to harvest personal data, which is then used to surveil, track, target, and pester people online, on social media, and on streaming television ads. The extent of this problem is so large that a billion-dollar industry known as *identity resolution* has come into existence, the sole purpose of which is to maintain files and information on every American, based on data taken from personal computers, often secretly, and selling that data to the highest commercial bidder.

2. This pervasive assault on privacy is notwithstanding that most Americans expect to remain *anonymous* online unless they intentionally provide identifying information. A recent study found that eighty six percent (86%) of Americans expect to be anonymous online and actively take steps to avoid being identified and spied upon.[1] Ninety percent (90%) of Americans believe they should have a say in whether their information is shared online.[2] Nevertheless, using its website, this Defendant causes invasive computer software to be surreptitiously installed on unsuspecting web browsers, which then captures personal data, and shares it with third parties for commercial benefit.

3. Specifically, as soon as a visitor lands on www.nike.com (the "Website"), Defendant triggers the installation of software on that visitor's web browser without permission. Defendant does not seek consent *prior to* installing software on each visitor's web browser (as many others do, as by using "cookie consent banners"). This is true even where a visitor has enabled its web browser's Global Privacy Control indicator ("GPC Flag"), which notifies Defendant that the visitor does not agree to installation of invasive code on its web browser.[3]

4. Defendant makes a further mockery of legal compliance by including a small link at the bottom of its website entitled "your privacy choices," which, when selected, allows users to feel that they are withholding consent for Defendant to share visitor data with third parties. But incredibly, even when a user somehow makes it to that obscure page, and specifically withholds permission for Defendant to share data with others (by which time Defendant has already violated

[1] https://www.pewresearch.org/internet/2013/09/05/part-1-the-quest-for-anonymity-online.

[2] https://www.odwyerpr.com/story/public/11834/2019-01-04/online-privacy-becomes-top-concern-2019.html

[3] A Global Privacy Control (GPC) flag is a setting in a web browser that automatically sends a universal signal to websites, telling them that the owner of the web browser is opting out of the sale or sharing of its personal information. This single, global signal is designed to simplify the process of exercising privacy rights by automatically declining the installation of code on the web browser from the moment the visitor lands on the webpage.

the law by triggering the installation of invasive code unlawfully), Defendant ***still deploys*** the software onto the visitor's website – which the visitor overtly instructed Defendant not to do.

5. As set forth below, Defendant's intrusions onto its visitors' private computer systems, without consent – and despite explicit requests for privacy from such intrusions – constitute a violation of Florida law, entitling Plaintiffs, and a class of similarly situated persons, to appropriate relief.

PARTIES

6. At all times material hereto, Plaintiff, ANGELA NEIL, was and is a citizen and resident of Palm Beach County, Florida.

7. At all times material hereto, Plaintiff, NEAL MAGENHEIM, was and is a citizen and resident of St. Lucie County, Florida.

8. Plaintiffs bring this action on behalf of themselves, and on behalf of all other similarly situated individuals.

9. At all times material hereto, Defendant, NIKE, INC., was and is an Oregon corporation, which is registered to do business, and doing business, in Palm Beach County, Florida.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative class members.

11. The Court has personal jurisdiction over Defendant in this action pursuant to 18 U.S.C. §1965, the Due Process Clause of the U.S. Constitution, and the Florida long-arm statute, §48.193, Florida Statutes, because Defendant's Website is usable and viewable by consumers located inside Florida, who order and pay for products through the Website from within Florida,

and who make financial payments to Defendant for its products from within Florida, which products are then delivered by Defendant to consumers inside Florida. Defendant has made and is making sales through the Website to customers located in Florida and/or has shipped products purchased through its Website to its Florida customers.

12. Furthermore, Defendant used the Website to install certain software (as explained in full below) on web browsers inside Florida, without consent, thus subjecting Florida citizens to unlawful intrusions, privacy violations, and surveillance, within Florida.

13. Finally, Defendant is registered with the Florida Secretary of State to do business in Florida, and maintains a registered agent in Florida, whose address is 801 US Highway 1, in North Palm Beach, Florida, which is located within this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because the Defendant has a registered agent in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTS

15. When a user visits any website, code from the landing web page instructs the browser to download resources required to render and interact with the page. These resources include images, HTML, JavaScript, Cascading Style Sheets (CSS), and other file types. When a resource is downloaded from a remote server, the browser transmits identifying information as part of the request via HTTP headers or the request URL (Uniform Resource Locator). This information includes:

a. **Cookies**: Small text name/value pairs stored on the device tied to a specific domain, subdomain, or folder of a website. They can uniquely identify users across sessions and domains, and multiple cookies may be set during a single visit.

b. **User-Agent**: A string allowing servers and network peers to identify the application, operating system, vendor, and/or version of the requesting user agent.

c. **IP Address**: The publicly routable IP/port from which the TCP (HTTP/1.1, HTTP/2) or QUIC (HTTP/3) connection originates (more about IP addresses below).

d. **HTTP Protocol Version**: The version number, such as HTTP/1.1, HTTP/2, or HTTP/3 indicates which specific set of rules and features is being used for a request and determines how data is processed.

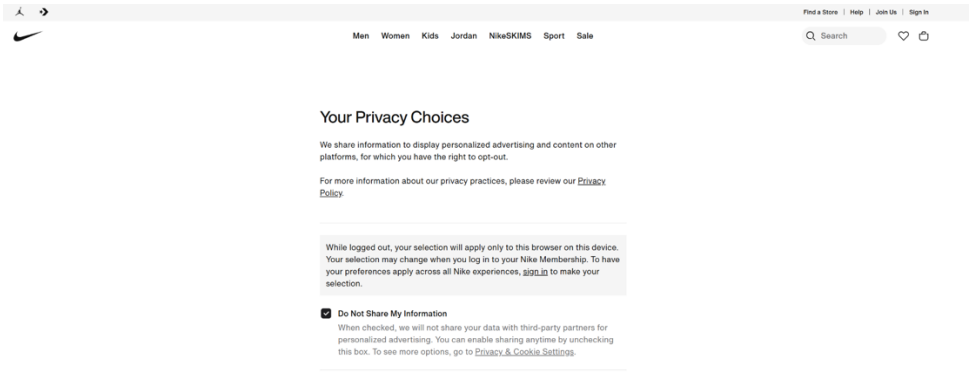
e. **Data Payload**: Any data specifically passed as part of the request.

f. **Origin URL**: The URL from which the resource is being requested.

16. When visiting www.nike.com, the code loaded from the Website instructs the visiting web browser to download resources required to render the page. These resources include elements linked to user tracking technologies that execute and collect data about a user. This occurs regardless of whether or not the user has opted out by initiating a GPC Flag (the JavaScript variable navigator.globalPrivacyControl, which can be read by the web page when the browser first visits) or via the custom "Do not share my personal information" selector located at https://www.nike.com/guest/settings/do-not-share-my-data.

17. In other words, the moment a visitor lands on the Website, Defendant instructs the visitor's web browser to download technologies that collect visitor data beyond what is necessary to utilize the Website, that share visitor data with third parties, and that can be used to track the visitor after they leave the Website – and moreover, Defendant does this *even if* the GPC Flag has instructed it not to do so, and *even if* the visitor has deselected all sharing permissions on the Website itself.

18. For example, Defendant provides an obscure corner of its Website in which a visitor can request that the Website not share their information with third parties:



19. This custom selector clearly states that "When checked, we will not share your data with third-party partners for personalized advertising. You can enable sharing anytime by unchecking this box." Furthermore, Defendant's Privacy Policy reiterates this promise, telling visitors, *inter alia*, that "You may opt-out of cross-context behavioral advertising or targeted advertising by using the relevant settings available in our Platform."

20. These promises are both belated and false. They are belated, because by the time any visitor makes it to Defendant's Privacy Policy or its privacy selector page, Defendant has already prompted the installation of software onto the visitor's personal web browser and begun sharing private data from the visitor's web browser with third parties. This is true even for those visitors who have their GPC Flag enabled and have thus notified Defendant of their privacy preferences from the moment the Website first loads. The promises are also false, because privacy selections made on the Website are not respected, and neither is a visitor's GPC Flag, all of which put Defendant on actual notice of privacy preferences, which Defendant simply ignores.

21. More specifically, upon visiting the Website, the following user tracking technologies execute and collect data by sending network requests to third party endpoints. This

takes place every time, *irrespective* of whether a GPC Flag is enabled, and continues *irrespective* of whether the visitor opts out of information sharing on the Website itself:

22. The Trade Desk: The Trade Desk (TDD) (https://www.thetradedesk.com) is a technology company that provides a self-service, cloud-based platform for advertising buyers to manage and optimize digital ad campaigns. Its platform, a Demand-Side Platform (DSP), allows marketers to use data-driven insights to plan, forecast, and purchase ads across various formats and devices, such as display, video, and connected TV. The company specializes in automated, data-driven programmatic advertising, which uses technology to buy and sell digital ad space in real-time auctions. When the Website is visited, it forces the user browser to make the following network requests to resource servers managed by The Trade Desk:

Network Request URL[4]	https://js.adsrvr.org/up_loader.1.1.0.js
Purpose[5]	Base Code
Example Data Payload Passed to TDD[6]	N/A
Hard Coded in HTML or Dynamically Loaded [7]	Dynamically Loaded

[4] Network Request URL refers to the URL of the request sent from the user's browser to a remote server. The URL may retrieve a remote resource to load the page and may contain user information intentionally collected by trackers.

[5] The purpose of the download, which can include **iFrame** (an embedded HTML document that can load further resources and pass along browser and user data); **Base Code** (remote code that enables functions including gathering web browser data or user information and can initiate a network request to transmit that data); or **Data Collection** (a request designed to transmit browser or user information for tracking or behavioral recording).

[6] An example payload passed with the request if the request uses the POST method to send data instead of GET.

[7] Indicates how the browser was instructed to make the network request. Options include:

- Hard Coded: The resource was hard-coded into the raw HTML of the web page.
- Dynamically loaded: The resource was loaded by another resource that was either hard coded or dynamically loaded on the page. One way this can occur is through a Tag Management System (TMS). A TMS is a centralized tool that allows a website or app owner to manage tags (small pieces of JavaScript code) from a single interface without needing to change the site's underlying code. By implementing a single "container" tag, the team responsible for tag management can add, update, and deploy various marketing and analytics

Originator of Network Request [8]	https://www.googletagmanager.com/gtm.js?id=GTM-NTF2X45&l =marketingClientDataLayer (Google Tag Manager)

Network Request URL	https://insight.adsrvr.org/track/cei?advertiser_id=fcx45do&cookie_sync=1&upv=3.0.0&upid=sseyzi1&ref=https://www.nike.com/
Purpose	iFrame
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://js.adsrvr.org/up_loader.1.1.0.js

Network Request URL	https://js.adsrvr.org/universal_pixel.js
Purpose	Base Code
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://insight.adsrvr.org/track/cei?advertiser_id=fcx45do&cookie_sync=1&upv=3.0.0&upid=sseyzi1&ref=https://www.nike.com/

Network Request URL	https://insight.adsrvr.org/track/realtimeconversion
Purpose	Data Collection
Example Data Payload Passed to TDD	{"data":[{"adv":"fcx45do","pixel_ids":["sseyzi1"],"referrer_url":"https://www.nike.com/", "dpop":"LDU","data_processing_option":null,"privacy_settings":[]}]}
Hard Coded in HTML or	Dynamically Loaded

tags (such as Google Analytics or advertising platforms) through the TMS. This provides a single source for defining behaviors (like page views or clicks) and sending data to multiple platforms, giving better control over data collection and a faster way to make updates.

[8] The specific line number or dynamic resource that invoked the network request.

Dynamically Loaded	
Originator of Network Request	https://js.adsrvr.org/universal_pixel.js

23. Google AdSense: Google AdSense is a product from Google used for ad delivery, analytics, and content. When the Website is visited, it forces the user browser to make the following network requests to resource servers managed by Google AdSense:

Network Request URL	https://pagead2.googlesyndication.com/ccm/collect?frm=0&en=page_view&dl=https%3A%2F%2Fwww.nike.com%2F&scrsrc=www.googletagmanager.com&rnd=829262182.1763069829&navt=r&npa=1&gtm=45He5bc0v831367757za200zd831367757xea&gcs=G100&gcd=13q3q3q3q5l1&dma_cps=-&dma=0&tag_exp=101509157~103116026~103200004~103233427~104527907~104528501~104684208~104684211~115583767~115616986~115938466~115938468~116217636~116217638&tft=1763069828563&tfd=4760&apve=1&apvf=f
Purpose	Data Collection
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://www.googletagmanager.com/gtm.js?id=GTM-NTF2X45&l=marketingClientDataLayer (Google Tag Manager)

Network Request URL	https://ade.googlesyndication.com/ddm/activity/src=4171764;type=category;cat=pdppages;ord=6991197175744;npa=1;u1=us;u2=en_us;u3=homepage;u4=%2F;u5=0;u6=;u8=en_us;u10=;u11=;u12=0;u13=0;u14=usd;u15=;u17=https%3A%2F%2Fwww.nike.com%2F;u23=;u24=;u25=us;u26=usd;u27=0;u28=Desktop;u29=0;u33=;u34=;u35=false;u36=en_us;u37=usd;u38=N;u40=;u41=0;u42=;u43=0;u44=;u45=;u48=0;u49=0;u50=N;u51=0;u52=null;u53=;u54=;u55=;u56=0;u58=0;u59=0;u60=https%3A%2F%2Fwww.nike.com%2F;u61=N;uaa=x86;uab=64;uafvl=Chromium%3B142.0.7444.162%7CGoogle%2520Chrome%3B142.0.7444.162%7CNot_A%2520Brand%3B99.0.0.0;uamb=0;uam=;uap=Windows;uapv=19.0.0;uaw=0;pscdl=denied;frm=0;_tu=KFA;gtm=45fe5bc0v9190996969z8831367757za200zb831367757zd831367757xea;gcs=G100;gcd=13q3q3q3q5l1;dma_cps=-;dma=0;dc_fmt=8;tag_exp=

	101509157~103233427~104527907~104528500~104684208~104684211~105446120~115583767~115938466~115938468~116217636~116217638;epver=2;~oref=https%3A%2F%2Fwww.nike.com%2F?
Purpose	Data Collection
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://www.googletagmanager.com/gtag/destination?id=DC-4171764&l=marketingClientDataLayer&cx=c&gtm=4e5bc0 (Google Tag Manager)

24. PubMatic: PubMatic is a digital advertising technology company that provides a supply-side platform (SSP) to help publishers monetize their content. PubMatic's platform facilitates real-time programmatic ad transactions, connecting publishers with advertisers and enabling them to maximize ad revenue across various formats like websites, apps, and connected TV (CTV). When the Website is visited, it forces the user browser to make the following network requests to resource servers managed by PubMatic:

Network Request URL	https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTI4NDkmdGw9MTI5NjAw&gdpr=0&gdpr_consent=&piggybackCookie=63a311be-19cd-48cb-b532-9435c6d228c3&r=https%3A%2F%2Fmatch.adsrvr.org%2Ftrack%2Fcmf%2Fgeneric%3Fttd_pid%3Dpubmatic
Purpose	Data Collection
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://insight.adsrvr.org/track/cei?advertiser_id=fcx45do&cookie_sync=1&upv=3.0.0&upid=sseyzi1&ref=https://www.nike.com/

25. Index Exchange (formally Casale Media): Index Exchange is a programmatic advertising company that connects media owners and marketers to buy and sell digital ad space.

When the Website is visited, it forces the user browser to make the following network requests to resource servers managed by Index Exchange:

Network Request URL	https://dsum-sec.casalemedia.com/rum?cm_dsp_id=39&external_user_id=63a311be-19cd-48cb-b532-9435c6d228c3&expiration=1765662749&gdpr=0&gdpr_consent=
Purpose	Data Collection
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://insight.adsrvr.org/track/cei?advertiser_id=fcx45do&cookie_sync=1&upv=3.0.0&upid=sseyzi1&ref=https://www.nike.com/

26. BidSwitch: BidSwitch is a technology company that provides a centralized middleware platform to connect supply-side platforms (SSPs) and demand-side platforms (DSPs) in the digital advertising ecosystem. When the Website is visited, it forces the user browser to make the following network requests to resource servers managed by BidSwitch:

Network Request URL	https://x.bidswitch.net/syncd?dsp_id=93&user_group=1&user_id=63a311be-19cd-48cb-b532-9435c6d228c3&expires=30&redir=https%3A%2F%2Fmatch.adsrvr.org%2Ftrack%2Fcmf%2Fgeneric%3Fttd_pid%3Dbidswitch
Purpose	Data Collection
Example Data Payload Passed to TDD	N/A
Hard Coded in HTML or Dynamically Loaded	Dynamically Loaded
Originator of Network Request	https://insight.adsrvr.org/track/cei?advertiser_id=fcx45do&cookie_sync=1&upv=3.0.0&upid=sseyzi1&ref=https://www.nike.com/

27. Because the Website prompts the download of these invasive items onto each visitor's private web browser, each visitor is secretly identified, surveilled, and commodified. A person may visit the Website and then move on to a different website or to social media. But now,

ads for Nike might be everywhere. They're on news websites, in the social media feed, and everywhere else the targeted visitor goes online. Moreover, the "file" on the visitor, kept by identity resolution companies, has been supplemented with additional data points needed to build the visitor's digital profile.

28. This happens because the Website invades the visitor's web browser, making the visitor's private browser, and private browsing, an open book to all the marketing companies named above. In this way, the software that Defendant installs on visitor web browsers acts as a spyware, decoding the user's identity through their IP address, implanting surveillance processes on the visitor's web browser, and following the visitor around the internet to serve ads or gather information – or sometimes, to simply observe and surveil browsing habits, often for years.

29. This conduct is deeply offensive and invasive of basic Florida privacy and property rights. Even just by simply collecting electronic addressing and routing information in the form of a visitor's IP address, Defendant's advertising agents can discern significant personal identifying data and information. An IP address is a unique identifier, expressed as four sets of three numbers (i.e. 123.456.789.012). The first six numbers reveal the network used by the website visitor, and the second six numbers reveal the device used by the visitor. Knowledge of the visitor's IP address, standing alone, can reveal a range of PII, and is the first step in an unagreed digital fingerprinting process that Defendant is facilitating; for example, as explained by the Canadian Government, capturing the IP address of a website visitor allows the holder of that information to:

a. Perform a reverse lookup (the resolution of an IP address to its associated domain name) to obtain a computer name, which can lead to physical location information;

b. Conduct a traceroute (a computer diagnostic tool for displaying the route (path) of packets across an IP network) to find the logical path to the computer, which can reveal the physical location of the computer;

c. Determine the geolocation of the computer, with varying degrees of accuracy. Depending on the lookup tool used, this could include country, region/state, city, latitude/longitude, telephone area code and a location-specific map;

d. Search the Internet using the IP address or computer names. The results of these searches might reveal peer-to-peer (P2P) activities (e.g., file sharing), records in web server log files, or glimpses of the individual's web activities (e.g., Wikipedia edits). These bits of individuals' online history may reveal their political inclinations, state of health, sexuality, religious sentiments and a range of other personal characteristics, preoccupations and individual interests;

e. Seek information on any e-mail addresses used from a particular IP address which, in turn, could be the subject of further requests for subscriber information;

f. Reveal organizational affiliations or organization to which the address is assigned, including a name, phone number, and physical address.[9]

30. But of course, collection of visitor IP addresses only scratches the surface here. Intercepted IP addresses are paired with other data intercepted by the actors identified above to further expand upon a website user's digital fingerprint, and to share that data with other websites, and data aggregators, who monetize it. Indeed, multiple data points are used to create a profile of each visitor, which gives websites (and anyone willing to pay for PII), a detailed overview of visitor search history, browsing activity, and frequently visited pages.

[9] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/#fn5-rf (last accessed July 24, 2025).

31. Treating a visitor's private web browser as if it were the personal property of Defendant and its marketers allows these parties to intercept and surveil internet search history, browsing patterns, and data inputs, creating a powerful and financially valuable digital fingerprint and has given rise to a multi-billion-dollar digital surveillance industry targeting all Americans, known as the *identity resolution* industry.

32. As one identity resolution platform explains on its website, identity resolution

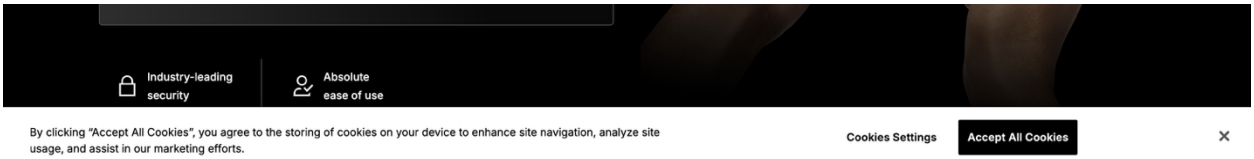
> is the process of accurately and consistently identifying individual customers across various touchpoints and channels . . . Imagine a scenario where a customer interacts with your brand through various channels—website visits, social media engagements, and email sign-ups. Without customer identity resolution, each interaction might create a separate profile for that customer in your database . . . With customer identity resolution, these disparate profiles are identified, merged, and streamlined into one comprehensive profile. For example, let's say a customer browses your website anonymously, adds items to their cart, and then later signs up for your newsletter. Without identity resolution, you might treat these interactions as separate events, missing the opportunity to understand the customer's behavior holistically.[10]

33. The data of all American internet users is now intercepted, stolen, and harvested across the internet, centralized, mined, and de-anonymized for commercial purposes, all with the help of the processes described above, which Defendant implements without consent (and despite affirmative lack of consent). The information used by individual companies and marketers, and by the identity resolution industry, to accomplish these tasks, is electronic addressing, routing, signaling, and other data, which exists on private personal computers, and private web browsers, and can only be accessed by intruding upon those devices.

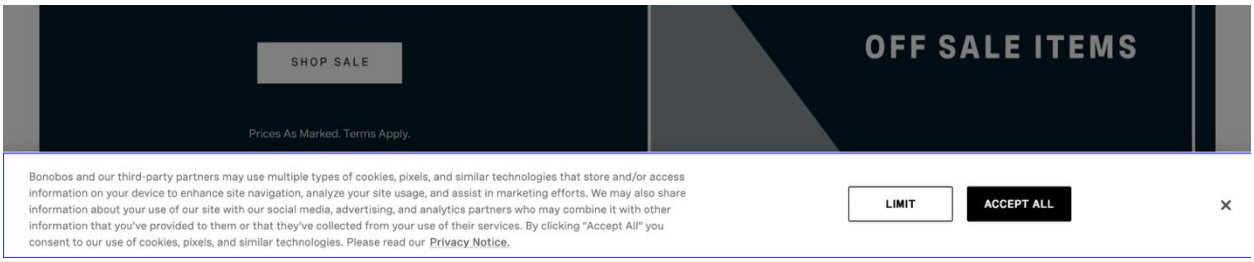
34. Of course, obtaining this information *legally* is easy enough. Websites need only disclose their intent to cause installation of invasive software on a visitor's web browser *before*

[10] https://www.salesforce.com/marketing/data/customer-identity-resolution/#what-is (accessed July 24, 2025).

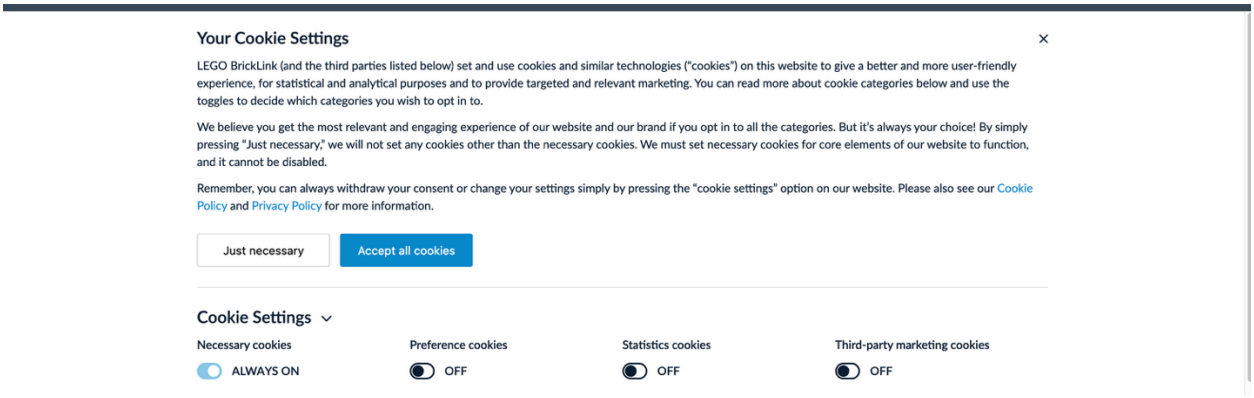
doing so and must respect visitor's privacy choices (such as GPC Flags). Consent requests will look familiar to all internet users and come in many varieties; requests can be simple:



35. Or requests can be detailed:



36. Or requests can provide a full array of consent options and information:



37. Whether a website operator chooses a simple or detailed consent form, some form of consent must be obtained before downloading software onto a private web browser to obtain personal data and to monitor otherwise private movements across the internet for commercial purposes. And yet, this Defendant has failed and refused to deploy even a free consent banner, which would advise its visitors that it is capturing their electronic data and usurping their web browsers *before* engaging in such activity.

38. Worse still, in addition to failing to obtain consent prior to violating the privacy and property of its own online visitors – including those who come with a GPC Flag engaged – Defendant created a small link at the bottom of the Website entitled "your privacy choices," which is a sham or ruse intended to deceive its visitors (those few who manage to navigate to that obscure webpage) by asking them to make privacy choices, which the Website disregards. This is a violation of the Website's own stated privacy policies, which specifically state that visitor opt-outs are respected by Defendant – but they are not; as such, Defendant violates its own privacy policies.

39. Why would Defendant engage in such behavior? Likely because, while it is easy to follow common-sense – and common decency – electronic privacy requirements, it is far more profitable to ignore privacy and invade personal electronic property. Indeed, when true consent is sought and respected, some considerable number of Website visitors will surely withhold that consent, thus depriving Defendant, its marketing partners, and the ever-expanding identity resolution industry, of key data points needed to create an exploitable digital fingerprint for every Website user, thus cutting into Defendant's profits. For this Defendant, the information gleaned from usurping private web browsers and invading online privacy may simply be too valuable to worry about or respect consent.

40. Indeed, the software that Defendant causes to be installed on visitors' web browsers is of significant monetary value to Defendant, to online marketers associated with Defendant, and to the *identity resolution* industry. For example, identity resolution (or customer relationship manager – CRM) platforms make up 23% of the global digital marketing software industry, whose total value is over $75 Billion today, and estimated to reach over $320 Billion by 2033; this value is created by surveilling "customer interactions across multiple touchpoints, email, social media,

web, and mobile" and is "indispensable for creating cohesive and effective marketing campaigns."[11]

41. In addition to profit generated by the identity resolution industry, individual ecommerce sites like Defendant profit by capturing visitor data and prompting installation of software from third party marketers. These mechanisms allow websites to optimize the way visitors interact with their website, trace and target their visitors across other websites and platforms, build a profile of visitor interests and preferences, and undertake enumerable other for-profit activities related to surveilling visitors' private web browsers.

42. Plaintiffs, and all similarly situated persons, have a reasonable expectation *that their own web browsers on their own computers* are private, and that Defendant has not invaded and destroyed that privacy by secretly causing installation of software on their web browsers, to ascertain, intercept, and gather otherwise private and personal information, and to transmit that information to others. Nevertheless, this is exactly what this Defendant does, entitling these Plaintiffs and the Class to all remedies permitted by law.

CLASS ALLEGATIONS

43. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiffs assert claims on behalf of all similarly situated persons, as follows:

> All persons who accessed the Website from within Florida during the two-year period preceding the filing of this action (the "Class").

44. Excluded from the Class is any of Defendants' officers, directors, and board members; all persons who make a timely election to be excluded from the Class; and the judges to whom this case is assigned and their immediate family.

[11] https://www.grandviewresearch.com/industry-analysis/digital-marketing-software-dms-market#:~:text=The%20global%20digital%20marketing%20software%20market%20size,platforms%20for%20customer%20engagement%20and%20revenue%20generation.

45. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

46. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

47. Numerosity. Fed. R. Civ. P. 23(a)(1). Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, Plaintiffs very conservatively estimates that the proposed Class is comprised of hundreds of thousands of members.[12] Class members may be identified through objective means; Defendant's analytic cookies log the IP address of every visitor, and Florida IP addresses that visited the Website over the past two years can be gathered from that log. Class members may thus be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notices.

48. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Plaintiffs and the Class were all subject to the same violation of their personal computer systems and private web browsers, and each is entitled to damages in the same amount, as set forth in more detail below.

49. Typicality. Fed. R. Civ. P. 23(a)(3). Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of the other Class members. Plaintiffs' damages and injuries are identical to the other Class members, and Plaintiffs seek relief consistent with the relief to which every other member of the Class is entitled.

[12] According to multiple online sources that keep such statistics, the Website has approximately 100 million visitors per month. Florida has approximately 7% of the U.S. population. Accordingly, at this time, Plaintiffs conservatively posits that the Class is comprised of hundreds of thousands of members, but discovery may reveal the number to be significantly larger than that.

50. Adequacy. Fed. R. Civ. P. 23(a)(4). Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are member of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflict of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including consumer class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

51. Superiority. Fed. R. Civ. P. 23(b)(3). Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Here, the damages suffered by Plaintiffs and the other members of the Class are relatively small amounts, but require evidence of a technical nature to pursue, and are far more efficiently pursued by a collective action than piecemeal over hundreds of thousands (or more) individual cases.

52. Plaintiffs will adequately and fairly represent the interests of the Class and has retained counsel experienced in class action litigation. Plaintiffs have no interests that are contrary to or in conflict with the interests of the members of the Class that he seeks to represent.

53. Common questions of fact and law exist as to all members of the Class and predominate over questions solely affecting any individual member of the Class; examples of the questions of law and fact applicable to all members of the Class are:

a. Whether Defendant has violated Florida law by failing to ask prior consent before using its Website to trigger download of third-party software onto private visitor computers;

b. Whether Defendant has violated Florida law by failing to ask prior consent before triggering download of third-party software onto private visitor computers;

54. Finally, all members of the proposed Class are readily ascertainable by records maintained by Defendant. Defendant has captured PII, including IP addresses, of all members of the Class who visited the Website during the applicable statute of limitations periods. This data can be used to ascertain every single member of the Class.

COUNT I
INVASION OF PRIVACY

Plaintiffs and the Class re-allege and incorporate Paragraphs 1 through 54 above, as though fully set forth herein.

55. As set forth in detail above, when Plaintiffs and each member of the Class landed on the Website, Defendant immediately caused software to be downloaded onto each person's private web browser, which was located on a personal computer. This took place the moment a visitor landed on the Website, prior to any opportunity to review or consent to any Privacy Policy, and prior to any opportunity to make selections on the privacy selector.

56. Moreover, even when a member of the Class enabled their GPC Flag, thereby providing immediate notice of non-consent to Defendant's conduct, or found their way to the privacy selector and refused permission to share data with third parties, Defendant ignored all these privacy requests, and continued to occasion the download of invasive software onto each visitor's computer, which was then used to track and spy on private activities, on personal computers, and to share that information with marketers, data brokers, and other third parties.

57. At all times material hereto, Plaintiffs and the Class had a reasonable expectation of privacy on their own web browsers and personal computers.

58. Defendant's conduct constitutes an intentional intrusion into those private web browsers, computer systems, and the personal online affairs of Plaintiffs and the Class. Defendant did not merely glean and broadcast private information (which it did), but also physically invaded Plaintiffs' and the Class's personal computers by prompting the installation of invasive software thereon, to continuously spy upon and broadcast private online activities.

59. Defendant's conduct is highly offensive to any reasonable person. Indeed, the surreptitious download of software onto the private computer of every Website visitor is outrageous and is beyond the bounds of conventional decency.

60. As a result of Defendant's invasions of privacy, Plaintiffs and each member of the Class are entitled to recover such amounts as the jury in this case determines appropriate to vindicate the privacy rights of Plaintiffs and the Class, punitive damages in an amount to be determined by a jury in this case, and disgorgement of all profits generated by Defendant as a result of its use and deployment of the software at issue in this case.

WHEREFORE, Plaintiffs respectfully requests that this Court (a) certify the Class as defined above, comprised of all similarly situated person; (b) award Plaintiffs and every member of the Class appropriate damages for invasion of privacy, even if only a nominal amount per person; (c) award such punitive damages as are deemed just and equitable for Defendant's intentional misconduct; (d) disgorge all profits made by Defendant by virtue of its unlawful conduct described herein, with disgorged profits to be shared equally amongst Plaintiffs and the Class; and (e) award such further relief as may be deemed just and equitable under the circumstances presented.

COUNT II
TRESPASS UPON CHATTLES

Plaintiffs and the Class re-allege and incorporate Paragraphs 1 through 54 above, as though fully set forth herein.

61. Defendant's conduct as described above constitutes a use and interference with private property owned by Plaintiffs and the Class; specifically, Defendant made use of and interfered with private web browsers and personal computer systems, which were in the exclusive lawful possession and custody of Plaintiffs and the Class.

62. Defendant's use of and interference with private web browsers and personal computer systems belonging to Plaintiffs and the Class was unauthorized and was without any lawful justification.

63. At the time of Defendant's use and interference, the private web browsers and personal computers with which Defendant was interfering were in the possession of Plaintiffs and the Class, which had an exclusive possessory interest in the same (and certainly a superior interest to Defendant, which had none).

64. Defendant had no legal right and no legal authority to interfere with or use web browsers and computer systems owned and possessed by Plaintiffs and the Class.

65. Defendant's interference and use deprived Plaintiffs and the Class of computing memory, which was diverted to run software unlawfully installed upon their computing systems. Because Defendant causes the same third-party software to be downloaded onto each visitor's computer, Plaintiffs and the Class were each deprived of the same amount of computing memory.

66. In addition, Plaintiffs and the Class are entitled to punitive damages in an amount to be determined by a jury in this case, and disgorgement of all profits generated by Defendant as a result of its use and deployment of the software at issue.

WHEREFORE, Plaintiffs respectfully requests that this Court (a) certify the Class as defined above, comprised of all similarly situated person; (b) award Plaintiffs and every member of the Class compensation for Defendant's interference and use of their computer memory; (c) award such punitive damages as are deemed just and equitable for Defendant's intentional misconduct; (d) disgorge all profits made by Defendant by virtue of its unlawful conduct; and (e) award all such further relief as is deemed just and equitable under the circumstances presented.

COUNT III
CONVERSION

Plaintiffs and the Class re-allege and incorporate Paragraphs 1 through 54 above, as though fully set forth herein.

67. Plaintiffs and the Class have ownership and uncontested possessory rights to their own personal computers, including all the memory or computing power within and upon those personal computers, and all the web browsers located on those personal computers, including all data regarding online browsing contained thereon.

68. Defendant exercised wrongful dominion and control over the personal computers of Plaintiffs and the Class when it prompted those computers to download software onto each computer's web browser, which Defendant had no privilege to do, and which was done in a manner inconsistent with Plaintiffs and the Class' ownership and possessory rights.

69. By this act, Defendant (a) converted computing power belonging to Plaintiffs and the Class to its own use and purposes; and (b) converted personal data belonging to Plaintiffs and the Class to be used for its own commercial purposes, by its marketing partners, and by the identity resolution industry.

70. Defendant undertook these actions intentionally, willfully exercising wrongful dominion and control over computing systems that belong to Plaintiffs and the Class, in a manner

inconsistent with the absolute ownership interest, and possessory rights of Plaintiffs and the Class to their own personal computer systems. This includes unauthorized access to computing systems, taking of electronic data, and use of electronic data to which Defendant had no legal right.

71. Defendant's actions resulted in deprivation of property rights of Plaintiffs and the Class, including lost computing memory caused by installation of unauthorized software on their computing systems, as well as usurpation (and dissemination) of personal data, including personally identifying information and online activity. This deprivation occurred without consent, and to the contrary, in many instances occurred despite express withholding of consent.

72. In addition to the monetary value of converted computing memory, Plaintiffs and the Class are entitled to all profits derived by conversion of their electronic data, including all profits fairly traceable to electronic targeting and re-targeting, as well as disgorgement of all profits generated by Defendant as a result of its conversion of computing systems and data, and punitive damages for intentional misconduct as may be deemed appropriate by a jury in this case.

WHEREFORE, Plaintiffs respectfully requests that this Court (a) certify the Class as defined above, comprised of all similarly situated person; (b) award Plaintiffs and every member of the Class compensation for Defendant's conversion of their computing systems and data; (c) award such punitive damages as are deemed just and equitable for Defendant's intentional misconduct; (d) disgorge all profits made by Defendant by virtue of its unlawful conduct; and (e) award all such further relief as is deemed just and equitable under the circumstances presented.

COUNT IV
UNJUST ENRICHMENT

Plaintiffs and the Class re-allege and incorporate Paragraphs 1 through 54 above, as though fully set forth herein.

73. Defendant received a benefit from Plaintiffs and the Class in the form of electronic data usurped from computer systems and private web browsers that belong to Plaintiffs and the Class, as well as the use of computing memory to run software that captured and delivered the misappropriated electronic data.

74. Defendant had knowledge of the benefit that it derived. On information and belief, Defendant has detailed analyses regarding revenues generated by virtue of the software that it causes to be downloaded on visitor websites, and Defendant is aware that this benefit is derived by taking data and computing power that belongs to Plaintiffs and the Class.

75. Defendant has accepted and retained the benefits derived from computing power and personal data taken from Plaintiffs and the Class and has used those items to generate and increase revenues.

76. It would be wholly inequitable for Defendant to retain the financial benefits of its usurpation of visitor data and computing power, particularly since Defendant's actions were unauthorized, undertaken even after consent was explicitly withheld in many cases, and violate principles of fairness, fair play, and equity.

77. Plaintiffs and the Class are entitled to restitution in the form of all profits derived by converting the electronic data of Website visitors, including all profits fairly traceable to electronic targeting and re-targeting, as well as disgorgement of all profits generated by Defendant as a result of its taking and use of computing systems and data from Website visitors, as well as punitive damages for intentional misconduct as may be deemed appropriate by a jury in this case.

WHEREFORE, Plaintiffs respectfully requests that this Court (a) certify the Class as defined above, comprised of all similarly situated person; (b) award Plaintiffs and every member of the Class compensation for Defendant's conversion of their computing systems and data; (c)

award such punitive damages as are deemed just and equitable for Defendant's intentional misconduct; (d) disgorge all profits made by Defendant by virtue of its unlawful conduct; and (e) award all such further relief as is deemed just and equitable under the circumstances presented.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial as to all claims so triable.

Dated this **16th** day of **December, 2025.**

Respectfully submitted,

SALPETER GITKIN, LLP
3864 Sheridan Street
Hollywood, FL 33021
Telephone: (954) 467-8622
Facsimile: (954) 467-8623

By: */s/ James P. Gitkin*
JAMES P. GITKIN, ESQ.
Fla. Bar No.: 570001
jim@salpetergitkin.com
shelley@salpetergitkin.com

ENTIN LAW GROUP, P.A.
Co-counsel for Plaintiffs
1213 S.E. Third Avenue
Fort Lauderdale, FL 33316
Telephone: (954) 761-7201

By: */s/ Joshua M. Entin*
JOSHUA M. ENTIN, ESQ.
Fla. Bar No.: 493724
josh@entinlaw.com
laurac@entinlaw.com

LAW OFFICES OF NOLAN KLEIN, P.A.
5550 Glades Rd., Ste. 500
Boca Raton, FL 33431
Telephone: (954) 745-0588

By: */s/ Nolan K. Klein*
NOLAN K. KLEIN, ESQ.

Fla. Bar No.: 647977
klein@nklegal.com
amy@nklegal.com

JS 44 (Rev. 04/21) FLSD Revised 12/02/2022

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)* **NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.**

I. (a) PLAINTIFFS

NEAL MAGENHEIM and ANGELA NEIL

DEFENDANTS

NIKE, INC.

(b) County of Residence of First Listed Plaintiff St. Lucie County
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

See attachment

Attorneys *(If Known)*

(d) Check County Where Action Arose: ☐ MIAMI- DADE ☐ MONROE ☐ BROWARD ■ PALM BEACH ☐ MARTIN ☐ ST. LUCIE ☐ INDIAN RIVER ☐ OKEECHOBEE ☐ HIGHLANDS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

☐ 1 U.S. Government Plaintiff

■ 3 Federal Question *(U.S. Government Not a Party)*

☐ 2 U.S. Government Defendant

☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff) and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
☐ Citizen of This State	■ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
☐ Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

REAL PROPERTY
☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
■ 360 Other Personal Injury
☐ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
☐ 365 Personal Injury - Product Liability
☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

CIVIL RIGHTS
☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/ Accommodations
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty

Other:
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee – Conditions of Confinement

FORFEITURE/PENALTY
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 690 Other

LABOR
☐ 710 Fair Labor Standards Acts
☐ 720 Labor/Mgmt. Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act

IMMIGRATION
☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

BANKRUPTCY
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
☐ 820 Copyrights
☐ 830 Patent
☐ 835 Patent – Abbreviated New Drug Application
☐ 840 Trademark
☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 485 Telephone Consumer Protection Act (TCPA)
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/ Exchange
☐ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

■ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Re-filed **(See VI below)** ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation Transfer ☐ 7 Appeal to District Judge from Magistrate Judgment ☐ 8 Multidistrict Litigation – Direct File ☐ 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S) (See instructions): a) Re-filed Case ☐YES ☐NO b) Related Cases ☐YES ■ NO

JUDGE: **DOCKET NUMBER:**

VII. CAUSE OF ACTION Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause ***(Do not cite jurisdictional statutes unless diversity)***: Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and/or (c)(4) - Case involving the surreptitious installation of software on Plaintiffs' web browser without permission.

LENGTH OF TRIAL via 7-9 days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT: ☒ CHECK IF THIS IS A **CLASS ACTION** UNDER F.R.C.P. 23

DEMAND $ +$5M

CHECK YES only if demanded in complaint:

JURY DEMAND: ■ Yes ☐ No

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE: December 16, 2025

SIGNATURE OF ATTORNEY OF RECORD: /s/ James P. Gitkin

FOR OFFICE USE ONLY : RECEIPT # **AMOUNT** IFP JUDGE MAG JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence**. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked. Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Refiled (3) Attach copy of Order for Dismissal of Previous case. Also complete VI.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

Remanded from Appellate Court. (8) Check this box if remanded from Appellate Court.

VI. Related/Refiled Cases. This section of the JS 44 is used to reference related pending cases or re-filed cases. Insert the docket numbers and the corresponding judges name for such cases.

VII. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity**. Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VIII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

Date and Attorney Signature. Date and sign the civil cover sheet.

Section I(c) - Attorneys

James P. Gitkin, Esq
Salpeter Gitkin, LLP
3864 Sheridan Street
Hollywood, FL 33021
Telephone: (954) 467-8622
Facsimile: (954) 467-8623
jim@salpetergitkin.com
shelley@salpetergitkin.com

Joshua M. Entin, Esq.
Entin Law Group, P.A.
1213 SE Third Avenue
Fort Lauderdale, FL 33316
Telephone: (954) 761-7201
josh@entinlaw.com
laurac@entinlaw.com

Nolan K. Klein, Esq.
Law Offices of Nolan Klein, P.A.
5550 Glades Rd., Ste. 500
Boca Raton, FL 33431
Telephone: (954) 745-0588
klein@nklegal.com
amy@nklegal.com

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

NEAL MAGENHEIM and ANGELA NEIL, on behalf of themselves and all others similarly situated,

Plaintiff(s)

v.

NIKE, INC., an Oregon corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* NIKE, INC.
c/o United Agent Group Inc., Registered Agent
801 US Highway 1
North Palm Beach, FL 33408

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

James P. Gitkin, Esq.
Salpeter Gitkin, LLP
3864 Sheridan Street
Hollywood, FL 33021
(954) 467-8622

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: