BCLP. Client Intelligent

RetailLawBCLP

RETAILERS SHOULD CONSIDER POTENTIAL REWARDS AND RISKS OF USING APIS

May 14, 2019

Application programming interfaces, or "APIs," have become a critical part of ecommerce, and retailers are increasingly finding new and creative ways to use APIs to enhance their offerings and their business. For example, Kroger deploys an API with information about its groceries, locations, coupons, and loyalty programs. BestBuy similarly offers APIs to third parties, including one for recommended purchases. LensCrafters, Williams-Sonoma, and other retailers have further deployed APIs to expand consumer access to their information. Still, many other retailers are connecting to PayPal and other fintech companies to provide multiple secure checkout options.

This post is the first in a two-part series concerning emerging uses and considerations involving APIs.

The provision of public APIs has exploded in recent years amid ecommerce. More than 60 percent of eBay listings are added via API. At least 50 percent of Salesforce transactions are via APIs. Ecommerce service companies Shopify ($25B) and Twilio ($15B) have exploded to multibillion dollar market valuations, in part, through providing APIs to retailers.

Without APIs, a third-party developer could theoretically create a bot to visit these retailers' websites and "scrape" key information, but such an approach is less effective than an API. First, through an API, the provider controls what third parties access, while "scraping" raises copyright risks. *See, e.g., Ticketmaster L.L.C. v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007) (granting injunctive relief on grounds that defendant infringed copyright and terms of use through automated screen-scraping of Ticketmaster's site in order to facilitate its own large-volume ticket brokerage). Second, even a slight change to the website could cause the bot to misunderstand the data being scraped. Third, this conversion step fails to capture the richer, more reliable, and more precise data available through the API.

The website ProgrammableWeb tracks more than 20,000 publicly known APIs; even more are maintained privately or subject to confidentiality agreements. Most public APIs were developed by their distributor, others were developed by industry groups, and a fraction were developed in response to government requirements. Through these APIs, financial information, inventory

information, federal government data, and other information and services can be accessed, pursuant to the terms of use imposed by the licensor.

Using APIs carries its own risk—almost inherently. Flaws in APIs can expose customer data and/or transaction histories, raising potential risk of claims under consumer privacy laws. According to HIMSS, healthcare APIs risk exploitation through denial of service, cookie tampering, and man-in-the-middle attacks. Disputes over API rights have also led to billion-dollar claims between corporate giants.

API usage is here to stay and will almost certainly increase in the future. Retailers should therefore consider how to manage this tool, while at the same time protecting customers' personal information and reducing liability risks. Our next post will further address some of these risks and mitigation strategies.

RELATED CAPABILITIES

- Retail & Consumer Products

MEET THE TEAM

Merrit M. Jones

San Francisco

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

professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.