HIQ LABS V. LINKEDIN

CASE STUDY AND ITS IMPLICATION FOR THE OPEN BANKING REGULATION IN THE U.S. COMPARED WITH THE CURRENT CASES AND REGULATIONS IN SOUTH KOREA

*Lisa Lyhyun Park**

* LL.M, 2023, The George Washington University Law School; M.A., 2020, Goethe Business School, Frankfurt University, Master of Finance; B.A.(LL.B), 2012, Ewha Womans University, Bachelor of Law. The author is a practicing attorney with experience and an educational background in corporations, securities, financial contract drafting and international cross-border transactional law.

INTRODUCTION

Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, including, for example, those that provide real-time payments, greater financial transparency options for account holders, marketing, and cross-selling opportunities,[1] like Venmo and Zelle. Screen scraping is the process of collecting data which actually appears on the screen of a device, whereas web scraping is the process by which the website's data—which is not visible to the user without taking additional steps—is extracted.[2]

The first part of this paper will analyze the recent court decision in *hiQ Labs v. LinkedIn* about data scraping and conclude with a comparative study of what factors the court should consider in analyzing the liability of a data scraper like hiQ Labs ("hiQ") and Venmo.[3] In the second part, this paper will derive the implication of the current open banking scraping regulation status and examine the possible liability issues in open banking.

II. HIQ LABS V. LINKEDIN COMPARATIVE CASE STUDY

After hiQ scraped public data from LinkedIn, it litigated against the platform for six years, ending in a confidential

1. BANK FOR INT'L SETTLEMENTS, REPORT ON OPEN BANKING AND APPLICATION PROGRAMMING INTERFACES (2019); Anil K., *Screen Scraping is Transforming Mobile Payments,* LINKEDIN (Aug. 21, 2019), https://www.linkedin.com/pulse/screen-scraping-transforming-mobile-payments-anil-k/.

2. Susan M. Pandy, *Modernizing U.S. Financial Services with Open Banking and APIs,* FED. RSRV. BANK BOS., (February 8, 2021), https://www.bostonfed.org/-/media/Documents/PaymentStrategies/Modernizing-US-Financial-Services-with-Open-Banking-and-APIs.pdf; EJ Stanley, *What is Web Scraping? A Complete Guide*, FORTRA, https://www.fortra.com/resources/guides/what-is-web-scraping (last accessed Feb. 25, 2025); CHERYL R. COOPER, CONG. RSCH. SERV., IN11745, OPEN BANKING, DATA SHARING, AND THE CFPB'S 1033 RULEMAKING (2023).

3. hiQ is a data analytics company founded in 2012. Amy Brantly, *hiQ Labs, Inc. v. LinkedIn Corp.: Protecting Smaller Data Rivals from Attempted Data Monopolists*, CAL. LAWS. ASS'N (Sept. 30, 2019), https://calawyers.org/antitrust-unfair-competition-law/hiq-labs-inc-v-linked-corp-protecting-smaller-data-rivals-from-attempted-data-monopolists/

settlement agreement.[4] In two similar cases in South Korea, the final court decided that the scrapers violated the South Korean antitrust law, imposing no other charges.[5] In both cases, the competitors shared the same industry; the first in accommodation and the other in the job-searching industry.

A. *Facts*

In mid-2017, hiQ sued LinkedIn to recognize hiQ's right of access to LinkedIn's public pages and sought an injunction if LinkedIn refused.[6] Using automated bots, hiQ had been scraping LinkedIn users' information, such as their names, job titles, work history, and skills, from their public profiles.[7] It then used that information and a proprietary algorithm to yield "people analytics," and sold the data to business clients.[8] In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ violated LinkedIn's User Agreement[9] and demanded that hiQ stop accessing and copying data from LinkedIn's server.[10] In response, hiQ filed three actions, as follows: (1) an injunctive relief based on California law; (2) a declaratory judgment that LinkedIn could not lawfully invoke the (i) Computer Fraud and

---

4. Kyle Dull, Julia Jacobson & Sasha Kiosse, *LinkedIn's Data Scraping Battle with hiQ Labs Ends with Proposed Judgment*, SQUIRE PATTON BOGGS (Dec. 19, 2022), https://www.privacyworld.blog/2022/12/linkedins-data-scraping-battle-with-hiq-labs-ends-with-proposed-judgment/.

5. *See* Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], 2015gahap517982, February 17, 2015 (S. Kor); *see* Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan. 13, 2021, 2020No611 (S. Kor.); *see also* Hyeong Joo Lim, et al., *Korean Supreme Court Provides Clarity on Web Scraping and Violation of the Relevant Korean Laws, including the Copyright Act and Information Protection Act (Supreme Court, 2021Do1533, May 12, 2022)*, YULCHON LLC (July 20, 2022), https://www.yulchon.com/en/resources/publications/newsletter-view/32426/page.do

6. Dull, *supra* note 4.

7. Brantly, *supra* note 3.

8. *Id.*

9. *hiQ Labs, Inc. v. Linkedin Corp.*, 273 F. Supp. 3d 1099, (N.D. Cal. 2017); *see User Agreement*, LINKEDIN (June 7, 2017), https://www.irisinvestigations.com/wp-content/uploads/2016/12/ToolBox/10-INTERNET%20&%20SOCIAL%20MEDIA/Terms%20of%20Service/LinkedIn%20User%20Agreement%2006-07-2017.pdf.

10. Brantly, *supra* note 3.

Abuse Act (CFAA), (ii) Digital Millennium Copyright Act (DMCA), (iii) Unauthorized computer access (California Penal code § 502 (c)), and (iv) Common law of trespass; and (3) a motion for a preliminary injunction.[11]

The case originated in the original district court injunction in 2017, and the Ninth Circuit affirmed the decision in 2019.[12] The Supreme Court, however, vacated the order in 2021.[13] After that, the Ninth Circuit issued a new order in April of 2022 affirming the original injunction, and the lower court issued an order dissolving the preliminary injunction in August of 2022.[14] On November 4, 2022, hiQ ultimately prevailed under the Computer Fraud and Abuse Act (CFAA) on the "unauthorized access" issue related to public website data, but also faced the ruling that it had breached LinkedIn's User Agreement due to its scraping and creation of fake accounts subject to its equitable defenses.[15] On December 6, 2022, the litigation between LinkedIn and hiQ reached a confidential settlement agreement resolving all outstanding claims.[16]

B. *LinkedIn's claims against scraper hiQ and the final court decision*

1. Computer Fraud Abuse Act: No violation (April 22, 2022, Ninth Circuit decision).

In April of 2022, on remand, the Ninth Circuit concluded that hiQ had raised serious questions as to the applicability of the CFAA to its conduct.[17] The plaintiff (hiQ) unquestionably faced irreparable harm in the absence of an injunction, as it would likely be driven out of business. Therefore, the court had severe

---

11. *Id.*

12. *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1103 (N.D. Cal. 2017), *aff'd*, 938 F.3d U.S. 985, 1005 (9th Cir. 2019).

13. *LinkedIn Corp. v. hiQ Labs, Inc.*, 141 S. Ct. 2752 (2021).

14. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1180, 1202–03 (9th Cir. 2022); *hiQ Labs, Inc. v. Linkedin Corp.*, 639 F. Supp. 3d 944, 958 (N.D. Cal. 2022).

15. *Id.* at 961, 965, 970.

16. Dull, *supra* note 4.

17. *hiQ Labs, Inc.*, 31 F.4th at1185.

doubts as to whether defendant (LinkedIn)'s revocation of permission to access the public portions of its site rendered the plaintiff's access "without authorization" within the meaning of the CFAA.[18]

This decision was affirmed by the Ninth Circuit, despite the recent Supreme Court decision.[19] The Supreme Court mainly relied on *Van Buren v. United States* in this decision. In *Van Buren*, the court decided for the CFAA, ruling that a person "exceeds authorized access" when they access files or other information that is off-limits to them on a computer system they otherwise have authorized access to.[20] The issue concerning *hiQ* was whether, once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data were "without authorization" within the meaning of the CFAA. Here, the panel concluded that "without authorization" was inapplicable, as prior authorization is not generally required in a case such as this—rather, a particular person is refused access.[21] The panel concluded that *Van Buren* reinforced this interpretation of the CFAA, even though *Van Buren* did not directly address the CFAA's "without authorization clause" but rather decided the statute exceeded the "authorized access clause."[22]

2. Breach of contract: Yes (November 4, 2022, District court mixed decision)

hiQ breached LinkedIn's User Agreement through a number of actions including scraping LinkedIn's website, and using that scraped data to create false identities on LinkedIn's platform. These actions are expressly prohibited by Section 8 of LinkedIn's User Agreement.[23] To create false identities, hiQ used temporary crowdsourced workers called "truckers." Although the truckers

18. *Id.* at 1188–89, 1191, 1197.
19. *Id.* at 1180, 1202–03.
20. *Van Buren v. United States*, 593 U.S. 374, 396 (2021).
21. *hiQ Labs, Inc.*, 31 F.4th at 1195.
22. *Id.* at 1183, 1198–99; *Van Buren*, 593 U.S. at 396.
23. *Id.* at 959, 961.

were hiQ's independent contractors, hiQ was not able to escape liability. The truckers acted as agents under hiQ's control in regards to the process of logging in to LinkedIn's website.[24]

3. Copyright infringement: Possible (April 2022 Ninth Circuit affirmation)

Following the Supreme Court decision, the Ninth Circuit noted that hiQ's copyright infringement remains a valid claim where a scraper is taking and repurposing copyrighted information.[25] In support of this view, the court cited to *Associated Press v. Meltwater U.S. Holdings, Inc.*, wherein the court held that a software company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use.[26]

4. Tort (trespass to chattels): Maybe applicable (April 2022 Ninth Circuit affirmation)

After the Supreme Court decision, the Ninth Circuit also noted that a scraper violating a cease-and-desist letter may still give rise to a common law tort claim for trespass. In the comment, the Ninth Circuit mentioned that a plaintiff's lack of consent is critical to any trespass claim.[27] As such, if a company operates a publicly accessible website, it should lay a clear marker that any potential scraping activity is not welcomed, both in its terms of service and via a cease-and-desist letter.

Several courts have weighed in on this issue, with mixed results. For example, in *eBay Inc. v. Bidder's Edge Inc.*, a federal district court found that scraping exceeded the scope of consent, establishing the likelihood of success on a trespass claim, because even though the website was publicly accessible, its servers were

---

24. *Id.*

25. Jason Russell & Matthew Tako, *Data scraping in a Post-hiQ World*, BLOOMBERG LAW (May 17, 2022), https://news.bloomberglaw.com/tech-and-telecom-law/data-scraping-in-a-post-hiQ-world.

26. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1202 (9th Cir. 2022) (citing *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013)).

27. *See id.* at 1202 n.21.

private property.[28] Therefore, scraping activity exceeded the scope of consent. Additionally, in *Register.com Inc. v. Verio Inc.*, the Second Circuit held that scraping constituted trespass because it could cause, even if it had not yet caused, physical harm to a company's servers.[29]

However, other courts found no trespass when no harm had occurred to the company's servers or computer operations. In both *Ticketmaster Corp. v. Tickets.Com Inc.* and *Intel Corp. v. Hamidi,* the courts held that mere scraping, without more, such as "actual or threatened injury" to property through damaging or interfering with a company's computer systems, did not rise to the level of trespass.[30]

C. hiQ's claims against LinkedIn and the court's final decision

1. Tortious interference with contract: Yes, but finally not clearly decided (November 4, 2022, District court mixed decision)

Ultimately, LinkedIn was not able to demonstrate a "legitimate business purpose" that could justify the intentional inducement of a contract breach.[31] Therefore, the court concluded that hiQ had brought into question the merits of its tortious interference with the contract claim.[32] Furthermore, on remand, the district court decided that litigation privileges applied in the case, so hiQ's tortious interference claim was barred.[33]

2. Unfair competition: Not decided (April 2022 Ninth Circuit affirmation)

In support of its unfair competition claim, hiQ presented evidence supporting its assertion that LinkedIn's decision to

---

28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.* at 1194.
32. *Id.*
33. *hiQ Labs, Inc. v. LinkedIn Corp.*, 639 F. Supp. 3d 944, 968 (N.D. Cal. 2022).

revoke hiQ's access to its data was made for the purpose of eliminating hiQ as a competitor in the data analytics field, thus potentially "violating the policy or spirit" of the Sherman Act.[34] While hiQ will have to do much more to prove such a claim, its arguments on the merits of its California's Unfair Competition Law (UCL) claim have done enough to support the issuance of a preliminary injunction.[35]

However, LinkedIn may well be able to demonstrate it was not motivated by anti-competitive purposes and that there is no threatened antitrust violation by claiming instead that it was motivated by a desire to preserve user privacy preferences and user trust. On remand, the Ninth Circuit did not reach hiQ's unfair competition claim, holding that a tortious interference claim is sufficient to support an injunction prohibiting LinkedIn from selectively blocking hiQ's access to public member profiles.[36] On remand, the district court decided that litigation privileges apply in this case, so hiQ's UCL claim was barred.[37]

3. Promissory estoppel: No violation (Initial and final District Court decision)

Another argument made by hiQ was for a preliminary injunction based on promissory estoppel.[38] The court noted that the claim appeared meritless because hiQ based its promissory estoppel argument on LinkedIn's alleged promise to its users that they control the visibility of their data.[39] In response, hiQ contended that LinkedIn reneged on that promise by restricting hiQ's access to data including data that was publicly available to all viewers.[40]

34. *hiQ Labs, Inc*, 31 F.4th at 1194 n.10.; *see also Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 973 P.2d 527, 544 (1999); *Web Scraping and Antitrust Law*, MCCARTHY LAW GROUP (Dec. 6, 2021), https://mccarthylg.com/web-scraping-and-antitrust-law/.

35. *hiQ Labs, Inc*, 31 F.4th at 1194 n.10.

36. *Id.* at 1194.

37. *hiQ Labs, Inc.*, 639 F. Supp. 3d at 968.

38. *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1118 (N.D. Cal. 2017), *aff'd*, 31 F.4th 1180 (2022).

39. *Id.* at 1118–19.

40. *Id.* at 1119.

The court rejected hiQ's argument, holding that LinkedIn's restrictions on hiQ's collection did not violate promises made to users for two reasons. First, the simple act of selecting the public profile setting does not mean that a user has consented to third-party collection and use of their data. Second, there was no indication that LinkedIn promised users that their data would be used for those purposes. Thus, LinkedIn's restrictions of hiQ's collection do not violate any promise made to LinkedIn's users[41]

4. Free speech: No violation (Initial and final District Court decision)

It was argued by hiQ that LinkedIn's actions violated California's constitutional free speech protections.[42] Article I, Section 2 of the California Constitution provides that "every person may freely speak, write, and publish his or her sentiments on all subjects."[43] The California Supreme Court has long recognized that this provision confers broader free speech rights than those provided by the First Amendment.[44] However, considering the potentially sweeping implications and the lack of any more direct authority, the court declined to conclude that hiQ had, at that juncture, raised "serious questions" that LinkedIn's conduct violated rights under the California Constitution.[45]

41. *Id.*

42. *Id.* at 1115.

43. *Id.*

44. *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1115 (citing *Dailey v. Superior Ct.*, 112 Cal. 94, 97–98 (1896)).

45. *Id.* at 1117.

COURT DECISIONS SUMMARY					
	District Court (Aug 17) for hiQ	9th (Sep 19) for hiQ	Supreme Court (Jun 21) for LinkedIn	9th (Apr 22) for hiQ	District Co (Nov 22) Mixed
LinkedIn Argument	**Defendant**	**Appellant**	**Appellant**		
1. CFAA - unauthorized access (civil and criminal liability) 18 U.S.C. § 1030(a)(2)(C).	X serious questions of applicability "Without authorization"	X serious questions of applicability for publicly available data	Van Buren: "exceeds authorized access"	X serious questions of applicability "Without authorization" inapplicable where prior authorization is not generally required	X
2. DMCA (copyright)				Maybe	
3. Unauthorized computer access					
4. Trespass				Maybe	
5. Misappropriation, unjust enrichment, conversion, breach of contract, breach of privacy				Maybe	O Breach of co
hiQ Argument	**Plaintiff**	**Appellee**	**Appellee**		
1. Tortious interference with contract	Overlaps with unfair competition			O Serious question raised "Support injunction"	CA's Litigat Preferenc
2. Unfair competition	O raised at least serious enough questions on the merits of its UCL claim at this juncture to support the issuance of a preliminary injunction.			Not reached	CA's Litigat Preferenc
3. Promissory estoppel	X Thus, LinkedIn's restrictions in hiQ's collection do not violate any promise made to its users.				
4. Free speech Art. I, Sec. 2 of California Constitution "every person may freely speak, write, and publish his or her sentiments on all subjects."	X lack of any more direct authority, the Court cannot conclude that hiQ has at this juncture raised "serious questions"				
5. Public interest	O For present purposes, the Court concludes that the public interest favors hiQ's position.				

III. RECENT CHARGES AGAINST SCRAPERS IN SOUTH KOREA

A. *Job Korea v. Saramin: scraping violates unfair competition law, but not copyright infringement (final court decision in 2017)*

1. Facts

In 58 instances, Saramin crawled[46] job information from Job Korea's website and posted it on its own website. Job Korea is an established online recruitment agency, using internet-based technology to provide job information and job placement services.[47] Saramin is an outsourcing and recruitment company that operates a job listing website which provides online information for domestic and foreign paid job postings.[48] In 2010, Job Korea sued Saramin and demanded a preliminary injunction at the Seoul Central District Court.[49] The critical issue was whether Job Korea's job information database (DB) was protected by copyright law.

2. Court's final decision

a. *Unfair competition violation: Yes*

Article 2, Subparagraph 1 item (k)[50] of South Korea's Unfair Competition Prevention Act stipulates that a person who gains

46. While web scraping is about extracting data from one or more websites, crawling is about finding or discovering URLs or links on the web. Usually, in web data extraction projects, you need to combine crawling and scraping. *See Web Scraping and Web Crawling*, ZYTE DEVELOPERS, https://www.zyte.com/learn/difference-between-web-scraping-and-web-crawling/ (last visited Oct. 28, 2024).

47. *See generally* JOBKOREA, https://www.jobkorea.co.kr/ (last visited Oct. 19, 2024).

48. *See Saramin HR Co, Ltd. Company Profile*, EMIS, https://www.emis.com/php/company-profile/KR/Saramin_Hr_CoLtd_en_3538922.html (last visited Oct. 18, 2024).

49. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Feb. 17, 2016, 2015Gahap517982 (S. Kor.).

50. Bujeonggyeongjaengbangji min yeongeopbimilbohoe gwanhan beomnyul [Law on the Prevention of Unfair Competition and the Protection of Trade Secrets] art. 2 subpara. 1 item (k) (S. Kor.) ("The act of illegally using information containing the technical or business ideas of others who have economic value in the transaction negotiation or transaction process, such as business offers, bidding, and public offerings,

another person's economic profit by using the results of another person's considerable investment or effort for one's own business in a way contrary to fair trade practices or competition order is constituting an infringement.[51] This infringement is defined as a type of unfair competition.[52]

The court decided that Saramin's act of unauthorized copying without extra cost constitutes an infringement of Job Korea's economic interest.[53] Saramin copied large quantities of the HTML source of Job Korea's website for commercial purposes, and posted it on its own website. This constituted using Job Korea's HTML source.[54] The HTML source is the result of considerable investment and effort generated by Job Korea's marketing and development expenses. For Saramin to use it for its own business is contrary to fair trade practices and/or competition order. Because Job Korea and Saramin both use employment information to conduct the same kind of business, Saramin's above actions resulted in benefits to Saramin, reducing marketing costs and increasing sales.[55] The plaintiff, Job Korea, suffered damages due to increased marketing expenses and an infringement of economic interests due to the reproduction of the HTML source.[56]

b. *Copyright infringement: No violation*

Article 2, subparagraph 1 of the South Korea's Copyright Act defines "work" as "a creative work belonging to the scope of

---

and providing them to others for the business interests of oneself or a third party. However, this is not the case if the person who received the idea was already aware of the idea at the time of the offer or if the idea is widely known in the same industry.") [hereinafter S. Kor. Unfair Competition Prevention & Trade Secret Protection Law].

51. Jay Yang et al., *Supreme Court Establishes Criteria for Application of the "Catch-All" Unfair Competition Provision,* KIM & CHANG (July 3, 2020), https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=21562.

52. *Id.*

53. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Feb. 17, 2016, 2015Gahap517982 (S. Kor.).

54. *Id.*

55. *Id.*

56. *Id.*

literature, computer works, or art."[57] In order to fulfill the "creativity" element, it must contain the expression of the author's own thoughts or feelings; it cannot be an imitation of someone else, but it doesn't have to be completely original.[58]

In *Saramin*, the court rejected the claim based on the following three points. First, the part of the text appearing on the screen among the HTML sources of Job Korea's website contains information related to recruitment provided by Job Korea.[59] This cannot be said to be an idea or emotion protected by copyright law.[60] Second, since the command part is just a tag describing the computer language for displaying recruitment information on the screen and does not seem to include a separate web programming element, it is difficult to see it as a creative expression worthy of copyright protection.[61] Third, based on the screen shown by the HTML source, the menu composition of recruitment-related information and the arrangement of information is very similar to the structure and contents of the original job posting website.[62] Therefore, it is challenging to admit that the HTML source is "creative."

57. Copyright Act, art. 2, para. 1 (S. Kor.), *translated in* Kora Legislation Research Institute's online database, https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=32626; *Id.*, art. 4, para. 1.

58. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan. 1, 2021, 2015No611 (S. Kor.) (finding the Copyright Act protects database creators who make significant human or material investments in their production, granting reproduction rights for substantial parts of the database, though protection is limited to five years and does not cover individual or insignificant parts to balance competition).

59. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Feb. 17, 2016, 2015Gahap517982 (S. Kor.) (finding the defendant unlawfully copied the HTML source using a crawling method, modified it, and used it to publish job information on their own website).

60. *Id.*

61. *Id.*

62. *Id.*

B. Yanolja v. GC Company (Good Choice): scraping violated unfair competition but no copyright infringement and criminal charges (incl. Information communication act) (2022)

1. Facts

GC Company conspired with a third-party from around June 1st to October 3rd of 2016 to crawl information from the communication network of Yanolja and infiltrate its API. During this period, it crawled 15,945,090 times without legitimate access.[63] Yanolja is a company that operates websites and mobile applications that provide accommodation information.[64] Similarly, GC Company is a company that operates a website and mobile application that provides lodging information.[65]

In early 2018, Yanolja filed a civil suit and a criminal complaint under the South Korean Data Copying Act.[66] Yanolja

---

63. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 25, 2022, 2021Na2034740 (S. Kor.); *see* Min-young Choi, *Hyeongsaneun mujoe, minsaneun "10eog baesang"... deiteo keulolling eodikkaji doena* [*Criminal: Not Guilty, Civil: "1 Billion Compensation"... How Far Does Data Crawling Go?*], HANKYOREH (Oct. 9, 2022), https://www.hani.co.kr/arti/society/society_general/1061963.html.

Application programming interface — a software intermediary that allows two applications to talk to each other. APIs are an accessible way to extract and share data within and across organizations. *Driving Business Growth Through Secure Integrations*, PWC (Sept. 29, 2023), https://www.pwc.com/ke/en/blog/driving-business-growth-secure-integrations.html.

64. Sun Lee, *Yanolja to Restructure Affiliates to Boost Profit Before Nasdaq IPO*, THE S. KOR. ECON. DAILY (Aug. 13, 2024), https://www.kedglobal.com/corporate-restructuring/newsView/ked202408130019.

65. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.] Jan. 13, 2021, 2020No611 (S. Kor.); *See* Hyeong Joo Lim, et al., *Korean Supreme Court Provides Clarity on Web Scraping and Violation of the Relevant Korean Laws, including the Copyright Act and Information Protection Act (Supreme Court, 2021Do1533, May 12, 2022)*, YULCHON LLC (July 20, 2022), https://www.yulchon.com/en/resources/publications/newsletter-view/32426/page.do.

66. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 19, 2021, 2018Gahap508729 (S. Kor.); *see* Lee, *supra* note 64 (detailing that Yanolja brought a criminal suit for the violation of the Copyright Act and the Criminal Code); *see also* Choi, *supra* note 63; *see also* Yoo Cheong-Mo, *Hotel Booking App Ordered to Compensate Rival for Alleged Info Theft*, YONHAP NEWS AGENCY (Aug. 23, 2021), https://en.yna.co.kr/view/AEN20210823005000315.

argued "[t]he information in question was created by their own efforts, including time and money, to provide added value to the information" and therefore not available to be duplicated by other entities such as GC Company.[67] However, the defendant's position was that "it is difficult to say that this data is copyrighted because the information is open to everyone," contending that there was no actionable claim.[68]

2. Court decision

After four years and eight months of litigation, the Yanolja court decided that there was not "unauthorized trespassing because the server was open."[69] However, with respect to the civil division, the court emphasized the importance of leading company's investment efforts and clarified the key to the crawling dispute was whether the Unfair Competition Prevention Act was violated.[70] The court decided in favor of the plaintiff, and awarded them 1 billion WON in compensation.[71]

a. Unfair competition: Yes

Yanolja, a leader in the online accommodation reservation service industry, has been collecting accommodation information for an extended period of time and continuously updates, verifies, and supplements the accommodation information database in its system.[72] The Seoul Central District Court decided that the information corresponds to the company's performance and that it cannot be regarded as a public domain that anyone can freely use.[73] GC Company's unauthorized copying, processing, and analysis of the information, with the purpose of understanding

---

67. Choi, *supra* note 63.

68. *Id.*

69. *Id.*

70. *See id.*

71. 1 billion WON is approximately 1 million USD. Lim, *supra* note 65.

72. *See generally Privacy Policy*, YANOLJA (May 14, 2021), https://global.yanolja.com/web/privacy (detailing how and why Yanolja collects user data).

73. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 19, 2021, 2018Gahap508729 (S. Kor.); *see* Choi, *supra* note 63.

and mimicking the sales strategy and current status of Yanolja, was an illegal violation Yanolja's economic interest.[74] Such an act constituted unfair competition as stipulated in Article 2, Subparagraph 1 (k) of the Act on the Prevention of Unfair Competition and Protection of Trade Secrets in South Korea.[75] The district court finally decided that Defendant (GC Company) was owed damages.[76]

b. Copyright Infringement: No reasonable infringement

However, the appellate court decided that GC Company only checked the whereabouts of some of Yanolja's databases and organized them into an Excel file.[77] There was no proof that they copied all, or even a significant part of Yanolja's business database.[78] It cannot be seen that GC Company's collection of indictment database items conflicts with the victim company's regular use of the database or is regarded as duplication of a substantial part that unreasonably harms the victim company's

74. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 19, 2021, 2018Gahap508729 (S. Kor.).

75. S. Kor. Unfair Competition Prevention & Trade Secret Protection Law, *supra* note 50 ("Data (among the data under subparagraph 1 of Article 2 of the Framework Act on the Promotion of the Data Industry and Utilization, it is provided to a specific person or a specific number of people as a business, and is accumulated and managed in a significant amount by electronic means, and is managed as confidential 1) Acquisition of data by a person without access authority by theft, fraud, unauthorized access, or other illegal means 2) A person who has access to data pursuant to a contractual relationship with the data holder uses or discloses the data for the purpose of obtaining unlawful profits or causing damage to the data holder, or a third party 3) Acquiring data knowing that 1) or 2) was involved, or using or disclosing the acquired data 4) Avoiding, removing, or changing technical protection measures applied to protect data without legitimate authority The act of providing, importing, exporting, manufacturing, transferring, lending, transmitting, or exhibiting for transfer or rental of technologies, services, devices, or parts of such devices, the main purpose of which is to incapacitate (hereinafter referred to as "incapacity"). However, this is not the case when devices or parts that neutralize technological protection measures are manufactured for research and development of technological protection measures.").

76. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 19, 2021, 2018Gahap508729 (S. Kor.).

77. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan 13, 2021, 2020No611 (S. Kor.).

78. *Id.*

interests.[79] Therefore, the appeals court found that GC Company did not infringe Yanolja's rights.

c. *Information and Communications Network Act: No violation*

The appellate court ruled that GC Company was not in violation of the former Information and Communications Network Act based on the prosecution's facts in this case. Here, it was unclear, based only on the evidence submitted by the prosecutor, that GC Company intruded upon the victim's information and communication network without or beyond the right of access.[80] In May of 2022, the Supreme Court affirmed the appellate court's decision.[81] The appellate court said that in a situation where Yanolja did not take any technical measures, like prohibiting access to servers, it is difficult to see that collecting information through methods such as crawling is an intrusion into an information and communication network without permission to access.[82] The prosecution appealed against the ruling, but the Supreme Court affirmed that the appellate court's judgment was correct and confirmed its innocence.[83]

IV. MAIN ISSUE: IMPORTANT FACTORS THE COURT MAY CONSIDER FOR THE CHARGE TO THE SCRAPER

Charges against a scraper are possible under unfair competition, copyright infringement, breach of contract, trespass,

79. *Id; see* Lim, *supra* note 65.

80. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan 13, 2021, 2020No611 (S. Kor.); *see* Lim, *supra* note 65.

81. Pierluigi Vinciguerra, *A Brief Wrap Up of The Latest News on Web Scraping*, SUBSTACK (Aug. 12, 2022), https://substack.thewebscraping.club/p/a-brief-wrap-up-of-the-latest-news (discussing the case of Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], May 12, 2022, 2021Do1533 (S. Kor.)).

82. Choi, *supra* note 63.

83. Daebeobwon [S. Ct.], May 12, 2022, 2021Do1533 (S. Kor.); Choi, *supra* note 63; see *generally* Vinciguerra, *supra* note 81 (explaining that the appellate court found the defendant, GC Company, not guilty, and that the Korean Supreme Court affirmed the decision).

and internet-related charges.[84] Here, the probable charges against the action of the platform to the scraper are an unfair competition violation and tortious interference with the contract.[85] The following analysis focuses on the charges against hiQ, Saramin, and GC Company as scrapers, and their relation to open banking liability.

A. Unfair competition: Yes: Saramin, GC Company

There are two important factors to analyze in determining whether the scraping action violates the unfair competition clause. First, there must be a significant investment or effort from another person.[86] In *Saramin*, the court decided that the unauthorized copying, without extra cost, constitutes an infringement of Job Korea's economic interest as this led to reduced marketing costs and an increase of sales for Saramin, and in the meantime, generated increased marketing expenses for Job Korea.[87] Second, the scraper must use the data illegally for its own business. In *GC Company*, the court held that processing and analyzing information that has been copied without authorization in order to understand the sales strategy and current status of GC Company violates the economic interest of Yanolja by using it illegally for GC Company's business, contrary to the law.[88]

---

84. These claims would be made under the CFAA in the US and under the Information and Communication Network Act in South Korea.

85. Unfair Competition Prevention and Trade Secret Protection Act, art. 2 para. 1 item (k), amended by Act. No. 18548, Dec. 7, 2021 (S. Kor.), translated in the Statutes of the Republic of Korea https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=62533&type=sogan&key=35 (search required).

86. *Id.*

87. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Feb. 17, 2016, 2015Gahap517982 (S. Kor.); *see* Ho-Jeong Jeong, *South Korea: Legal Standards in Korea for Permissible Web Crawling*, MONDAQ BUS. BRIEFING (Jan. 2, 2023), https://www.mondaq.com/copyright/1266552/legal-standards-in-korea-for-permissible-web-crawling#authors.

88. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Aug. 25, 2022 2021Na2034740 (S. Kor.); *see* Jeong, *supra* note 87.

B. Breach of contract: Yes: hiQ

Depending on whether the user agreement expressly prohibits scraping, a breach of contract claim could be valid. In *hiQ*, the court held that if the user agreement expressly prohibits scraping, the scraper will be held liable under breach of contract.[89] In *GC Company* and *Saramin*, this issue was not separately treated, but the *GC Company* court mentioned that the GC Company is not bound by the user terms because as the scraper it was not a user, and the user terms did not expressly prohibit the Application Programming Interface ("API")[90] server approach.[91]

C. Copyright Infringement: No violation: Saramin, GC Company; Possible: hiQ

Three important factors must be analyzed to decide whether scraping results in copyright infringement: (1) whether the scraped or crawled part was creative, (2) whether a significant part was copied, and (3) whether the scraping was fair use. In *Saramin*, the court held that the scraped job posting and HTML sources are general recruitment information, not protected under copyright law,[92] addressing the first factor. For the second factor, in *Yanolja*, there was no proof that they copied all or a significant part of the database, and therefore, there was no proof that they had unreasonably harmed the victim company's interest.[93] In South Korea, the Copyright Act includes a fair use doctrine and allows the possibility of exemption from the act of crawling,[94] which is the third factor to be analyzed. Although crawling may

89. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1201–1202 (9th Cir. 2022).

90. API: Application Programming Interface. *See What is an API (Application Programming Interface)?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/api/ (last visited Nov. 12, 2024).

91. Lim, *supra* note 65; *see* Jeong, *supra* note 87.

92. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Feb. 17, 2016, 2015Gahap517982 (S. Kor.); *see* Jeong, *supra* note 87.

93. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan 13, 2021, 2020No611 (S. Kor.); Jeong, *supra* note 87.

94. *Id.*

be exempted from liability under the Copyright Act for fair use, there are still possibilities of it being exposed to civil or criminal liabilities under other statutes.[95]

In the United States, one can still use copyrighted material on a limited scale under the fair use principle when one transforms the copyrighted material in a new or original way.[96] However, in *Associated Press v. Meltwater U.S. Holdings Inc.*, a federal district court in New York found that scraping copyrighted news articles and then repacking them in a subscription newsletter did not constitute fair use and was instead copyright infringement.[97] In *Meltwater*, the scraper tried to classify itself as a search engine to circumvent copyright laws.[98] But the court rejected the search engine classification, noting that the scraper was "an expensive subscription service" that was "neither designed nor operated to improve access to the complete, linked news story," nor was it a "publicly available tool to improve access to the content across the internet."[99]

D. Trespass: Possible: hiQ; No criminal charges: GC Company

Whether a scraper will be charged with trespassing depends on the existence of "consent." In hiQ, the court stated that a plaintiff's lack of consent is critical to any trespass claim.[100] As such, if a company operates a publicly accessible website, it should lay a clear marker that any potential scraping activity is not welcome, both in its terms of service and via a cease-and-desist letter.

However, whether harm or damage factors are critical is controversial. Some courts in the U.S. found no trespassing occurred when harm to the company's servers or computer

95. *Id.*

96. Vlad Krotov, Leigh Johnson & Leiser Silva, *Legality and Ethics of Web scraping*, 47 COMMC'NS ASS'N INFO. SYS. 539, 562 (2020).

97. Jason Russell & Matthew Tako, *Data Scraping in a Post-hiQ World*, TECH. & TELECOM. L. (May 17, 2022), https://www.skadden.com/-/media/files/publications/2022/05/data_scraping_in_a_post_hiq_world.pdf.

98. *Id.*

99. *Id.*

100. *hiQ Labs, Inc. v. LinkedIn Co.*, 31 F.4th 1180, 1195–96 (9th Cir. 2022).

operations did not occur.[101] Other courts like the Second Circuit held that scraping constituted trespass because it could, even if it had not yet, cause physical harm to a company's servers.[102] In *GC Company* and *Saramin*, trespass was not separately mentioned. The Supreme Court of Korea held in *GC Company* that there was no "disruption of work by computer," or in other words trespass because the server was open.[103]

E. Internet-related charges: No violation of Information and Communications Network Act; GC Company; No violation CFAA: hiQ

1. Without permission to access

The most important factor is whether the data is public and whether prior authorization is necessary. In *hiQ*, the court held that "without authorization" within the meaning of the CFAA was inapplicable.[104] There, hiQ's scraping activity after receiving the cease-and-desist letter was an activity where prior authorization was not generally required. Furthermore, in this case, a particular person was refused access rather than a general public access was declined.[105] In *GC Company*, the court decided "crawling public data" is not "without authorization" because no separate ID or password was necessary to receive the information.[106]

2. Exceeded authorization

Van Buren, cited by the Supreme Court in hiQ, clarifies that "exceeded authorization" does not apply when one has improper motives regarding information that is normally available to them;

101. *Id.* at 1201 n.21.

102. *Id.*

103. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan. 13, 2021, 2020No611 (S. Kor.); South Korean Criminal Law Section 314 (2).

104. *hiQ Labs, Inc.*, 31 F.4th at 1201.

105. *See id.* at 1195, 1201.

106. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan. 13, 2021, 2020No611 (S. Kor.).

rather, it only applies when one has improperly obtained information their normal computer access did not extend to.[107] In that case, a police officer using a system to retrieve license plate information for an improper purpose was allowed to do so, and it was decided that he had not exceeded authorization.[108]

In *GC Company*, the court decided that crawling public data does not fall under "exceeded authorization,"[109] as the command syntax of the API server used by the defendants was allowed by that server.[110] Even if the function, such as the search area range, was somewhat limited to the mobile app, it seemed to be set only for the convenience of the user. It cannot be seen that the access authority has been exceeded only by the fact that the search range has been expanded due to the user's need.

V. IMPLICATION FOR OPEN BANKING DATA POLICY IN THE U.S.

The recent court decision from *hiQ* has an important implication for the open banking framework in the U.S. The widespread use of scraping in financial payment systems in the U.S. faces a new risk from the country's market-driven approach.[111] In contrast, South Korea chose to rely on the government rather than litigation from the free market, which led to a limit on scraping in the financial payment systems.[112]

---

107. *hiQ Labs, Inc.*, 31 F.4th at 1198 (quoting *Van Buren v. U.S.*, 593 U.S. 374, 396 (2021)).

108. *Van Buren*, 593 U.S. at 396.

109. Seoul Jungang Jibangbeobwon [Seoul Cent. Dist. Ct.], Jan. 13, 2021, 2020No611 (S. Kor.).

110. *Id.*

111. David Strachan, *Open Banking Around the World: Toward a Cross-Industry Data Sharing Ecosystem*, DELOITTE, https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html (last visited Oct. 19, 2024).

112. *See, e.g.*, David Tost, *South Korea launches government-backed consumer finance data service*, GLOB. GOV'T FINTECH (Dec. 14, 2021), https://www.globalgovernmentfintech.com/south-korea-launches-government-backed-consumer-finance-data-service; *Opeunbaengking jeonmyeonsihaeng* [*Full Implementation of Open Banking*], GEUMYUNGWIWONHOE [FIN. SERVS. COMM'N] (Dec. 18, 2019) https://www.fsc.go.kr/comm/getFile?srvcId=BBSTY1&upperNo=74040&fileTy=ATTACH&fileNo=6.

A. Open Banking Regulation Status

To better meet their needs, consumers provide their financial service providers with data in a structural way; this is known as open banking.[113] This data sharing is done discretely and is reversible.[114] There are three types of financial data involved: Customer data, Transaction data, and Value-added customer data.[115] Open Banking regulation frameworks are divided into four categories worldwide: (1) mandated by the government, (2) policy currently being defined, (3) encouraged by the government, and (4) market-driven.[116] Although the U.S. and South Korea both primarily employ market-driven frameworks, South Korea additionally relies on some governmental encouragement to sustain this framework, while the U.S. generally does not.[117]

113. *Open Banking: Definition, How It Works, and Risks*, INVESTOPEDIA (May 10, 2024), https://www.investopedia.com/terms/o/open-banking.asp; *see also* COOPER, *supra* note 2, at 1.

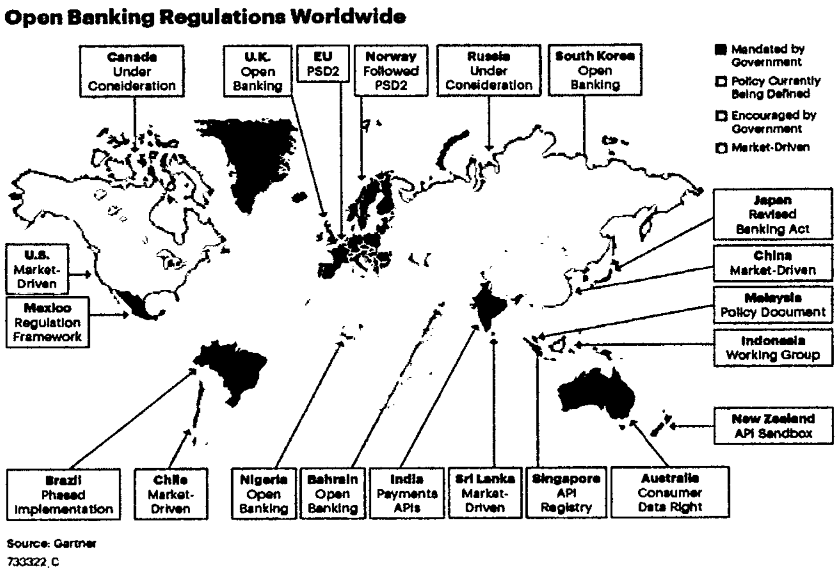
114. Tom Wijnen, *From Open Banking to Open Finance: Not if but When Does it Happen?*, THE PAYPERS: VOICE OF THE INDUS. (Feb. 14, 2023), https://thepaypers.com/thought-leader-insights/from-open-banking-to-open-finance-not-if-but-when-does-it-happen—1260341.

115. FDATA North America, *Opportunities in Open Banking*, FIN. DATA & TECH. ASS'N 7 (2019).

116. These four categories fall generally into two, broader categories of either market-driven or regulatory-driven frameworks. *See* David Strachan, *Open Banking Around the World, Towards a Cross-Industry Data Sharing Ecosystem*, DELOITTE, https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html (last visited Oct. 19, 2024).

117. *Id.*

Figure 1: OPEN BANKING REGULATIONS WORLDWIDE [118]



1. Status in the U.S.

The U.S. has not introduced separate regulations in the financial sector regarding open banking, but instead is operating on principles of information sharing to strengthen cooperation between banks and fintech companies at a market-autonomy level to prevent fraud.[119] Unlike the European or UK regulations in place, the American framework is different, as it is not mandatory.[120] Rather, it is verified by the financial institution itself and leverages third-party API access.[121] The right for customers to use their account information, such as for financial

118. Gartner, *Assess the Use of Banking API Standards for Competitive Advantage*, CURITY, https://curity.io/gartner-marketing/ (last accessed Feb. 16, 2025).

119. Casey Jennings & Jaimie Nawaday, *Open Banking is Coming to America*, JDSUPRA (Nov. 18, 2022), https://www.jdsupra.com/legalnews/open-banking-is-coming-to-america-9783680/.

120. *Id.*; *About Us*, U.K. GOVT.: COMPETITION & MKT. AUTH., https://www.gov.uk/government/organisations/competition-and-markets-authority/about (last visited Oct. 20, 2024).

121. Jennings & Nawaday, *supra* note 119.

transactions, is already protected under the Dodd-Frank Act, which was enacted in 2010.[122] Under the American framework, the Consumer Financial Protection Bureau (CFPB) respects consumers' right to the portability of financial data and their right to self-determination.[123] In 2017, the CFPB announced an outline of principles for collecting customer information.[124] The following year, the National Automated Clearing House Association (NACHA) announced the definition of a standard API for sharing account information, payment, fraud prevention, etc., with about 100 financial companies.[125] In 2020, the CFPB published an Advanced Notice of Proposed Rule Making and an Outline of Proposals and Alternatives in preparation for a Small Business Advisory Review Panel (SBREFA), which was issued on October 27, 2022.[126] Furthermore, the CFPB proposed a rule to permit Fintech's access to financial data in 2023,[127] and the final rule on that was expected in 2024.[128]

---

122. COOPER, *supra* note 2, at 2; Dodd-Frank Wall St. Reform & Consumer Prot. Act § 1033, 12 U.S.C. § 5533.

123. COOPER, *supra* note 2, at 2.

124. *Id.*

125. OPEUNBAENGKING, GEUM-YUNGSAN-EOB JIHYEONG BYEONHWAUI SEOMAG [OPEN BANKING, THE BEGINNING OF CHANGE IN THE LANDSCAPE OF THE FINANCIAL INDUSTRY], KPMG (2019), https://assets.kpmg.com/content/dam/kpmg/kr/pdf/2019/kr-issuemonitor-open-banking-20190524.pdf; *see Afinis Interoperability Standards: 2018 – The Year in Review*, NACHA (July 2, 2021), https://www.nacha.org/system/files/2019-05/Afinis-2018-Report-FINAL%20%281%29.pdf (highlighting the first two API use cases that NACHA released were "Get Bank Contact Information" and "Account Validation," which help verify account information to facilitate payments and prevent fraud).

126. *Required Rulemaking on Personal Financial Data Rights*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/personal-financial-data-rights/ (last visited Oct. 18, 2024); Vlad Macovei, *The Hopes and Limitations of Consumer Data Services in the US*, THE PAYPERS (Feb. 23, 2023), https://thepaypers.com/interviews/the-hopes-and-limitations-of-consumer-data-services-in-the-us—1261497.

127. *See* Evan Weinberger & Tonya Riley, *Banks, Fintechs Battle Over Customer Data in Open Banking Plan*, BLOOMBERG L. (Jan. 3, 2024), https://news.bloomberglaw.com/banking-law/banks-fintechs-battle-over-customer-data-in-open-banking-plan (stating that the CFPB's comment deadline for the open banking proposal was in December 2023, as the proposal was launched earlier that year).

128. Macovei, *supra* note 126.

2. Status in South Korea

The Financial Services Commission and the Bank of Korea agreed to legislate open banking in February of 2023.[129] Currently, open banking is operated according to the Korea Financial Telecommunications and Clearings Institute regulations, which were fully implemented on December 18, 2019.[130] On the second anniversary of these regulations, the number of open banking users reached 30 million.[131] The regulation states that bank and fintech operators can use the open banking system to conveniently develop information inquiry and transfer functions from bank accounts.[132] Furthermore, a revision of the Credit Information Act introduced "My Data" business; starting in 2019, its operators have received customer consent and conducted open banking to access customer information held by financial institutions.[133]

129. Okjin Bae, *Legalizing Open Banking*, ETNEWS (Aug. 29, 2022), https://www.etnews.com/20220829000166.

130. JBASEL COMM. ON BANKING SUPERVISION, BANK FOR INT'L SETTLEMENTS, DIGITALISATION OF FINANCE 6 (2024); *see S.Korea Launches "Open Banking" Services to Lower Fee, Enhance Convenience*, XINHUA (Dec. 18, 2019), http://www.xinhuanet.com/english/2019-12/18/c_138640557.htm.

131. *Open Banking Net Users Reach 30 Million at Two-year Anniversary*, FIN. SERV. COMM'N (Dec. 21, 2021), https://www.fsc.go.kr/eng/pr010101/77102.

132. *See Financial Information*, KOREAN FIN. TELECOMM. & CLEARINGS INST., https://eng.kftc.or.kr/business/financialInformation (last visited Nov. 1, 2024) (stating that open banking, a service available via financial institutions and fintech firms, allows customers to view financial information from different sources in one location); *see also* KOREA HERALD, *S. Korea Expands Open Banking Ecosystem, Invites Fintech Firms*, (July 28, 2021), https://www.koreaherald.com/view.php?ud=20210728000847 ("[U]sers of financial services provided by fintech businesses can also access the open banking platform, in which they can check balances of pre-paid accounts.").

133. HEUGJIN KWON, KOREAN INST. FIN., INTRODUCTION AND DEVELOPMENT DIRECTION OF OPEN BANKING (2020); *see* HYUNJU HELEN PAK, KYUNG HWA MOON & YUN HO CHOI, CHAMBERS GLOB. PRAC. GUIDES, BANKING REGULATIONS 4 (2021).

B. Analyzing the possible liabilities in open banking

1. Screen scraping

The original method for implementing open banking relationships between financial institutions and data aggregators[134] involved "screen scraping." Venmo (a platform owned by PayPal) is proof of the popularity of mobile payments that use screen scraping.[135] Using screen scraping, a consumer would be asked to provide her financial institution login credentials to a data aggregator, which would then use those credentials to periodically log in to the consumer's financial institution account to obtain financial data that would ultimately be displayed on the consumer's data aggregator account page.[136] Consumers were asked to turn over financial institution login credentials, effectively placing the entirety of their sensitive financial records at the disposal of the data aggregator.[137] Realizing the risk of data protection, the South Korean government banned screen scraping in open banking in January 2022, and changed to a linked method.[138] However, the recent

---

134. Data aggregation service is a type of data sharing service wherein consumers give the aggregator permission to access information across their financial accounts and put it into a standardized summarized form to help make it easier for consumers to manage their money (e.g., Mint, Yodlee). *See* Cheryl Cooper, *supra* note 2, at 1.

135. K, *supra* note 1.

136. *Id.*

137. Rich Zukowsky, *Open Banking, APIs, and Liability Issues*, DAVID WRIGHT TREMAINE LLP (Dec. 18, 2019), https://www.dwt.com/blogs/financial-services-law-advisor/2019/12/open-banking—liability.

138. Raon, *Korean MyData to be Fully Operational from January 2022*, MEDIUM (Aug. 16, 2021), https://medium.com/raonsecure/korean-mydata-to-be-fully-operational-from-january-2022-ba587f3996c3 (stating that the Korean Financial Services Commission of South Korea, the financial regulator responsible for protecting financial customers among its other objectives, adopted an API-based MyData service which banned the scraping method and made mandatory the use of the API-system for collecting consumer data); *see* Sangseung Oh et al., *New Sustainable Fintech Business Models Created by Open API Technology: A Case Study of Korea's Open Banking API Platform*, 16 SUSTAINABILITY 1, 15 (2024) (noting a network that links all banks directly).

proposal from CFPB does not ban data operators like Venmo from screen scraping.[139]

Screen scraping differs from web scraping in that its purpose is to obtain data from an application and display it on another interface.[140] As the consumer provides its login credentials to the data aggregator, in the process of screen scraping, trespass and criminal (CFAA) claims will not arise because the access was authorized. However, unfair competition, copyright infringement, and breach of contract claims might still be valid in situations where the use of data will be in dispute. Additionally, where there was unauthorized access, the consumer will be held liable for the charges.

2. API

APIs allow consumers to give financial institutions the right to share their economic data with aggregators through the use of 'tokens,' which only include a specific set of economic data. This system is considered much more secure than screen scraping, as consumers' data is more protected via tokens.[141] As this process does not involve a scraping process, an authorized transaction does not raise any issues mentioned above by screen and web scraping.[142] The CFPB released a list of frequently asked questions on electronic fund transfers in June 2021 that said banks are liable if consumers provide account credentials to a data aggregator that is subsequently hacked and allows

139. *See Journey From Screen Scraping to Open Banking More Marathon Than Sprint*, PYMTS (Jan. 3, 2024), https://www.pymnts.com/bank-regulation/2024/journey-from-screen-scraping-to-open-banking-will-be-more-marathon-than-sprint/ (critiquing the CFPB's proposed rule for merely diminishing reliance on screen scraping).

140. Chris Miranda, *Web Scraping vs Screen Scraping? Is There a Difference?*, PARSEHUB (May 28, 2021), https://www.parsehub.com/blog/web-scraping-vs-screen-scraping/; Stanley, *supra* note 2.

141. *Id.*

142. Unauthorized use triggers provisions of the Electronic Fund Transfer Act and Regulation E. *Id.*

unauthorized charges.[143] It is also important to note that, in South Korea, the liability lies in the platform (bank or fintech).[144]

Therefore, the API method, as used by Zelle, which is owned by seven major American banks and shared with other financial institutions, creates a more secure platform than Venmo (which uses scraping) from a data privacy perspective.[145] For the next step, APIs could be made available to Fintech companies like Venmo, they would no longer need to scrape, but could simply join the open API from Zelle. A good example of this is in South Korea, where open APIs are shared with 18 banks, 62 fintech, 73 secondary financial sectors, and 14 securities companies.[146] Although this step may increase the bank run risk, this would

143. Evan Weinberger, *Banks Seek Guidance on Who's Liable for Open Banking Data Fraud*, BLOOMBERG L. (Oct. 31, 2022), https://news.bloomberglaw.com/banking-law/banks-seek-guidance-on-whos-liable-for-open-banking-data-fraud.

144. Hanuel Kim, *Opeunbaengking seobiseu, jeonjageum-yungsago saeng-gimyeon?...chaeg-im sojaeneun 'peullaespomsa'* [*Open Banking Service, What If an Electronic Financial Accident Occurs? Who is Responsible? The 'Platform Company'*], MEDIAPEN (Oct. 31, 2019), http://www.mediapen.com/news/view/472933.

145. *See* Zukowsky, *supra* note 137; *A Safer Alternative to Financial Data Aggregation*, NINTH WAVE (Nov. 16, 2021), https://ninth-wave.com/blog/a-safer-alternative-to-financial-data-aggregation/ (using Zelle as an example how APIs work in banking); Lianna Norman, *Is Zelle safe? What to Know About the Consumer Financial Protection Bureau Scams Investigation*, FLORIDA TODAY (Aug. 14, 2024), https://www.floridatoday.com/story/news/2024/08/14/zelle-investigation-safety-which-banks-own-customer-disputes/74764704007/ (stating that a financial tech firm and consumer reporting agency that is co-owned by seven banks owns Zelle); *see generally* Spencer Tierney, *Banks That Use Zelle: List and What to Know*, NERDWALLET (Sara Clarke ed., Oct. 3, 2024), https://www.nerdwallet.com/article/banking/banks-that-use-zelle#zellelist (listing the participating banks and credit unions in Zelle's network); K, *supra* note 1 (noting that Venmo is a payment platform that utilized screen scraping).

146. *South Korea Regulators to Expand Open Banking Ecosystem*, FINTECH NEWS HONG KONG (Feb. 6, 2021), https://fintechnews.hk/14708/fintechkorea/south-korea-regulators-to-expand-open-banking-ecosystem (discussing that a goal for the South Korean open banking system is to be open to all licensed fintech companies and banks); Kim, *supra* note 144 (discussing the eighteen banks the Financial Services Commission announced to begin participating in the open banking customer services); Oh et al., *supra* note 138, at 9 (noting that the third-party financial service providers in South Korea consist of fifty three financial companies, fifty four big tech companies, and twenty-one small and medium sized fintech companies); Press Release, Financial Services Commission, Open Banking Services Available from Savings Banks (Apr. 28, 2021) https://www.fsc.go.kr/eng/pr010101/75825?srchCtgry=&curPage=&srchKey=sj&srchText=&srchBeginDt=2021-04-01&srchEndDt=2021-04-30.

lead the banks to consider adopting (or creating) other payment methods, like digital currencies.[147]

VI. CONCLUSION

Through *hiQ*, the validity of scraping was under review for over six years in the Ninth Circuit. Although the industry has changed since then, scraping has played a prolonged role in open banking. As financial institutions have more critical information than job carriers like LinkedIn, scrutiny over the validity of Venmo's scraping practices has increased. Besides the claim raised in *hiQ*, concerns about data abuse and hacking liability raise further First Amendment implications for scraping, as the risks fall on the customers. Considering the risks posed by the scraping method, it is strongly recommended that financial technologies like Venmo join the API systems of financial institutions like Zelle, which would help secure the First Amendment rights of its customers.

---

147. *See* Signe Krogstrup, et al., *Containing Technology Driven Bank Runs: AI, Social Media, And Mobile Banking May Bring More Bank Runs; Safeguards Of Yesterday May Not Be Sufficient Tomorrow*, FIN. & DEV. MAG., Mar. 2024, at 48, 48–51 (discussing that bank runs occur when a large number of a bank's customers withdraw their deposits simultaneously fearing that the bank may become insolvent or otherwise fail and that banks have considered implementing a central bank digital currency due to the increase use of electronic payments in lieu of cash).