THOMSON REUTERS
Westlaw®

In the age of digital interconnectivity, API is front and center

By Meaghan H. Kent, Esq., and Thai-Hoa X. Su, Esq., *Venable LLP**

MAY 6, 2020

In today's digital world, APIs, or application programming interfaces, play a rapidly growing role in meeting our need for more interconnectivity.

APIs are software intermediaries that allow different programs and applications to share data — communicating and interacting with each other to expand business functionalities.

As we all grow increasingly reliant on remote access and work, API will continue to serve as an essential element of facilitating business and everyday life.

To that end, every business needs to consider how best to protect this valuable resource. In this article, we discuss several ways in which legal issues surrounding APIs arise and how businesses can better protect their APIs.

COPYRIGHT LAW

Computer programs are protected as literary works under U.S. copyright law. Even though software can be considered functional, Congress provided in the Copyright Act that software code itself is protected by copyright and can be registered as a textual work. This includes API code.

It is worth noting that the U.S. Supreme Court has granted certiorari in the long-running *Oracle v. Google* case, involving Google's use of Java API in creating Android.

The case is set to decide two key issues related to API:

(1) Whether the structure, sequence, and organization of the Java API packages are copyrightable (*see Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014)); and

(2) whether Google's use of the Java API packages was a fair use (*see Oracle Am., Inc. v. Google LLC,* 886 F.3d 1179 (Fed. Cir. 2018)).

The briefing in that case is complete, including from dozens of amici, and oral argument was set to occur on Tuesday, March 24, 2020; however, that argument has been postponed in light of COVID-19 restrictions.

Once argued and decided, there may be further clarity on the scope of API copyrightability, though it is generally expected that API will remain protected by copyright.

Since APIs are copyrightable, the typical bundle of rights exists for the copyright owner, including the right to limit the use, copying, distribution, and creation of derivative works.

That is, only copyright owners have the right to make derivative works, which are works based on or derived from one or more pre-existing works.

For instance, in the API context, someone who copies an API and uses it without permission, such as by incorporating it into their own code, infringes that API (*see Oracle v. Google*).

TRADEMARK LAW

Trademarks are words, logos or other designations that identify the source of a product or service.

As we all grow increasingly reliant on remote access and work, API will continue to serve as an essential element of facilitating business and everyday life.

The owner of the trademark has the right to control the use of the trademark to prevent consumers from becoming confused as to the source, sponsorship, or affiliation of goods or services associated with the mark.

Trademark issues also arise with APIs. One example occurs when a developer incorporates an API into their code then advertises or claims interconnectivity with the API and its source.

If the API was used without permission and the interconnectivity is not authorized, the trademark use is also unauthorized, as it creates a false association or endorsement.

CONTRACT LAW

A contract is a legally binding agreement, written or oral, between two parties that creates mutual obligations.

Contract law is usually implicated in the API world in two forms:

(1) API licensing agreements and

(2) a website or application's terms of use (TOUs).

In the first example, a licensing agreement is a written contract between two parties, in which a property owner allows another party to use that property under defined parameters.

The ability to develop third-party APIs using a company's data is usually heavily regulated through API licenses. API licenses are important because they allow data owners to set the expectations and standards for third-party developers.

Most licenses allow data owners to unilaterally amend the terms at any time, which can protect data owners if, down the road, changes need to be made to the data itself or to the type of access developers have.

Companies should be wary of allowing developers liberal access to their data, as circumstances can quickly change in the ever-evolving API world.

For example, in 2011, Twitter had originally given developers very liberal access to their API, but some developers started copying Twitter's API interface to compete with Twitter. Twitter later had to change the terms of its API license to restrict developer use.

In the second example, companies can be vulnerable to third parties reverse engineering APIs or scraping data from websites or applications to create their own API without a license.

Data scraping is a method in which a computer program extracts data from output generated from another program. Any information that can be viewed on a website or application is vulnerable to scraping.

Aside from implementing security measures to block data scraping, companies can legally protect themselves by having TOUs that expressly prohibit reverse engineering and the scraping of information or data.

A developer that engages in reverse engineering and data scraping is legally bound by those terms and could be liable for breach.

THE COMPUTER FRAUD AND ABUSE ACT

Where API developers do not have a data owner's permission to use its data or integrate with its programs or applications or when they engage in data scraping, such integration and scraping may serve as the basis of a Computer Fraud and Abuse Act (CFAA) claim.

The CFAA prohibits the intentional unauthorized access or exceeding authorized access to a protected computer and obtaining information from that computer.

The CFAA is generally a criminal statute, and to qualify as a civil action, the violation must have resulted in a "loss" of at least $5,000 during any one-year period.

"Loss" has been defined as "any reasonable costs to any victim, including responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]" 18 U.S.C. §1030.

When analyzing CFAA claims, courts typically consider whether a defendant has violated a website, program, or application's TOU as part of the "unauthorized access" or "exceeds authorized access" analysis.

For example, in *Craigslist, Inc. v. Naturemarket, Inc.*, the court found that "Plaintiff alleged that Defendants accessed its computers in violation of the TOUs, and therefore without authorization."

In contrast, in *Cvent, Inc. v. Eventbrite, Inc.*, the court found the TOUs were "not displayed on the website in any way in which a reasonable user could be expected to notice them" because they were "buried at the bottom of the first page, in extremely fine print."

Thus, to strengthen the basis for a CFAA claim, data owners should have TOUs that clearly deny users' ability to integrate with, modify, make derivative works of, or access information and data on their website, program, or application, including explicit provisions against data scraping, unless users have been granted such rights in a licensing agreement, and be sure that the TOUs are conspicuous and agreed to by the user.

With our rapidly increasing reliance on remote access and interconnectivity, businesses must take a second look at how they are currently protecting and how they can better protect API as a valuable resource.

Please contact the authors or others in Venable's Intellectual Property Division with questions or for assistance in ensuring that you have the appropriate protections in place.

This article first appeared in the May 6, 2020, edition of Westlaw Journal Intellectual Property.

* © 2020 Meaghan H. Kent, Esq., and Thai-Hoa X. Su, Esq., Venable LLP

ABOUT THE AUTHORS


Meaghan H. Kent (L) is a partner in **Venable LLP**'s Intellectual Property Litigation practice in Washington. She focuses on intellectual property law, including copyrights, trademarks, right of publicity and patents. She can be reached at mhkent@Venable.com. **Thai-Hoa X. Su** (R) is an associate in the firm's Intellectual Property Litigation practice in Washington. She can be reached at txsu@Venable.com. This article was originally published March 26, 2020, on the firm's website. Republished with permission.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.