Proskauer

Another Web Scraping Dispute Focused on Travel Data

New Media and Technology Law Blog on **November 17, 2023**

- Flight and travel data has always been valuable for data aggregators and online travel services and has prompted litigation over the years.
- Latest suit from Air Canada against a rewards travel search site raises some interesting liability issues under the CFAA.
- The implications of this case, if the plaintiffs are successful, could impact the legal analysis of web scraping in a variety of circumstances, including for the training of generative AI models.

In a recent post, we recounted the myriad of issues raised by recently-filed data scraping suits involving job listings, company reviews and employment data. Soon after, another interesting scraping suit was filed, this time by a major airline against an award travel search site that aggregates fare and award travel data. Air Canada alleges that Defendant Localhost LLC ("Localhost" or "Defendant"), operator of the Seats.aero website, unlawfully bypassed technical measures and violated Air Canada's website terms when it scraped "vast amounts" of flight data without permission and purportedly caused slowdowns to Air Canada's site and other problems. (*Air Canada v. Localhost LLC*, No. 23-01177 (D. Del. Filed Oct. 19, 2023)).[1]

The complaint alleges that Localhost harvested data from Air Canada's site and systems to populate the seats.aero site, which claims to be "the fastest search engine for award travel."

It also alleged that in addition to scraping the Air Canada website, Localhost engaged in "API scraping" by impersonating authorized requests to Air Canada's application programming interface.

Air Canada claims that Localhost's activities burdened Air Canada's system and caused its site to become unresponsive at times for customers (a claim that was common in the early scraping cases alleging trespass to chattels-type claims like the *eBay v. Bidder's Edge* dispute), where that court's preliminary injunction analysis included discussion about the effect web crawling activities had, or could have, on eBay's systems).

Air Canada asserts that it attempted to thwart Localhost's scraping activities by bolstering its bot detection and other code-based defenses to unwanted scraping but was largely unsuccessful. The complaint also expressly stated that Localhost ignored the site's robots.txt instructions, the voluntary standard for communicating to scrapers the web site owner's preferences regarding automated access to web pages, and which in Air Canada's case, disallowed all data scrapers.

Air Canada advanced multiple claims, including: (1) breach of contract, as automated scraping activities are prohibited by the website terms; (2) "unauthorized access" violations under the Computer Fraud and Abuse Act (CFAA); (3) various Lanham Act violations for Defendant's alleged use of Air Canada logos in travel listings and results displayed on its site;[2] and (4) trespass to chattels, or the common law interference with Air Canada's use and possession of its servers and infrastructure. Air Canada requests monetary damages and injunctive relief barring Defendant from accessing or scraping Air Canada's site or otherwise using the Air Canada sites in a manner that violates the terms, or publishing any fare data and reward information scraped from the site.

Thoughts on the Case

Air Canada's breach of contract claims are based on alleged violations of its site terms that prohibit scraping. The terms are presented as a "browsewrap" agreement, whereby the website operator claims that users are presumed to be bound by a website's terms by mere use of the site, without the need for any outward manifestation of assent. Air Canada's terms state, in relevant part: "Each time you access or use the Website, you are entering into a contract with us and you agree to be bound by these Terms of Use." The enforceability of browsewrap terms remains unsettled. The complaint states that Air Canada also sent a cease-and-desist letter that purportedly gave Defendant actual notice of the terms and its supposed violation.

Air Canada also advanced a CFAA claim against Localhost for its alleged "unauthorized access" to its systems. Air Canada's site seems to allow users to search flights and awards travel opportunities without signing in, raising a question of whether such flight data is "public" data. As previously explored in this blog, including our coverage of the hiQ-LinkedIn scraping litigation, the success of a CFAA "unauthorized access" claim depends, in part, on the nature of the scraped data. In its 2022 opinion in that case, the Ninth Circuit limited the applicability of the CFAA as a tool against the scraping of publicly available website data.

Still, as previously covered in a prior post, a Delaware federal district court (the same district as the instant case) allowed scraping-related CFAA claims brought by an airline to go forward against an online booking site. In that case, the court stated: "[F]or the CFAA's 'without authorization' and 'exceeds authorized access' elements to apply, some sort of authentication mechanism (e.g., the use of usernames and passwords) must be employed to limit access to the website. If the information on the website is publicly available without requiring users to authenticate themselves, a violation of the terms of use or the defiance of a cease-and-desist letter will not give rise to liability under the CFAA."

Additional discovery would presumably be needed to discern the extent of authentication methods employed by Air Canada (though, the complaint states the airline hired a third party vendor to erect additional barriers to scraping once it became aware of the extent of Localhost's scraping). Ultimately, the parties may end up arguing the CFAA "unauthorized access" issue over whether the authorization "gates" of Air Canada's site were open or closed to users and whether the technical defenses to scraping adopted by Air Canada were sufficient to lower the "gate," as understood by the Supreme Court's noteworthy *Van Buren* decision.

This complaint raises issues which could be relevant to a wide range of web or API scraping disputes, including generative AI training cases. (Of course those cases often include copyright claims, something that is not part of this case.) Thus, as with the variety of other ongoing scraping cases out there, we will follow this case to see what principles will emerge.

---

[1] Fare data has long been scraped by aggregators and specialized travel sites and has produced a fair share of screen scraping litigation (e.g., we last wrote about a dispute involving an airline obtaining an injunction against and later settling with an online travel site and another dispute involving a booking site that allegedly scraped the ticketing portion of an airline's site).

[2] Note: Air Canada advanced various Lanham Act claims, including counterfeiting, trademark infringement, unfair competition, false advertising and trademark dilution relating to the alleged use of Air Canada marks and logos in connection with seats.aero's travel reservations and incentive services. Discussion of these types of claims is beyond the scope of this post.

View original.

Related Professionals

- **Jeffrey D. Neuburger**