VERIPATH, INC., a Delaware Corporation	Civil Action No. _____
Plaintiffs,	**COMPLAINT FOR PATENT INFRINGEMENT**
v.	
DIDOMI, a foreign entity,	**DEMAND FOR JURY TRIAL**
Defendant.	

Plaintiff VeriPath, Inc. ("Plaintiff" or "VeriPath") alleges as follows:

NATURE OF ACTION

1.   This is an action under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*, for infringement by Defendant Didomi. ("Defendant" or "Didomi") of a U.S. Patent.

THE PARTIES

2.   Plaintiff VeriPath is a corporation organized under the laws of Delaware and registered to do business in the state of New York, with its principal place of business at 665 S. Bayview Ave, Freeport, NY, 11520.

3.   Upon information and belief, Defendant Didomi is a société par actions simplifiées (simplified stock company) ("Didomi") organized under the laws of France.

JURISDICTION AND VENUE

4.   This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

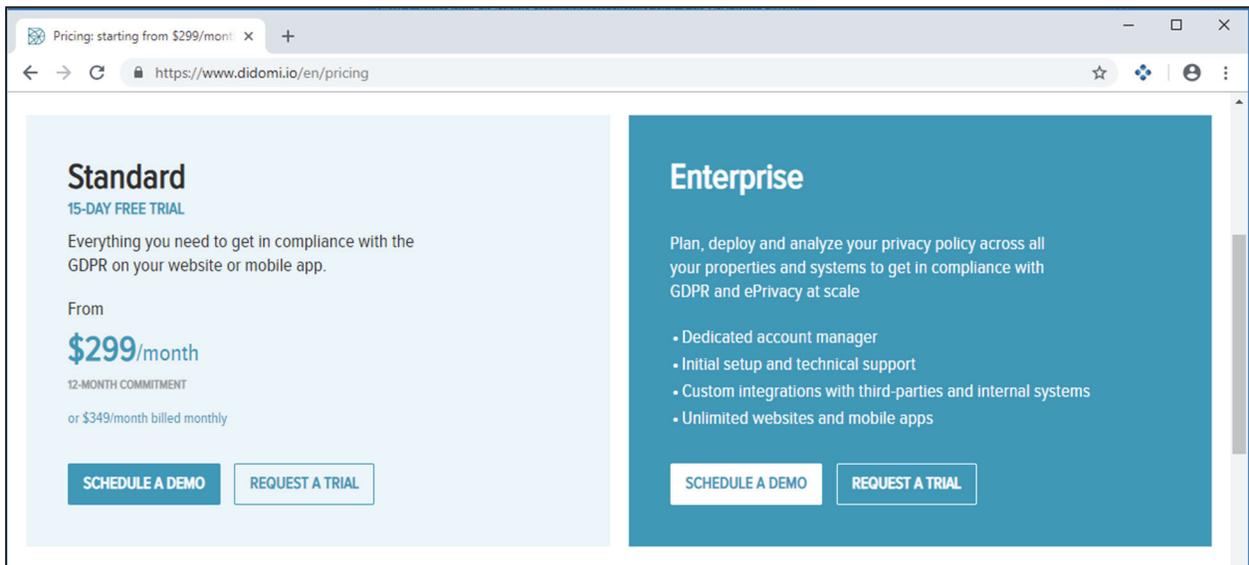5.   On information and belief, Defendant has a main office in New York. *See* Ex. B.

6.   Defendant conducts business in the United States. *See* Ex. C.

7.   Defendant's Chief Technology Officer is based in the United States, in the New York City area. Ex. L.

8.   Defendant's website is in English and displays the United States flag. *See* Ex. E.
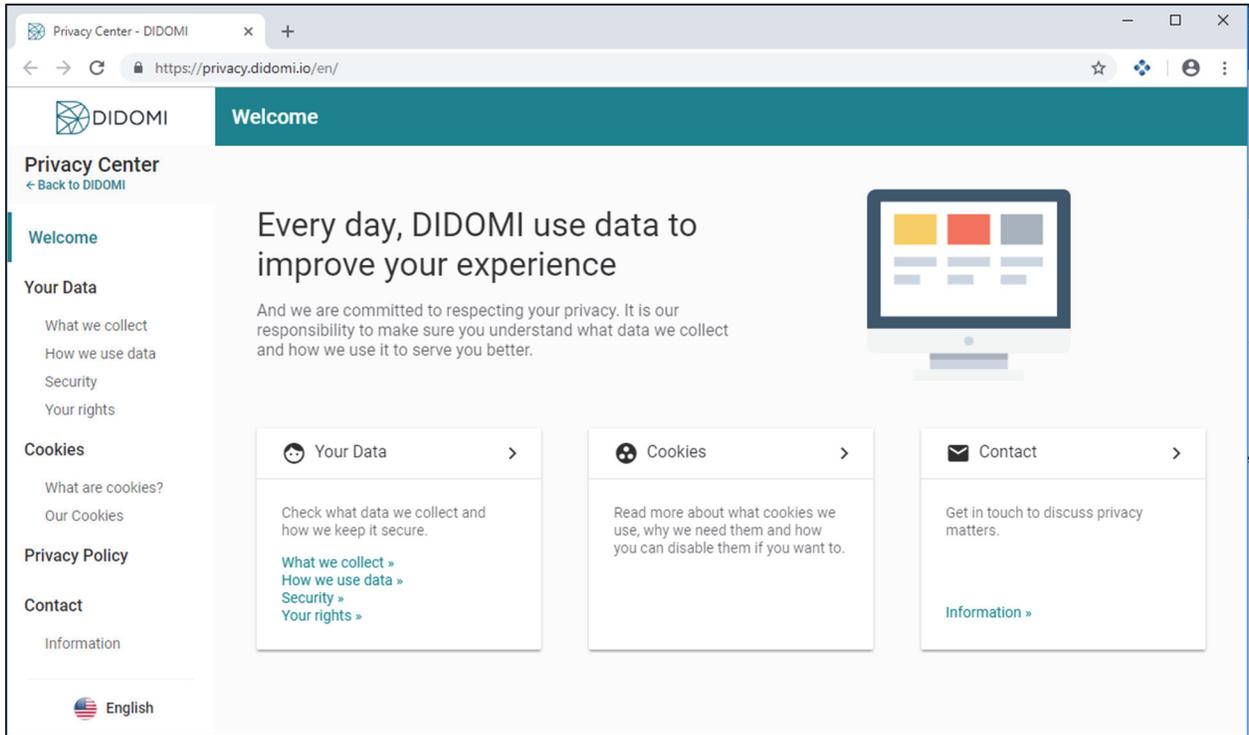

9.   Defendant offers its products for sale in the United States, in United States Dollars, on its English language-webpage. *See* Exs. D & F.

10.   On information and belief, Defendant conducts business in the state of New York.

11.   Defendant cites IAPP (International Association of Privacy Professionals), based out of New Hampshire, as one of its clients. *See* Exs. E & M.

12.   Defendant is a member of multiple IAB Tech Lab working groups, which are based out of New York City. *See* Exs. G (mobile group), H (blockchain group), & I (IAB Tech Lab location in New York City).
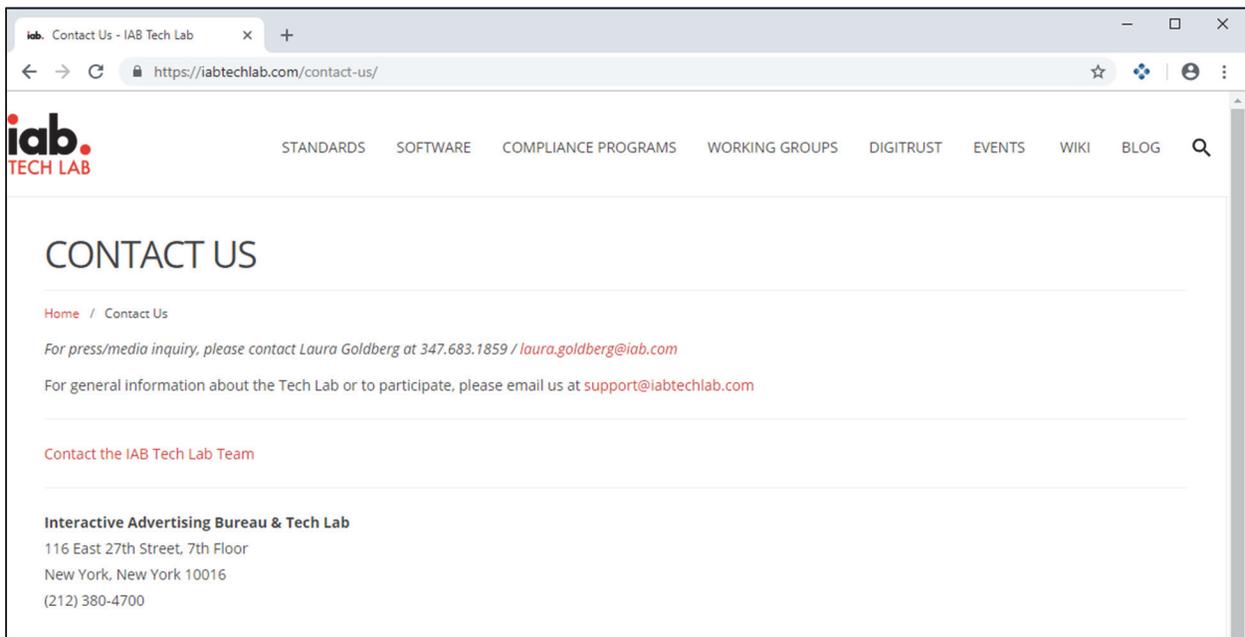
13.   On information and belief, Defendant transacts business in the state of New York by selling its products or running demonstrations of its software. These claims arise from Defendant's sales or demonstration of its Compliance Console and Privacy Center product as explained below.

14.   Defendant conducts substantial business in the state of New York, including (1) on information and belief, committing at least a portion of the infringing acts alleged herein and (2) regularly transacting business, soliciting business, and deriving revenue from the sale of services, including infringing services, to entities in the state of New York which are related to

the claims herein. *See* Exs. D & F (offers for sale and to schedule a demo on website, in English language). Thus, Defendant has purposefully availed itself of the benefits of the state of New York, and the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice.

15.   Venue is proper in this district pursuant to 28 U.S.C. §§ 1391 and 1400.

THE '451 PATENT

16.   VeriPath is a patent-protected data privacy and compliance manager and data incentivization platform.

17.   VeriPath is the owner by assignment of United States Patent No. 10,075,451 ("the '451 patent"), including the right to sue for past damages. Ex. K.

18.   The '451 patent was duly and legally issued by the United States Patent and Trademark Office on September 11, 2018, is active, and is entitled "Methods and Systems for User Opt-In to Data Privacy Agreements." A true and correct copy of the '451 patent is attached hereto as Exhibit A.

19.   Defendant has been aware of the '451 patent since at least February 6, 2019. Ex. J.

20.   Defendant directly infringes, literally or under the doctrine of equivalents, one or more claims of the '451 patent by, without authority, making, using, importing, selling, or offering to sell its Compliance Console and Privacy Center within the United States, in violation of 35 U.S.C. § 271(a).

21.   In addition to directly infringing the '451 patent pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Defendant indirectly infringes the '451 patent by instructing, directing, and/or requiring others, including its customers, purchasers,

users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the '451 patent, pursuant to 35 U.S.C. § 271(b) & (c).

<div align="center">

COUNT I
(Willful Infringement of United States Patent No. 10,075,451 by Defendant)

</div>

22.   VeriPath realleges and incorporates herein by reference the allegations set forth in the foregoing paragraphs.

23.   The '451 patent is presumed to be valid under 35 U.S.C. § 282.

24.   Defendant directly or indirectly infringes or induces infringement by its customers, literally or under the doctrine of equivalents, one or more claims of the '451 patent in violation of 35 U.S.C. § 271.

25.   Claim 1 of the '451 patent recites, as follows:

> 1. A method for controlling access to a user's personal information comprising:
> providing a software component for inclusion in an application, the software component having an application programming interface (API);
> obtaining, from the application executing on a device of a user of the application, personal information about the user of the application, the personal information obtained via the API by the software component executing on the device;
> identifying the type of the obtained personal information;
> determining, based on at least the type of obtained personal information, a required permission from the user for at least one proposed use of the obtained personal information;
> presenting, to the user, a first offer to provide access to at least one enhanced function of the application in exchange for the required permission; and
> responsive to the user providing the required permission, providing the user with access to the at least one enhanced function of the application.

26.   Defendant directly infringes, literally or under the doctrine of equivalents, one or more claims of the '451 patent by, without authority, making, using, importing, selling, or

offering to sell its Consent Management Platform and Privacy Center ("Privacy Products")

within the United States, in violation of 35 U.S.C. § 271(a).

27.   Defendant's Privacy Products enable web sites to comply with GDPR and other

data protection and privacy regulations.

Regulatory information

The Didomi platform allows you to publish clear legal information for your customers, in compliance with the GDPR.

- ✓ Standard information on personal data collected, data processing, user rights, and a dedicated section for your complete privacy policy
- ✓ Standardized data processing records to allow clear, transparent and structured communication
- ✓ Fully editable and customizable by the Data Privacy Officer from the Compliance Console
- ✓ Support for multiple languages with standard translations provided by Didomi

28.   Defendant "offers a Consent Management Platform (CMP) that can be deployed

on your websites and mobile applications to collect user consent before using personal data."

Didomi offers a Consent Management Platform (CMP) that can be deployed on your websites and mobile applications to collect user consent before using personal data. Our SDKs take care of all the interactions with the user and are integrated with third-parties to share consent automatically when possible (through the IAB framework or direct integrations). Our SDKs are highly customizable and offer many options to control the firing of third-party tags/SDKs.

29.   Defendant's Privacy Products provide consent management functionality in a

method for controlling access to a user's personal information.

Consent Management

Collect user consent across all your workflows and properties with banners, popups, form fields, etc.

Deploy our SDK once and manage your privacy rules easily over time without technical knowledge.

- ✓ Fully compliant with the EU Cookie law, GDPR and the upcoming ePrivacy, and optimized for maximum consent rates

- ✓ Integrated with the IAB GDPR framework, Google DFP/Adsense/Adx and tag managers for enforcing user consent across all your vendors

- ✓ Fully customizable (shape, position, color, language, etc.) from the Compliance Console without technical work

- ✓ Individual consents are automatically stored for future proof and can be retrieved at any time

30.   Defendant's Privacy Products provide a software component for inclusion in an application, the software component having an application programming interface (API).

API

The Didomi platform offers a standard REST API that you can use to manage all aspects of the platform. Its base URL is: `https://api.didomi.io/v1/` .

Our API uses standard HTTP verbs (`GET` , `POST` , etc.) to retrieve or modify resources and standard HTTP error codes (`4xx` and `5xx`) to communicate errors when they happen with detailed error information in the body. All standard HTTP clients are able to talk to our API without modifications.

The API always responds in JSON, including for errors. The only exception are routes that also support different formats like reports and, even in that case, JSON is the default format unless otherwise specified.

This section will guide you through setting up an API client and using the main resources exposed by our API. You will also want to consult our complete API specification as a reference when using our API.

You will need an API key and secret to call our API. If you do not have an API key yet, reach out to support@didomi.io.

31.   Defendant's Privacy Products "offer the Didomi SDK as a hosted JavaScript library that you can directly include on your website with a <script> tag."

```
Load the SDK

Script

We offer the Didomi SDK as a hosted JavaScript library that you can directly include on your website with
a <script> tag. Place the following tag at the top of the <head> section of your HTML pages, before
any other script tag:

 1   <script type="text/javascript">
 2   window.gdprAppliesGlobally=true;
 3   (function(){function n(){if(!window.frames.__cmpLocator){if(document.body&&document.boc
 4   </script>
 5
 6   <script type="text/javascript">
 7   window.didomiConfig = {
 8     website: {
 9       apiKey: '<Your API key>',
10       vendors: {
11         iab: {
12           all: true
13         }
14       }
```

32.   Defendant's Privacy Products include a software component, for inclusion in its

customer's applications, having an API.

```
Make sure to:

 • Place the tag as close to the opening <head> tag on your page as possible, before any other tag
   gets embedded
 • Add your API key into the tag (replace the <Your API Key> value)
 • Configure the gdprAppliesGlobally variable to false if you are not an EU-based company and
   only want to collect consent from EU visitors
```

33.   Defendant's Privacy Products obtain or facilitate obtaining, from the application

executing on a device of a user of the application, personal information about the user of the

application, the personal information obtained via the API by the software component executing

on the device.

> **Important: Embed our tag before any other tag**
>
> Yes, it's so important that we say it more than 4 times on this page!
>
> Keep in mind that the role of our JavaScript SDK is to share consent information with all the other scripts on the page. In order to do so, it **MUST** be placed before any other tag or the tags from your vendors will not be able to collect consent information from us. Put it as close as possible to the opening `<head>` tag. If our SDK gets included after the other tags then the consent information will not be correctly shared and you will not be compliant with the GDPR requirements.

34.   Defendant's Privacy Products identify or facilitate identifying the type of the obtained personal information.

> **Loading optimization**
>
> The SDK is loaded as an `async` JavaScript resource which ensures that it executes asynchronously while the page is being parsed and the other resources loaded. That way, it will have a minimal impact on your page load time and your content.
>
> **Fully compliant with the IAB GDPR framework**
>
> The notice is fully compliant with the IAB GDPR framework and will share the consent information collected from users with third-parties adhering to this framework to let them know what processing they are allowed to run. We also offer options to control the loading of third-party tags through your tags managers or special script tags.

> # Configure vendors and purposes
>
> As per the regulation, the consent notice collects consents for a specific set of vendors and purposes. You must configure the notice to let it know what vendors are used on your website and it will automatically determine what purposes are required.
>
> Read our dedicated section to learn how to configure your vendors.

35.   Defendant's Privacy Products identify or facilitate identifying information such as the country from which a user is accessing a website.

Configuration by user country

If you want to apply a different configuration depending on the country that the user is from, you can add country-specific properties in a `configByCountry` property where each key is a ISO 3166-1 alpha-2 country code in uppercase (the country code is case-sensitive). This allows you to replace part or all of the configuration for some countries.

36.   Defendant's Privacy Products determine or facilitate determining, based on at least the type of obtained personal information, a required permission from the user for at least one proposed use of the obtained personal information.

Country and GDPR

If you are an EU-based company then you must display the notice and collect consent no matter what country the user is from. Make sure that the `gdprAppliesGlobally` variable is set to `true` at the beginning of our tag (it's a separate variable than `window.didomiConfig`):

```
window.gdprAppliesGlobally=true;
```

Conversely, if you are not in the EU, you are not required to apply GDPR to non EU-based visitors (although you can if you want to). In that case, you can set the `gdprAppliesGlobally` variable to `false`.

37.   Defendant's Privacy Products "support[] classifying vendors and cookies in 4 categories."

Didomi supports classifying vendors and cookies in 4 categories:

- Analytics (`analytics`): cookies and vendors used for audience measurement, optimization, A/B testing, etc.
- Essential (`essential`): cookies that are required for the website to function (language settings, authentification, privacy preferences, etc.) i.e. to allow the electronic communication or the provision of an online service required by the user. These cookies cannot be disabled.
- Marketing (`marketing`): all cookies that are used by vendors running advertising or direct marketing (targeting, attribution, emailing, etc.).
- Social networks (`social`): cookies used by social networks services (Facebook, Twitter, LinkedIn, etc.) for various purposes.

As most third-party vendors do not offer a way to disable cookies from your website, Didomi blocks cookies by only embedding vendors on a webpage once consent has been collected . Didomi supports multiple integration modes to setup that feature, with consent collected from the consent notice.

ⓘ **Do not block essential cookies**

As per the regulation, you do not need user consent for setting essential cookies (authentication, tag management, CDNs, privacy, etc.).
You should directly add third parties from that category into your page without letting Didomi manage them.

38.   Defendant's Privacy Products present or facilitate presenting, to the user, a first offer to provide access to at least one enhanced function of the application in exchange for the required permission.
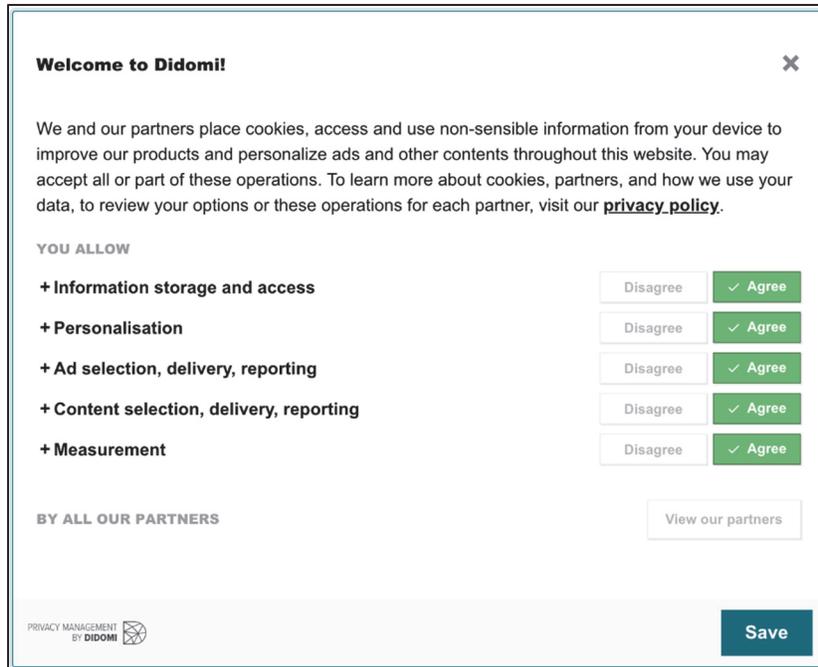
39.   Defendant's Privacy Products, responsive to the user providing the required permission, provides or facilitates providing the user with access to the at least one enhanced function of the application.

40.   Defendant's Privacy Products, prevent vendors tags from loading until the user given consent for the vendor and its purpose.
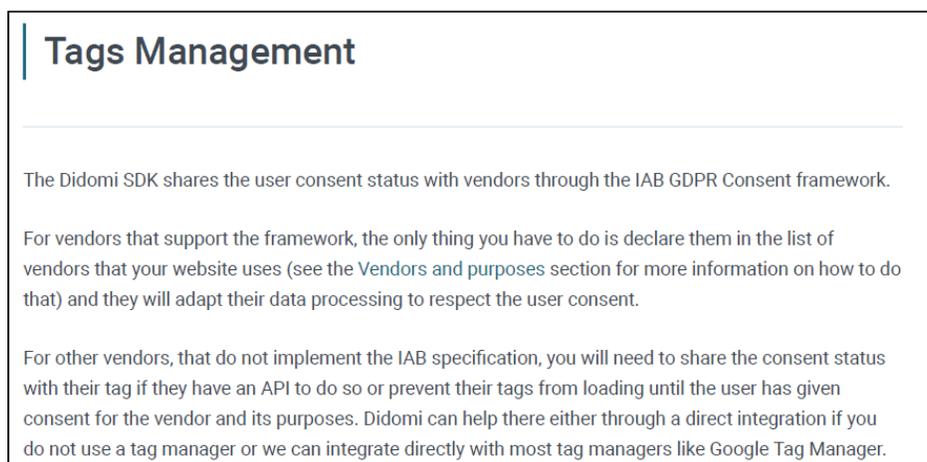
41.   Defendant's Privacy Products include a function that will be called "only when the user has given consent to the vendor specifically. It could be immediately if the user has

already given consent or later on after the user gives consent."

Enable a vendor when the user has allowed it

With this structure, your function gets called exactly once and only when the user has given consent to the vendor specifically. It could be immediately if the user has already given consent or later on after the user gives consent.

```
1   window.didomiOnReady = window.didomiOnReady || [];
2   window.didomiOnReady.push(function (Didomi) {
3       if (Didomi.isConsentRequired()) {
4           // Consent is required: your visitor is from the EU or you are an EU company
5           // Only enable the vendor when consent is given
6           Didomi.getObservableOnUserConsentStatusForVendor('vendor-id')
7               .first() // Only get the first consent status update
8               .filter(function(status) { return status === true; }) // Filter out updates
9               .subscribe(function (consentStatusForVendor) {
10                  // The user has given consent to the vendor
11                  // Enable it
12              });
13      } else {
14          // Consent is not required, enable your vendor immediately
15      }
16  });
```

ⓘ If your tag is configured to only collect consent for visitors from the EU, you can enable all your tags for other visitors without waiting for the consent. Use the isConsentRequired() function to check if consent is required or not for the current visitor on the page.

42.   As explained in the foregoing paragraphs, Defendant's Privacy Center infringes at least claim 1 of the '451 patent.

43.   Defendant's infringement of the '451 patent has been willful since at least February 6, 2019.

44.   VeriPath has been and continues to be injured by Defendant's infringement of the '451 patent. VeriPath is entitled to recover damages adequate to compensate it for Defendant's infringing activities in an amount to be determined at trial but in no event less than a reasonable royalty.

45.   Unless enjoined by this Court, Defendant's acts of infringement will continue to damage VeriPath irreparably.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that this Court:

a.   Enter a judgment that Defendant has infringed one or more claims of the '451 patent;

b.   Grant a permanent injunction restraining and enjoining Defendant and its officers, directors, agents, servants, employees, successors, assigns, parents, subsidiaries, affiliated or related companies, and attorneys from directly or indirectly infringing one or more claims of the patents-in-suit;

c.   Award Plaintiff damages in an amount sufficient to compensate VeriPath for Defendant's infringement of the '451 patent, but not less than a reasonable royalty, together with interests and costs;

d.   Award Plaintiff treble damages for Defendant's willful infringement;

e.   Award prejudgment interest to VeriPath under 35 U.S.C. § 284;

f.   Grant such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

VeriPath respectfully demands a trial by jury on all claims and issues so triable.

Dated: February 22, 2019

Frederick L. Whitmer

_____

Frederick L. Whitmer
Kilpatrick Townsend & Stockton, LLP
The Grace Building
1114 Avenue of the Americas
New York, NY USA 10036
212.775.8700
FWhitmer@kilpatricktownsend.com

Of Counsel
John C. Alemanni
(*pro hac vice application forthcoming*)
Kilpatrick Townsend & Stockton, LLP
4208 Six Forks Road, Suite 1400
Raleigh, NC 27609
919.420.1700
JAlemanni@kilpatricktownsend.com

Michael T. Morlock
(*pro hac vice application forthcoming*)
Kilpatrick Townsend & Stockton, LLP
1100 Peachtree St. NE, Suite 2800
Atlanta, GA 30309
404.815.6500
MMorlock@kilpatricktownsend.com