BCLP. Client Intelligent

RetailLawBCLP

APIS HAVE BROAD APPLICATIONS, FROM E-COMMERCE TO PAYROLL MANAGEMENT

Jun 03, 2019

This post is the second in a two-part series concerning emerging uses and considerations involving application programming interfaces, or "APIs."

Most retailers and other large and mid-size businesses, and even some small businesses, utilize public APIs:

- Businesses who vet their employees against a government database may be doing so through an API.
- Businesses that rely on vendors to provide data or electronic services (such as HR and payroll management) may be receiving them through APIs.
- Businesses that maintain databases associated with their website or applications, likely communicate with that database through an API.
- Businesses that provide electronic data or electronic services are likely doing so through an API. When the API license is presented as a take-it-or-leave-it agreement, the terms are often written to protect the provider from any liability for an offering from which the provider derives no direct financial benefit.

Still, regardless as to whether the license is free, prospective business licensees need to consider at least the following:

- The use of most public APIs is contingent upon the user's agreeing to the distributor's contractual requirements. APIs made available for free may be provided pursuant to "licenses" or may alternatively be provided pursuant to a "terms of use" that sets forth the conditions under which use is permitted. Under either approach, if the user refuses to accept the terms, then use is barred. APIs made available for a fee may also be styled as a "terms of use" but commonly have "license" or "service" in their titles. (Sometimes separate "license" and "terms of use" documents coexist with the terms of use governing how the API is actually used.)

Ultimately, traditional assumptions about bargaining power play out, with the dominant players often demanding conformity.

- Can the API be used for a commercial purpose?
- Is there a warranty?
- Is there a non-indemnified risk of infringing another's IP rights?
- Does the user owe indemnity to the API provider?
- Is there a right to track how the API is used?
- What license does the API provider receive in any data given to it?
- Is there an acknowledgment of the provider's rights to the API and its implementations?

The incentive to give a warranty for reliance on an API is reduced when the provider receives nothing for the API. Nonetheless, using an API is accompanied by risk. Just because a business receives data through an API does not mean that API was allowed to relay that data. The API could be implemented in a way that (unwittingly) permits infringement of another's patent, copyright, trade secret, or other rights, or the API may violate other contractual rights. For example, a photo sharing site may entitle users to download photos via an API, but if a photo's original poster was infringing another's copyright, then the subsequent downloading of the photo by another may unwittingly expose the downloader to liability infringement.

Data privacy and security may also become relevant. As a matter of responsible IT management, the API provider may log what requests were made for information to its servers and by whom. Sometimes, the terms of use may expressly disclose how such API calls are tracked; in other circumstances, the tracking may be hidden in a privacy policy. In any setup, there is a risk that a user's private information may be exposed in the course of requesting information through an API.Given the current state of case law, an API provider may seek an acknowledgement that the provider owns the API and the implementation behind it. Further, the API provider may bar the development of an independent implementation for the API. In such circumstances, a careful review by legal counsel would be prudent.

APIs are a valuable part of ecommerce and software development. This sampling of considerations underscores the serious considerations in any API strategy by a provider or user. As a company's provision or use of APIs increases, the company should do so cognizant of the risks and within the framework of effective API management.

There are circumstances in which a user's content or other data will be submitted to an API or the use of the API will create data. Some API providers may fear a copyright or other claim if the user does not license the submitted content. Most such licenses, however, are broadly written to cover

future contingencies, and the language may have broader ramifications than the API provider or user initially intend.

Some API providers compel their users to indemnify the provider. When such clauses are narrowed to indemnification for the user's own conduct, they may be reasonable, but, often, the user is not well positioned to know the full scope of potential risks—and such asymmetry necessitates a closer review of the user's indemnification risk.

A common restriction is that the API be used for non-commercial purposes. Moreover, the provider may even have a business model that charges for commercial uses of the API. Failure to abide by the requirement may subject the user to paying damages at the provider's standard rates. If the API use was voluminous and/or over an extended period of time, the damages could create significant liability. Meanwhile, the agreement governing the API may give the provider a right to track how the API is used, potentially for the provider's own business purposes or even to audit whether the API is used for non-commercial uses.

RELATED PRACTICE AREAS

- Retail & Consumer Products

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435