

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

HIQ LABS, INC.,
Plaintiff,
v.
LINKEDIN CORPORATION,
Defendant.

Case No. [17-cv-03301-EMC](#)

**ORDER DENYING PLAINTIFF’S
MOTION FOR SUMMARY
JUDGMENT; GRANTING IN PART
AND DENYING IN PART
DEFENDANT’S MOTION FOR
SUMMARY JUDGMENT; DENYING
DEFENDANT’S MOTIONS TO
EXCLUDE; AND GRANTING IN PART
DEFENDANT’S MOTION FOR
SANCTIONS**

Docket Nos. 336-339, 355

I. INTRODUCTION

Before this Court are cross-motions for summary judgment. LinkedIn Corporation (“LinkedIn”) moves for partial summary judgment on its breach of contract claim and on hiQ Labs, Inc.’s (“hiQ”) tort claims. hiQ moves for partial summary judgment on its statute of limitations defense to LinkedIn’s claim under the Computer Fraud and Abuse Act (“CFAA”). Additionally, LinkedIn moves to exclude the expert testimony of Stephen McElfresh, to exclude the damages opinions of Benjamin Sacks, and to impose spoliation sanctions on hiQ for the destruction of electronically stored information. For the reasons below, the Court **GRANTS in PART and DENIES in PART** LinkedIn’s motion for partial summary judgment. It **DENIES** hiQ’s motion for summary judgment. The Court **DENIES** LinkedIn’s motions to exclude as moot and **GRANTS in PART** LinkedIn’s motion for sanctions.

1 scraping. (Docket No. 336-1 (“Lawit Decl.”) Ex. C (“User Agreement”) § 8.2.) The User
 2 Agreement seeks to govern both registered users and visitors. (*Id.* at § 1.2 (“[B]y . . . accessing or
 3 using our services . . . you are entering into a legally binding agreement.”).)

4 LinkedIn dedicates a team to prevent scraping on LinkedIn’s platform and deploys
 5 mechanisms to block data scrapers except for those with LinkedIn’s express permission to do so,
 6 such as the Google search engine. (Docket No. 29 (6/24/17 Rockwell Decl.) at ¶¶ 4, 12.) One
 7 such mechanism is LinkedIn’s “Anti-Abuse Infrastructure” and “Anti-Scraping Technical
 8 Strategy” that is effective at blocking scrapers without regard to or knowledge of their identities.
 9 (LCE 0010-12 (Bray Dep.); LCE 1298-1302 (Wu Dep.); LCE 1313-15 (Rockwell Decl.); LCE
 10 0810-11 (Murphy Rpt.)) LinkedIn also uses a “robots.txt” file—a technical protocol providing
 11 instructions to automated technologies visiting LinkedIn’s site. (6/24/17 Rockwell Decl. at ¶ 12.)
 12 Those instructions prohibit unauthorized access and warn that use of bots to access LinkedIn
 13 without express permission is strictly prohibited. (*Id.*; Countercl. at ¶ 33.) Entities seeking to
 14 crawl LinkedIn apply for permission and, if allowed, must abide by the terms of LinkedIn’s
 15 robots.txt and LinkedIn Crawling Terms and Conditions. (LCE 0812 (Murphy Rpt.))

16 B. hiQ

17 Founded in 2012 and dormant by 2019, hiQ was a “people analytics” company that
 18 provided information to businesses about their workforces. (FAC at ¶¶ 33, 34; Docket No. 23-4
 19 (6/22/17 Weidick Decl.) at ¶ 3; Docket No. 219-2 (9/24/21 Weidick Decl.) at ¶ 6.) It offered two
 20 products: “Keeper” and “Skill Mapper.” Keeper analyzed and predicted the retention risk for the
 21 employees of a given employer, and indicated which employees were at greatest risk of being
 22 recruited away. Employers could then develop action plans to retain its talent. (6/22/17 Weidick
 23 Decl. at ¶ 5.) “Skill Mapper” aggregated and summarized the breadth and depth of the skills
 24 possessed by an employer’s workforce by analyzing all of the skills its employees listed in their
 25 LinkedIn profile, including skills acquired from previous positions. Using this information,
 26 employers could build succession plans, drive employee engagement, promote internal mobility,
 27 and reduce costs associated with external talent acquisition. (*Id.* at ¶ 6.)

28 hiQ relied on LinkedIn for its data primarily by scraping wholly public LinkedIn profiles

1 using automated software. (FAC at ¶ 34; Docket No. 335-4 (Schmidt Decl.) Ex. A at 107–10,
2 Table 3.) hiQ had continuously attempted to circumvent LinkedIn’s general technical defenses
3 since May 2014. (Schmidt Decl. Ex. A at 42; LCE 0729 (randomly varied time delay); LCE
4 0703-04 (hiQ CTO Miller: “[w]hen we started to get blocked . . . we started doing business with
5 companies that provide libraries of IP addresses”).) It experimented and attempted to reverse
6 engineer LinkedIn’s systems and to avoid detection by simulating human site-access behaviors.
7 (LCE 0706, 0714-16 (Miller Dep.); LCE 1601-03 (notes on reverse engineering LinkedIn’s
8 systems); LCE 0730 (make requests in small sets; change user agent and cookies); LCE 0737-48
9 (Scraper Wars Presentation).) hiQ also hired independent contractors known as “turkers” to
10 conduct quality assurance while “logged-in” to LinkedIn by viewing and confirming hiQ
11 customers’ employees’ identities manually. (HCE Ex. 102 (turker training document).) When
12 LinkedIn’s general defenses restricted the turkers’ real accounts, hiQ instructed them to create
13 fake ones. (LCE 0148-49 (internal hiQ email).)

14 hiQ has known that LinkedIn prohibits scraping since at least 2015. (LCE 0927 (email to
15 hiQ then-CEO excerpting relevant portion of LinkedIn’s Use Agreement); LCE 0106-08 (Graves
16 Dep.)) It accepted LinkedIn’s User Agreement in running advertising and signing up for
17 LinkedIn subscriptions. (Lawit Decl. ¶¶ 7-8, Exh. J-M; LCE 0118-19 (Graves Dep.); LCE 0615
18 (Medeiros Dep.); Docket No. 327 at 15, 39 (hiQ Answer to Countercl.)) hiQ also was a LinkedIn
19 Member with a Company Page. (Docket No. 24 (hiQ Br.) at 12; Docket No. 327 at 15, 39 (hiQ
20 Answer to Countercl.) at 14; Lawit Decl. ¶ 5, Ex. I (record of hiQ company page).)

21 C. Pre-Litigation History And The Filing Of This Action

22 hiQ organized annual “Elevate” conferences for participants to share insights and best
23 practices in the people analytics field, as well as to market itself. (HCE Exs. 2-5, 14, 15.) Some
24 LinkedIn employees started discussing attending the Elevate conference as early as October 2014.
25 (HCE Ex. 91.) Between 2015 and 2017, LinkedIn employees attended, spoke at, and received
26 awards at these conferences. (HCE Ex. 81 (Reid Tr. 46:5-54:11); HCE Ex. 55 (“LinkedIn
27 Attendees at hiQ’s Elevate Conferences”); LCE 0062-63 (LinkedIn employee notes from
28 conference); HCE Ex. 75 (Jennings Dep. Tr.) at 65:14-66.3; HCE Ex. 56 (awards to LinkedIn

1 employees.)

2 hiQ began developing Skill Mapper in 2016 and planned to demonstrate it at the April 20,
3 2017 Elevate conference. (HCE Ex. 74 (Graves Dep. Tr.) at 80:21-81:9.) It, however, had trouble
4 scraping LinkedIn public profiles due to LinkedIn’s general technical defenses. (LCE 1174-75
5 (4/5/17 CEO Weidick email reporting technical and legal issues with scraping); LCE 1258
6 (Weidick email noting that the “first order of business is to get scraping up and running to some
7 viable place.”) hiQ was seeing ban rates of 99% or more. (LCE 0051 (ban rates between 99%-
8 100%); LCE 0770 (reporting ban rate greater than 99%).) During this time, hiQ’s data scientist
9 anonymously requested access to LinkedIn’s APIs, apparently on its CEO’s instruction, to “test[]
10 the water.” (LCE 1608 (Weidick email); LCE 0039-44 (Dev Dep.); LCE 1165-66 (Weidick
11 Dep.)) LinkedIn rejected the request. (LCE 0049-50.)

12 hiQ also experienced financial strains at that time. It had less than six months of cash left
13 before May 2017. (LCE 1150–51, 1161.) It had trouble renewing its existing customers—a
14 challenge that LinkedIn experienced also with its own product that competed with hiQ’s. (LCE
15 0673–76, 1288.) On May 15, 2017, hiQ’s Board of Directors met to consider a complete
16 reexamination of its business model. (LCE 1220–53.) hiQ, however, maintains that it was a
17 thriving startup on the cusp of its third and largest round of investor funding, “with more than a
18 dozen Fortune 500 clients, 23 employees, and a first-mover advantage in people analytics.”
19 (Docket No. 365-3 (“hiQ Opp.”) at 1.)

20 Around 2016 and 2017, LinkedIn was developing an offering known as “Talent Insights”
21 similar to hiQ’s Skill Mapper. In October 2016, LinkedIn’s Director of Analytics and Business
22 Development, Lorenzo Canlas, circulated screenshots of and notes on hiQ’s products—including
23 the then un-announced Skill Mapper—to the LinkedIn Talent Insights development team. (HCE
24 Ex. 59.) Canlas forwarded that team his invitation to hiQ’s 2017 Elevate Conference, reminded
25 them to attend, and noted that “hiQ will be unveiling their new skills mapped [sic] product if you
26 want to get some intel on similar products to [Talent Insights].” (HCE Ex. 27.) Before the
27 conference, LinkedIn internally identified hiQ as an “initial direct competitor” to Talent Insights.
28 (HCE Ex. 32.) After attending the conference, two Talents Insight team members shared their

1 notes on hiQ and noted that Skill Mapper “[wa]s powered mostly by scraped LinkedIn data.”
2 (HCE Ex. 29.) In response, LinkedIn’s Senior Director of Product Marketing, Kate Garvey asked
3 about “LinkedIn’s policy on blocking (soon-to-be) competitors from scraping our data.” (*Id.*)
4 Although LinkedIn generally did not “pursue cases of public profile scraping,” Eric Owski who
5 headed the Talent Insight’s team stated that he would “see if we push a bit harder.” (*Id.*) Ms.
6 Garvey responded that she was “a big fan of making my job easier by knocking out the
7 competition.” (*Id.*)

8 About a month after that email, on May 23, 2017, LinkedIn sent hiQ a cease-and-desist
9 letter that threatened action under the CFAA, the Digital Millennium Copyright Act (“DMCA”),
10 California Penal Code § 502(c), and the California common law of trespass. (HCE Ex. 17.) The
11 letter asserted hiQ’s unauthorized scraping of LinkedIn’s profiles violated the law. (*Id.*) It
12 advised hiQ LinkedIn had “restricted” hiQ’s company page and “ha[d] implemented technical
13 measures to prevent hiQ from accessing, and assisting others to access, LinkedIn’s site, through
14 systems that detect, monitor, and block scraping activity.” (*Id.*) According to hiQ, these actions
15 by LinkedIn were part of a larger plan to “collect competitive intel from hiQ then shut down its
16 business,” once LinkedIn identified hiQ as a competitor. (hiQ Opp. at 5.)

17 In response to the cease-and-desist letter, hiQ demanded that LinkedIn recognize its right
18 to access LinkedIn’s public pages. (FAC at ¶¶ 42-43.) LinkedIn refused. (*Id.* at ¶ 44.) hiQ
19 subsequently sued LinkedIn, seeking injunctive relief based on California law and a declaratory
20 judgment that LinkedIn could not lawfully invoke the CFAA, the DMCA, California Penal Code §
21 502(c), or the common law of trespass against it. (Docket No. 1.) Additionally, it asserted against
22 LinkedIn tortious interference claims, claims under the California Unfair Competition Law
23 (“UCL”), promissory estoppel, and violation of right to free speech under the California
24 Constitution. (*Id.*) hiQ concurrently filed a request for a temporary restraining order that the
25 parties later agreed to convert into a motion for a preliminary injunction. (Docket No. 23.)

26 D. Preliminary Injunction

27 On August 14, 2017, this Court granted hiQ’s motion for a preliminary injunction.
28 (Docket No. 63.) It credited hiQ’s assertion that the survival of its business was threatened absent

1 a preliminary injunction. (*Id.* at 5.) It determined that the balance of hardships tipped sharply in
2 hiQ’s favor because LinkedIn’s interest in preventing hiQ from scraping the public profiles of
3 LinkedIn’s members did not outweigh hiQ’s interest in continuing its business. (*Id.* at 7–8.) The
4 Court held that hiQ raised at least serious questions going to the merits of its California UCL
5 claims and the applicability of the CFAA, but not the promissory estoppel and free speech claims.
6 (*Id.* at 16, 20–21, 23.) Finally, the Court determined that the public interest favored hiQ because
7 giving companies like LinkedIn free rein to decide who could collect and use data otherwise
8 available to the public risked the possible creation of information monopolies. (*Id.* at 24.)

9 The Court ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing
10 technical barriers to hiQ’s access to LinkedIn members’ public profiles, and to refrain from
11 erecting any legal or technical barriers that block hiQ’s access to those profiles. (*Id.* at 25.)

12 E. hiQ’s Business Post-Injunction

13 After this Court issued the preliminary injunction, hiQ’s business diminished significantly
14 because of, according to hiQ, “the cloud of uncertainty caused by LinkedIn’s conduct [that]
15 lingered over the business.” (Docket No. 219-2 (Weidick Decl.) at ¶ 4.) hiQ lost out on funding
16 from investors, all of its employees left, and it could no longer solicit new clients or renew current
17 client contracts. (*Id.*)

18 hiQ wound down its operations in 2018, though its servers continued running into 2019 to
19 deliver on client contracts. (*Id.* at ¶ 6.) hiQ let lapse its accounts with several cloud service
20 providers key to hiQ’s business, including Salesforce that stored its client data, and Splunk and
21 Amazon Web Services that stored its scraping data.

22 F. LinkedIn’s Appeal Of The Injunction

23 LinkedIn appealed this Court’s preliminary injunction order in September 2017 and the
24 parties stipulated to stay all interim deadlines. (Docket No. 80.) The Ninth Circuit upheld this
25 Court’s order in September 2019. *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1004 (9th Cir.
26 2019) (“*hiQ I*”).

27 LinkedIn then filed a petition for writ of certiorari to the United States Supreme Court.
28 (Docket No. 129.) The Supreme Court granted the petition, vacated the judgment, and remanded

1 this case for further consideration in light of *Van Buren v. United States*, 141 S. Ct. 1648 (2021).
2 *See LinkedIn Corp. v. hiQ Labs, Inc.*, 141 S. Ct. 2752 (2021).

3 The Ninth Circuit again affirmed the preliminary injunction. *See hiQ Labs, Inc. v.*
4 *LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022) (“*hiQ II*”). It concluded that *Van Buren* reinforced
5 its determination that hiQ has raised serious questions about whether LinkedIn may invoke the
6 CFAA to preempt hiQ’s possibly meritorious tortious interference claim under California Unfair
7 Competition Law. *Id.* at 1180.

8 G. Post-Preliminary Injunction Procedural History In This Court

9 On February 14, 2020, three months after the issuance of *hiQ I* and before LinkedIn
10 petitioned for writ of certiorari, hiQ filed its Amended Complaint. It alleged, *inter alia*, that
11 “LinkedIn effectively eviscerated hiQ’s business,” that hiQ lost most of its employees, was unable
12 to find further investors, and lost major clients, and that it “has largely been forced out of business
13 entirely.” (FAC at ¶¶ 45, 81.) Compared to the original complaint, the FAC removed the
14 promissory estoppel and free speech claims and added antitrust claims under Sections 1 and 2 of
15 the Sherman Act. (*Id.* at ¶¶ 109-168.)

16 On April 14, 2021, LinkedIn moved to dismiss certain claims in the FAC. (Docket No.
17 137.) The Court granted that motion in part. (Docket No. 158.) It denied LinkedIn’s motion to
18 dismiss the tortious interference claims as they were not barred by the *Noerr-Pennington* doctrine
19 or the California Litigation privilege. (*Id.*) It dismissed the antitrust claims because hiQ failed to
20 allege anticompetitive conduct. (*Id.*) The Court granted hiQ leave to amend its antitrust claims to
21 the extent they are based on the theories of unilateral refusal to deal and the essential facilities
22 doctrine. (*Id.*) hiQ subsequently declined to amend the pleadings. (Docket No. 163.)

23 After LinkedIn learned about hiQ’s dormancy, it filed a motion to dissolve the preliminary
24 injunction. (Docket No. 216.) On August 1, 2022, this Court dissolved the preliminary
25 injunction, holding that LinkedIn had established a significant change in facts by showing that hiQ
26 no longer had an ongoing business. (Docket No. 329.)

27 ///

28 ///

1 A. Breach Of Contract

2 LinkedIn moves for partial summary judgment on its breach of contract claim for (1) hiQ’s
3 scraping of LinkedIn’s site and using the collected data to sell its Keeper and Skill Mapper
4 products, and (2) hiQ’s use and for directing “turkers” to make fake accounts and to copy url data
5 as part of hiQ’s scraping operation. hiQ only contests the breach and damages elements.
6 Specifically, as to the first accused conduct, hiQ argues that questions of fact remain as to whether
7 the User Agreement is ambiguous and consequently whether hiQ breached that Agreement. For
8 the turkers’ actions, hiQ argues that they did not constitute a breach that resulted in damages and
9 that it was not responsible for them. hiQ also argues that its affirmative defenses bar the breach
10 claim.

11 1. Liability

12 a. Scraping and Using Collected Data

13 LinkedIn’s User Agreement expressly prohibits scraping of its site. Section 8 of the User
14 Agreement (“LinkedIn ‘DOs’ and ‘DON’Ts”) states:

- 15 8.2 Don’ts. You agree that you will not:
- 16 ...
- 17 • Scrape or copy profiles and information of others through
18 any means (including crawlers, browser plugins and add-ons,
and any other technology or manual work);
 - 19 ...
 - 20 • Use manual or automated software, devices, scripts[,] robots,
21 other means or processes to access, “scrape,” “crawl” or
“spider” the Services or any related data or information;
 - 22 • Use bots or other automated methods to access the Services,
23 add or download contracts, send or redirect messages;
 - 24 ...

25 As relevant to hiQ’s argument, the User Agreement also delineates members’ rights and
26 obligations as follows:

27 2. Obligations

28 ...

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

When you share information, others can see, copy and use that information.

...

3.1 Your License to LinkedIn

...

c. We will get your consent if we want to give others the right to publish your posts beyond the Service. However, other Members and/or Visitors may access and share your content and information, consistent with your settings and degree of connection with them.

...

Despite the clear language cited above, hiQ argues that LinkedIn’s User Agreement was nonetheless ambiguous because of (1) inconsistent provisions within the Agreement, and (2) extrinsic evidence, including LinkedIn’s conduct which suggested that scraping was not categorically barred.

“Whether language in a contract is ambiguous is a question of law to be answered by the court.” *Coremetrics, Inc. v. Atomic Park.com, LLC*, No. C-04-0222 EMC, 2005 WL 3310093, at *3 (N.D. Cal. Dec. 7, 2005); accord *Abifadel v. Cigna Ins. Co.*, 8 Cal. App. 4th 145, 159 (1992). However, extrinsic evidence may be required to determine the intent of the parties to the contract. *Abifadel*, 8 Cal. App. 4th at 159. The usual formula under California law when determining whether to admit parol evidence is as follows:

First, the court provisionally receives (without actually admitting) all credible evidence concerning the parties’ intentions to determine “ambiguity,” whether the language is “reasonably susceptible” to the interpretation urged by a party. If in light of the extrinsic evidence the court decides the language is “reasonably susceptible” to the interpretation urged, the extrinsic evidence is then admitted to aid in the second step—interpreting the contract.

Winet v. Price, 4 Cal. App. 4th 1159, 1165 (1992) (citing *Blumenfeld v. R. H. Macy & Co.*, 92 Cal. App. 3d 38, 45 (1979)). The threshold issue of whether the parol evidence is necessary to determine the meaning of the language is a question of law. *Id.* Similarly, “when the parol evidence is not conflicting,” construction of the contract is a question of law. *Id.*

User Agreement Provisions. Contrary to hiQ’s characterization, the User Agreement’s

1 provisions do not conflict with each other. According to hiQ, the User Agreement’s statements
 2 that “Visitors may access and share your content and information consistent with your settings”
 3 and that “[w]hen you share information, others can see, copy and use that information” are
 4 inconsistent with the prohibition of scraping data—a means to access and copy LinkedIn
 5 members’ information. (User Agreement §§ 2, 3.1.) Thus, hiQ argues that the inconsistency
 6 creates a question of fact as to whether its conduct constitutes a breach of the User Agreement.

7 The Court disagrees. Informing members that their data may be “see[n], cop[ied], and
 8 use[d]” does not contradict the prohibition against “scrap[ing], crawl[ing], or spider[ing] the
 9 Server.” (User Agreement §§ 2, 8.2.) The two concepts are not mutually exclusive—a warning to
 10 members that a third party may collect their public-facing data is not a blessing for third parties to
 11 do so through expressly prohibited means. Thus, the contract’s language itself does not create
 12 ambiguity within the User Agreement.

13 ***Extrinsic Evidence.*** hiQ’s extrinsic evidence includes an internal email between LinkedIn
 14 employees stating that LinkedIn “generally do[es]n’t pursue cases of public scraping,” the fact that
 15 LinkedIn scraped its competitor’s websites, and the fact that LinkedIn’s parent company scraped
 16 LinkedIn. (hiQ Opp. at 13 (citing HCE Ex. 29, 80, 47).) Also, hiQ argues that LinkedIn’s non-
 17 enforcement implied that the agreement does not bar scraping.

18 However, “parol evidence is admissible only to prove a meaning to which the language is
 19 ‘reasonably susceptible,’ not to flatly contradict the express terms of the agreement.” *Winet*, 4
 20 Cal. App. 4th at 1167 (emphasis added) (citations omitted). hiQ seeks to introduce parol evidence
 21 to prove that it may “[u]se manual or automated software, devices, scripts[,], robots . . . to access,
 22 ‘scrape,’ ‘crawl’ or ‘spider’ the [LinkedIn] Services” even though the User Agreement says hiQ
 23 “agree[d] that [it] will not” do so. (User Agreement § 8.2.) That extrinsic evidence does not
 24 negate or diminish the express terms of the User Agreement. Furthermore, LinkedIn’s failure to
 25 abide by or enforce the Agreement, which perhaps gives rise to an affirmative defense, does not
 26 contradict or render ambiguous the unambiguous terms of the Agreement.

27 In sum, the relevant language of the User Agreement unambiguously prohibits hiQ’s
 28 scraping and unauthorized use of the scraped data.

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

b. Turkers

hiQ argues against liability for the turkers’ conduct because (1) no evidence shows that the turkers ever scraped any profile information, (2) it is not responsible for its independent contractors’ acts, and (3) no evidence shows actual harm.

Undisputed evidence shows that hiQ’s turkers registered false LinkedIn identities under its instructions in breach of the User Agreement. Section 8 of the User Agreement (“LinkedIn ‘DOs’ and ‘DON’Ts”) states:

8.2 Don’ts. You agree that you will not:

...

- Create a false identity on LinkedIn;

...

(*Id.* at § 8.2.) hiQ’s turker training document for the Keeper product explicitly instructed, “It is a good idea to make a fake account with a fake email, to deal with the possibility of being banned on LinkedIn.” (LCE 0150-51 (“turk instructions redux”); LCE 0118-19, 0124-25 (Graves Dep. Tr.)) Undisputed evidence suggests that turkers followed this instruction. (*See* LCE 0124 (Graves Dep. Tr.)) Regardless of whether the turkers scraped LinkedIn’s site, they breached the User Agreement’s prohibition on creating false identities.

Although turkers were hiQ’s independent contractors, hiQ cannot escape liability because they also acted as its agent regarding the log-in process to LinkedIn. *See City of Los Angeles v. Meyers Bros. Parking Sys., Inc.*, 54 Cal. App. 3d 135, 138 (1975) (“[A]n agent may also be an independent contractor.”). “[T]he difference between an agent and an independent contractor is primarily the degree of retained control.” *Park v. Burlington N. Santa Fe Ry. Co.*, 108 Cal. App. 4th 595, 613 (2003). “Ordinarily, the question of agency is one of fact,” but “where the evidence is undisputed the issue becomes one of law.” *Magnecomp Corp. v. Athene Co.*, 209 Cal. App. 3d 526, 536 (1989).

Here, undisputed evidence shows that hiQ retained a high degree of control over turkers’ log-in process. Its training documents provided suggestions on how to log into LinkedIn’s accounts. (*See, e.g.*, LCE 0151 (“It is a good idea to make a fake account with a fake email, to

1 deal with the possibility of being banned on LinkedIn.”); HCE Ex. 102 (“Log into linkedin.com,
2 you may want to create new accounts for turking to avoid having your account harassed. It is
3 important that you are browsing anonymously.”).) When LinkedIn “cracked down on usage in a
4 way that [wa]s making problems for turking,” hiQ “instruct[ed] turkers on how to proceed.” (LCE
5 1048 (hiQ email).) hiQ itself considered the turkers their agents. (LCE 0328 (hiQ internal email
6 stating, “by turking *we* may be violating some of [LinkedIn’s] terms of use, such as the
7 requirement that users of LinkedIn don’t create false identities and will use their real names on
8 their profiles”) (emphasis added).) hiQ has not pointed to contrary evidence regarding its control
9 over the turkers’ logging in process. There is no dispute then that turkers thus acted as hiQ’s
10 agents and their liabilities accrue to it. *See* Cal. Civ. Code § 2330 (“An agent represents his
11 principal for all purposes within the scope of his actual or ostensible authority, and all the rights
12 and liabilities which would accrue to the agent from transactions within such limit, if they had
13 been entered into on his own account, accrue to the principal.”).

14 Finally, although hiQ contends LinkedIn suffered no damages from turkers’ actions,
15 “nominal damages are available for breach of contract and can support entry of judgment in favor
16 of a plaintiff who suffered ‘no appreciable harm.’” *Meta Platforms, Inc. v. BrandTotal Ltd.*, No.
17 20-CV-07182-JCS, 2022 WL 1990225, at *22–23 (N.D. Cal. June 6, 2022) (quoting *Elation Sys.,*
18 *Inc. v. Fenn Bridge LLC*, 71 Cal. App. 5th 958, 965–66 (2021)). hiQ has therefore breached
19 LinkedIn’s User Agreement through the turkers’ conduct.

20 c. Summary

21 In sum, hiQ breached LinkedIn’s User Agreement both through its own scraping of
22 LinkedIn’s site and using scraped data, and through turkers’ creation of false identities on
23 LinkedIn’s platform.

24 2. Affirmative Defenses

25 a. Unclean Hands

26 hiQ asserts that LinkedIn “dirtied its hands” by bringing “its breach of contract claim as
27 part of its plan to ‘cut off’ hiQ’s access to otherwise public data and put hiQ out of
28 business.” (hiQ Opp. at 10 (internal citation omitted).) LinkedIn responds that the alleged

1 misconduct does not directly affect hiQ’s obligations under the User Agreement, but merely
2 enforces LinkedIn’s bargained-for rights.

3 In California, “unclean hands is available as an affirmative defense to a contract claim.”
4 *Cal-Agrex, Inc. v. Tassell*, 258 F.R.D. 340, 348, n.2 (N.D. Cal. 2009) (citing *Camp v. Jeffer*,
5 *Mangels, Butler & Marmaro*, 35 Cal. App. 4th 620, 638 (1995)). “Whether the particular
6 misconduct is a bar to the alleged claim for relief depends on (1) analogous case law, (2) the
7 nature of the misconduct, and (3) the relationship of the misconduct to the claimed injuries.” *E.*
8 *W. Bank v. Rio Sch. Dist.*, 235 Cal. App. 4th 742, 751 (2015) (citation omitted). hiQ has cited no
9 analogous case law supporting the application of the unclean hands defense to the facts present
10 here. Failing to meet the first prong of the three-part test “alone is sufficient to warrant the denial
11 of the defense.” *Id.* at 751–52 (holding unclean hands does not apply as a matter of law “because
12 there is no analogous case applying the doctrine” to facts there). Therefore, the Court grants
13 summary judgment on hiQ’s unclean hands defense in favor of LinkedIn.

14 b. Waiver

15 “Under California law, a party to a contract waives a contractual right by ‘indicating an
16 intent to relinquish the right.’” *Williams v. Apple, Inc.*, 338 F.R.D. 629, 646 (N.D. Cal. 2021)
17 (quoting *Wind Dancer Prod. Grp. v. Walt Disney Pictures*, 10 Cal. App. 5th 56, 78 (2017)). “The
18 waiver may be either express, based on the words of the waiving party, or implied, based on
19 conduct indicating an intent to relinquish the right.” *Wind Dancer*, 10 Cal. App. 5th at 78 (internal
20 quotations and citations omitted). “The waiver may be . . . implied . . . when that party’s acts are
21 so inconsistent with an intent to enforce the right as to induce a reasonable belief that such right
22 has been relinquished.” *Id.* Thus, “the pivotal issue in a claim of waiver is the intention of the
23 party who allegedly relinquished the known legal right.” *Id.* (internal quotations and citations
24 omitted). “Waiver is ordinarily a question of fact unless ‘there are no disputed facts and only one
25 reasonable inference may be drawn.’” *Id.* (quoting *DuBeck v. Cal. Physicians’ Serv.*, 234 Cal.
26 App. 4th 1254, 1265 (2015)).

27 As discussed below for hiQ’s summary judgment motion, there is a genuine dispute of
28 material fact as to whether LinkedIn knew about hiQ’s scraping and use of scraped data as early as

1 October 2014. If it did, a reasonable jury could find that LinkedIn relinquished its enforcement
2 against hiQ’s scraping through its conduct—aside from generally deploying anti-scraping
3 technology against all scrapers, it did not take steps to legally enforce against known scraping by
4 hiQ for years, and it allowed its employees to attend hiQ’s conferences. Therefore, summary
5 judgment is improper for the waiver defense for hiQ’s scraping and unauthorized data usage.

6 There is no evidence, however, showing that LinkedIn knew about hiQ’s use of turkers
7 before this action, so LinkedIn could not have relinquished its right to enforce the User
8 Agreement’s provision prohibiting the creation of false identities. The Court therefore grants
9 summary judgment for the waiver defense on that conduct.

10 c. Estoppel

11 The doctrine of estoppel generally requires the following elements: (1) “the party to be
12 estopped must be apprised of the facts;” (2) “he must intend that his conduct shall be acted upon,
13 or must so act that the party asserting the estoppel had a right to believe it was so intended;” (3)
14 “the other party must be ignorant of the true state of facts;” and (4) “he must rely upon the conduct
15 to his injury.” *Lentz v. McMahon*, 49 Cal. 3d 393, 399 (1989).

16 Regarding hiQ’s scraping and use of scraped data, there remains a genuine dispute of
17 material fact as to all four elements. As explained in hiQ’s summary judgment below, LinkedIn
18 might have known about hiQ’s conduct in 2014. Viewed in the light most favorable to hiQ,
19 LinkedIn employees’ participation in hiQ’s Elevate conferences where hiQ discussed its products
20 led hiQ to believe that LinkedIn acquiesced in its circumvention of LinkedIn’s general defense
21 mechanisms to scrape public profiles. A reasonable jury could find that hiQ relied on such
22 acquiescence in developing its business over the years with near total dependency on LinkedIn.
23 The Court thus denies summary judgment on the estoppel defense regarding hiQ’s scraping and
24 use of scraped data.

25 Regarding hiQ’s use of turkers, there is no evidence that LinkedIn was apprised of
26 relevant facts as explained above. The Court therefore grants summary judgment on estoppel for
27 that conduct.

28

1 d. Unconscionability

2 hiQ raises the affirmative defense of unconscionability for the first time in its opposition
3 brief, arguing that the User Agreement is procedurally and substantively unconscionable.
4 LinkedIn responds that (1) hiQ has waived this affirmative defense by failing to plead it in hiQ's
5 answer, and that (2) even if not waived, hiQ cannot establish unconscionability.

6 LinkedIn has not shown prejudice from hiQ's belated assertion of unconscionability, so
7 hiQ has not waived this affirmative defense. *See Camarillo v. McCarthy*, 998 F.2d 638, 639 (9th
8 Cir. 1993) (absent prejudice, an affirmative defense may be raised for the first time at summary
9 judgment); *Mir v. Levine*, 745 F. App'x 726, 727 (9th Cir. 2018) (absent showing of prejudice, no
10 waiver of defendants' collateral estoppel defense even though it was not raised until summary
11 judgment). The Court therefore analyzes hiQ's defense on the merits.

12 "Unconscionability has both a procedural and a substantive element, the former focusing
13 on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided
14 results." *Lennar Homes of Cal., Inc. v. Stephens*, 232 Cal. App. 4th 673, 687 (2014) (internal
15 quotations and citations omitted). "The prevailing view is that procedural and substantive
16 unconscionability must both be present in order for a court to exercise its discretion to refuse to
17 enforce a contract or clause under the doctrine of unconscionability;" however, "they need not be
18 present in the same degree." *Id.* (emphasis in original). Rather, courts apply a "sliding scale" to
19 determine unconscionability. *Id.* "The more substantively oppressive the contract term, the less
20 evidence of procedural unconscionability is required to come to the conclusion that the term is
21 unenforceable, and vice versa." *Id.* at 687–88 (internal quotations and citations omitted).
22 "Substantive unconscionability addresses the fairness of the term in dispute" and "traditionally
23 involves contract terms that are so one-sided as to 'shock the conscience,' or that impose harsh or
24 oppressive terms." *Wherry v. Award, Inc.*, 192 Cal. App. 4th 1242, 1248 (2011) (quoting *Szetela*
25 *v. Discover Bank*, 97 Cal. App. 4th 1094, 1100 (2002)).

26 hiQ seeks to establish substantive unconscionability by arguing that LinkedIn's prohibition
27 on "copying profiles" is "incompatible with simply visiting the website." (hiQ Opp. at 12.) It
28 points to evidence that LinkedIn cannot distinguish between a request for profile data from human

1 users and that from scrapers. (HCE Ex. 71 (Bray 7/27/2022 Dep. Tr.) at 233:24-234:1.) That
 2 means, after receiving a request from a web browser, LinkedIn’s server returns a copy of the
 3 HTML code to human users and scrapers alike. Therefore, hiQ reasons, every visitor of
 4 LinkedIn’s site violates the prohibition against “copy[ing] profiles and information through . . .
 5 any . . . technology.” (User Agreement § 8.2.)

6 hiQ does not contend that the prohibition against the conduct at issue here—scraping,
 7 using scraped data without consent, and creating false identities—is unconscionable as a general
 8 matter. Its attack on the conscionability is based on a circumstance not applicable here—merely
 9 visiting LinkedIn’s site. hiQ would have the Court construe LinkedIn’s User Agreement as
 10 prohibiting anyone from ever using its own service. No reasonable user would so interpret the
 11 User Agreement. hiQ thus fails to offer any evidence supporting substantive unfairness of the
 12 User Agreement.

13 Absent substantive unconscionability, the Court needs not consider procedural
 14 unconscionability. The Court grants LinkedIn’s motion for summary judgment on this affirmative
 15 defense.

16 e. Other Affirmative Defenses

17 LinkedIn moves for summary judgment on hiQ’s affirmative defenses of *in pari delicto*,
 18 ratification, and consent, and hiQ does not oppose in its response brief. hiQ has thus waived any
 19 argument for those affirmative defenses. *See Pac. Dawn LLC v. Pritzker*, 831 F.3d 1166, 1178 n.7
 20 (9th Cir. 2016) (deeming argument waived where party failed to raise argument in opposition to
 21 motion for summary judgment). The Court therefore grants LinkedIn’s motion for summary
 22 judgment on hiQ’s affirmative defenses of *in pari delicto*, ratification, and consent.

23 3. Conclusion

24 In sum, the Court therefore **DENIES** LinkedIn’s motion for summary judgment on the
 25 breach of contract claim as to hiQ’s scraping and unauthorized use of data because there remains a
 26 genuine dispute of material facts for hiQ’s waiver and estoppel defenses, but **GRANTS** the
 27 motion as to hiQ turkers’ conduct.
 28

1 B. California Litigation Privilege

2 LinkedIn argues that hiQ’s tort and UCL claims are barred by Cal. Civ. Code § 47(b)
3 because hiQ’s alleged damages were caused by LinkedIn’s cease-and-desist letter (“C&D letter”)
4 that was a communication made in anticipation of potential litigation. hiQ responds that the
5 privilege does not apply because the C&D letter was not the sole cause of its damages, but rather
6 only part of LinkedIn’s broader anti-competitive scheme to “shut down” hiQ. hiQ further urged
7 this Court to apply the “sham” analysis under the *Noerr-Pennington* doctrine and find that the
8 “C&D letter was merely the ‘enforcement mechanism . . . [of LinkedIn’s] anticompetitive
9 scheme.’”

10 1. Legal Standard

11 “The essence of the *Noerr-Pennington* doctrine is that those who petition any department
12 of the government for redress are immune from statutory liability for their petitioning conduct.
13 The doctrine derives from two Supreme Court cases holding that the First Amendment Petition
14 Clause immunizes acts of petitioning the legislature from antitrust liability. The doctrine has since
15 been applied to actions petitioning each of the three branches of government, and has been
16 expanded beyond its original antitrust context.” *Theme Promotions, Inc. v. News Am. Mktg. FSI*,
17 546 F.3d 991, 1006-07 (9th Cir. 2008). *Noerr-Pennington* thus applies to “petitions sent directly
18 to the court in the course of litigation” as well as “conduct incidental to the prosecution of the
19 suit.” *Sosa v. DIRECTV, Inc.*, 437 F.3d 923, 934 (9th Cir. 2006).

20 Although similar to the *Noerr-Pennington* doctrine, the California litigation privilege is
21 broader. See *Vinson v. Cal. Dep’t of Corrs. & Rehab.*, No. 13-CV-00699-JST, 2014 WL 4594208,
22 at *6 (N.D. Cal. Sept. 15, 2014) (comparing the two privileges, stating that the California litigation
23 privilege is “[a] similar, though broader, rule”). The relevant statute reads in pertinent parts: “A
24 privileged publication or broadcast is one made: [¶] . . . [¶] (b) In any . . . (2) judicial proceeding
25 . . .” Cal. Civ. Code § 47(b). The California litigation privilege applies to “any communication
26 (1) made in judicial or quasi-judicial proceedings; (2) by litigants or other participants authorized
27 by law; (3) to achieve the objects of the litigation; and (4) that have some connection or logical
28 relation to the action.” *Silberg v. Anderson*, 50 Cal. 3d 205, 212 (1990). “[T]here is no ‘sham’

1 exception to the California litigation privilege comparable to the exception for *Noerr-*
 2 *Pennington* immunity.” *Dairy, LLC v. Milk Moovement, Inc.*, No. 2:21-CV-02233 WBS AC,
 3 2022 WL 2392622, at *5 (E.D. Cal. July 1, 2022); *see also NextG Networks, Inc v. NewPath*
 4 *Networks, LLC*, No. C 08-1565 VRW, 2008 WL 11399757, at *3 (N.D. Cal. Oct. 15, 2008)
 5 (noting that lack of “sham exception” to California’s litigation privilege is “unsurprising given the
 6 California Supreme Court’s characterization of the privilege as absolute”).

7 California courts have given § 47(b) “expansive application” and “the privilege has been
 8 extended to *any* communication, whether or not it is a publication, and to *all* torts other than
 9 malicious prosecution.” *Edwards v. Centex Real Est. Corp.*, 53 Cal. App. 4th 15, 29 (1997)
 10 (emphasis in original). And when applicable, the privilege is “absolute” regardless of the
 11 communicator’s “motives, morals, ethics, or intent.” *Silberg*, 50 Cal. 3d at 220. “Any doubt
 12 about whether the privilege applies is resolved in favor of applying.” *Kashian v. Harriman*, 98
 13 Cal. App. 4th 892, 913 (2002).

14 Prelitigation communications may fall within the scope of the absolute privilege.
 15 *Edwards*, 53 App. 4th at 30 (“[C]ourts have applied the judicial privilege to certain discrete
 16 categories of communications made in advance of actual litigation.”). However, such statements
 17 must meet additional requirements. Specifically, the “communication must have some relation to
 18 an imminent lawsuit or judicial proceeding which is *actually* contemplated seriously and in good
 19 faith to resolve a dispute, and not simply as a tactical ploy to negotiate a bargain.” *Id.* at 36
 20 (emphasis in original) (citing *Silberg* 50 Cal. 3d at 212–14). The “mere potential or ‘bare
 21 possibility’ that judicial proceedings ‘might be instituted’ in the future is insufficient to invoke the
 22 litigation privilege.” *Id.* (quoting Rest.2d Torts, §§ 586–588, com. e, pp. 247–251); *see also*
 23 *Action Apartment Assn., Inc. v. City of Santa Monica*, 41 Cal. 4th 1232, 1251 (2007). Whether a
 24 party acts in good faith is a question of fact. *Action Apartment*, 41 Cal. 4th at 1251. However, “if
 25 there is no dispute as to the operative facts, the application of the litigation privilege is a question
 26 of law.” *Kashian*, 98 Cal. App. 4th at 913.

27 2. The Good Faith Requirement

28 Because the C&D letter herein was *prelitigation* communications, “the factual question of

1 whether [such] prelitigation communication [were] made in good faith must be resolved prior to
2 the application of the privilege.” *Intermarketing Media, LLC v. Barlow*, No.
3 820CV00889JLSDFMX, 2021 WL 5990190, at *4 (C.D. Cal. May 4, 2021); *see also Edwards*, 53
4 App. 4th at 35 n.10 (noting that even in the case of the “classic example” of prelitigation
5 communication, *i.e.*, “the threat of an attorney to file suit if a claim is not settled,” the factual
6 determination as to good faith must precede application of the privilege). Importantly, under the
7 California litigation privilege the communicator’s “motives, morals, ethics, or intent” are
8 irrelevant, so long as there was a good faith intent to pursue legal action. *Silberg*, 50 Cal. 3d at
9 220. Thus, so long as LinkedIn had an intent to bring forth litigation when it sent the C&D letter,
10 the underlying motivation in doing so is irrelevant, *i.e.*, any anti-competitive motivations are
11 irrelevant.

12 hiQ has not presented any evidence that LinkedIn sent the C&D letter with bad faith intent
13 to not commence litigation. In fact, the evidence suggests the contrary. Specifically, the C&D
14 letter was sent by LinkedIn’s attorneys who contemplated and understood the legal implications of
15 the letter and the repercussions of any subsequent legal action. (*See* Docket No. 336-2 at 2
16 (Bajoria Decl.) (stating that he “determined that there appeared to be a sufficient factual and legal
17 basis to send a cease-and-desist letter . . .” and “believed the assertions of that letter were both
18 factually and legally justified.”); *see also* Lawit Decl. at 8 (stating that “[w]hen sending a cease-
19 and-desist letter, we hope that litigation will not be necessary but we always know that litigation is
20 a possibility and, accordingly, make sure that we have a legal basis to proceed if the factual
21 allegations prove to be true and we cannot reach an acceptable outcome . . .”).) Additionally, the
22 record indicates that LinkedIn has initiated litigation after sending C&D letters in the past,
23 supporting the notion that litigation was seriously contemplated when sending the C&D letter.
24 (*See* Lawit Decl. at 9 (indicating that LinkedIn has subsequently brought suit six times after
25 sending a C&D letter).) Certainly, LinkedIn’s vigorous litigation herein underscores the
26 seriousness of its intent to pursue its rights. These facts indicate more than a “bare possibility”
27 that a judicial proceeding “might be instituted” in the future. Therefore, no reasonable jury could
28 find that litigation was contemplated in bad faith. LinkedIn has thus satisfied the prelitigation

1 requirement under Cal. Civ. Code § 47.

2 3. Nature of LinkedIn's Conduct

3 “[B]ecause the litigation privilege applies only to communications, the ‘threshold issue’ is
4 whether [LinkedIn’s] conduct was communicative”—it was. *Mireskandari v. Gallagher*, 59 Cal.
5 App. 5th 346, 368 (2020) (citations omitted). “The distinction between communicative and
6 noncommunicative conduct hinges on the gravamen of the action [T]he key in determining
7 whether the privilege applies is whether the injury allegedly resulted from an act that was
8 communicative in its essential nature.” *Mireskandari v. Gallagher*, 59 Cal. App. 5th 346, 369
9 (2020) (quoting *Rusheen v. Cohen*, 37 Cal. 4th 1048, 1058 (2006)). Importantly, “if the gravamen
10 of the action is communicative, the litigation privilege extends to noncommunicative acts that are
11 necessarily related to the communicative conduct[.]” *Id.* (quotation omitted). “Stated another
12 way, unless it is demonstrated that an independent, noncommunicative, wrongful act was the
13 gravamen of the action, the litigation privilege applies.” *Rusheen*, 37 Cal. 4th at 1065.

14 hiQ argues that C&D letter was not the sole gravamen of its complaint. It claims that the
15 C&D was merely part of LinkedIn’s broader anti-competitive scheme to “shut down” hiQ. In its
16 view, LinkedIn “gathered competitive intelligence on hiQ’s customers, partners, and product
17 features” before ultimately “driv[ing] hiQ out of the market.” (hiQ Opp. at 1.) But the facts show
18 that hiQ’s alleged damages hinge entirely on the C&D letter. Specifically, when asked what
19 “monetary remedies” hiQ was seeking in the action against LinkedIn, hiQ’s CEO and 30(b)(6)
20 witness, Mr. Mark Weidick, stated that the company had a massive milestone and “opportunity to
21 be a billion dollar business” but that “stopped after [LinkedIn’s] accusations and threats were put
22 in the market from the cease and desist letter.” (LCE 1207–08 (Weidick Dep. Tr.)) Further,
23 hiQ’s damages expert, Mr. Benjamin Sacks, stated that his damages analysis stops on the day the
24 C&D letter was sent because he “assumed that there was no value in the company” after that date.
25 (LCE 0998–1004 (Sacks Dep. Tr.); *see also* HCE Ex. 90 (Sacks Dep. Tr. at 245:20-247:10); HCE
26 Ex. 88 (Sacks Second Amended Expert Report) at 2 (“I am instructed to assume that the C&D
27 interfered with hiQ’s existing and prospective contracts and business relationships, effectively
28 destroying hiQ’s business[.]”)) Such evidence indicates that hiQ’s damages resulted from the

1 C&D letter and that the letter is the gravamen of the complaint.

2 Because the C&D letter was the gravamen of hiQ’s complaint, it follows that the four
 3 elements of the privilege are satisfied, barring hiQ’s tortious interference and UCL claims.
 4 Specifically, the C&D letter was a communication made in anticipation of litigation, *i.e.*, a judicial
 5 proceeding. *See Edwards*, 53 Cal. App. 4th at 35 n.10 (“The classic example of an instance in
 6 which the privilege would attach to prelitigation communications is the attorney demand letter
 7 threatening to file a lawsuit if a claim is not settled.”). The letter was sent by attorneys on behalf
 8 of LinkedIn. *See Silberg*, 50 Cal. 3d at 219 (holding that “[d]efendant’s statements . . . suitability
 9 were made by a participant, *i.e.*, the attorney for a party”). The object of the letter was to assert
 10 rights. And the letter bears “some relation” to the action (indeed it was the catalyst for this action)
 11 as it sparked hiQ’s lawsuit against LinkedIn as well set forth the claims with which LinkedIn has
 12 now asserted against hiQ.

13 4. Conclusion

14 Having found that the California litigation privilege applies, the Court **GRANTS** summary
 15 judgment for LinkedIn on hiQ’s UCL and tortious interference claims. LinkedIn’s motions to
 16 exclude hiQ’s expert opinions supporting those claims are therefore **DENIED** as moot.

17 **V. HIQ’S MOTION FOR SUMMARY JUDGMENT (DOCKET NO. 355)**

18 hiQ moves for summary judgment on LinkedIn’s claim under the CFAA because it is time-
 19 barred by the statute’s two-year statute of limitations. Based on two email chains³ among
 20 LinkedIn employees, hiQ argues that LinkedIn had reasonable notice of hiQ’s scraping activity in
 21 2014—more than two years before the filing of this action on June 7, 2017. LinkedIn disputes
 22 whether the employees in question had notice and, even if they did, whether their knowledge can
 23 be imputed to LinkedIn.

24
 25
 26 ³ The Court overrules LinkedIn’s evidentiary objection that hiQ’s attempt to impute the
 27 knowledge or statements of participants in the email chains to LinkedIn lacks foundation. “At the
 28 summary judgment stage, we do not focus on the admissibility of the evidence’s form. We instead
 focus on the admissibility of its contents.” *See Fraser v. Goodale*, 342 F.3d 1032, 1036 (9th Cir.
 2003). hiQ can lay the requisite foundation at trial by, for example, calling those participants as
 witnesses.

1 A. Legal Standard

2 A claim under the CFAA is timely if brought “within 2 years of the date of the act
3 complained of or the date of the discovery of the damage.” 18 U.S.C. § 1030(g). “When
4 ‘legislators have written the word “discovery” directly into the statute . . . state and federal courts
5 have typically interpreted the word to refer not only to actual discovery, but also to the
6 hypothetical discovery of facts a reasonably diligent plaintiff would know.’” *West v. Ronquillo-*
7 *Morgan*, No. CV 20-2711 DSF (EX), 2021 WL 2953160, at *3 (C.D. Cal. May 10, 2021) (quoting
8 *Merck & Co. v. Reynolds*, 559 U.S. 633, 645 (2010)); *see also Maddalena v. Toole*, No. 2:13-CV-
9 4873-ODW, 2013 WL 5491869, at *4 (C.D. Cal. Oct. 1, 2013) (“Like many statutes of limitation,
10 the statute[] at issue in this action do[es] not require that the claimant have actual knowledge of
11 the violation. Rather, . . . 1030(g) demands only that the claimant have had a reasonable notice to
12 discover the violation.”).

13 Because LinkedIn has the burden of proof at trial to establish that it is entitled to the
14 benefit of the discovery rule, “to defeat summary judgment [it is] required to come forward with
15 evidence establishing a triable issue of fact with regard to whether the discovery rule applies.”
16 *O’Connor v. Boeing N. Am., Inc.*, 311 F.3d 1139, 1150 (9th Cir. 2002) (citation omitted).
17 Summary judgment is improper “unless the only reasonable inference that can be drawn is that
18 [LinkedIn] knew or should have known” its damage from hiQ’s scraping before June 7, 2015. *Id.*;
19 18 U.S.C. § 1030(g).

20 “A two-part analysis determines whether [LinkedIn] reasonably should have known of [its]
21 claim.” *O’Connor*, 311 F.3d at 1150 (citations omitted). First, courts consider “whether a
22 reasonable person in [LinkedIn’s] situation would have been expected to inquire about the cause
23 of [its] injury.” *Id.* Second, if LinkedIn was on inquiry notice, courts must next determine
24 whether an inquiry “would have disclosed the nature and cause of [LinkedIn’s] injury so as to put
25 [it] on notice of [its] claim.” *Id.* LinkedIn is “charged with knowledge of facts that [it] would
26 have discovered through inquiry.” *Id.* (citations omitted).

27 B. The October 2014 Email Chain

28 On October 8, 2014, several LinkedIn employees exchanged emails regarding an

1 upcoming hiQ Elevate conference. All the LinkedIn employees on the email chain were members
2 of the Talent Analytics Team that supported LinkedIn’s Human Resources group. In the chain,
3 one employee, Daniel Maurath, initially emailed the Talent Analytics Team’s group alias address
4 and asked if anyone had heard of hiQ. (Docket No. 356 Ex. C.) Another employee, William
5 Gaker, responded, “This looks like a sales conference for a company presenting a new product. I
6 would love to see what data they are using. It sounds like they might be scraping our site to see
7 who has updated profiles and using that as a signal to predict turnover.” (*Id.*) He later followed
8 up, “It might be good for someone (or at least alert someone who handles how our data gets used)
9 to go to make sure this vendor isn’t accessing our data without our permission.” (*Id.*) The email
10 chain concluded with Mr. Maurath agreeing to “request to attend” hiQ’s conference and “at least
11 find out more info.” (Docket No. 356 Ex. D.) However, no one attended the conference,
12 investigated hiQ, or reported hiQ to LinkedIn’s legal department. (Docket No. 358-3 Ex. 33
13 (Lawit Dep. Tr. (8/26/22)) at 72:18-73:3; Docket No. 358-1 (Maurath Decl.) at ¶ 4; Docket No.
14 358-2 (Rigano Decl.) at ¶ 4.)

15 No matter what the employees on the email chain knew, a genuine dispute of material fact
16 remains regarding whether their knowledge can be imputed to LinkedIn. In the employment
17 context, “[k]nowledge acquired by an agent while acting within the course and scope of his
18 employment is chargeable to his principal, his employer.” *Mountain Copper Co. v. Welcome*
19 *Growers Gin Co.*, 197 Cal. App. 2d 253, 256 (1961). The parties agree that the employee must
20 have a duty to disclose that knowledge. (Docket No. 360-2 (“LinkedIn Opp.”) at 22; Docket No.
21 385-3 (“hiQ Reply”) at 4 (“[T]he question is whether the facts were acquired within the scope and
22 course of employment, and accordingly, whether the LinkedIn employees who concededly had
23 knowledge of, or suspected, hiQ’s scraping activity *had a duty to disclose that knowledge.*”)
24 (emphasis added).) *See* Cal. Civ. Code § 2332 (“As against a principal, both principal and agent
25 are deemed to have notice of whatever either has notice of, and ought, in good faith and the
26 exercise of ordinary care and diligence, to communicate to the other.”); *Triple A Mgmt. Co., Inc. v.*
27 *Frisone*, 69 Cal. App. 4th 520, 534–35 (1999) (“The basis for imputing knowledge to the principal
28 is that the agent has a legal duty to disclose information obtained in the course of the agency and

1 material to the subject matter of the agency, and the agent will be presumed to have fulfilled this
2 duty.”); *United States v. Georgia-Pacific Co.*, 421 F.2d 92, 98 n.9 (9th Cir. 1970) (“[A] principal
3 is bound by the knowledge of its agent concerning a matter upon which it is the agent’s duty to
4 give the principal information.”) (citing Restatement, Agency 2d § 272).

5 The parties dispute whether LinkedIn’s employees had a duty to disclose their knowledge
6 of hiQ’s suspected scraping to LinkedIn, and that is a factual dispute for the jury. *See Maron v.*
7 *Swig*, 115 Cal. App. 2d 87, 90 (1952) (holding whether it was within the scope of agency to take
8 certain actions was a question of fact for the jury).

9 On one hand, the LinkedIn employees did not seem to explicitly have anti-scraping
10 responsibilities. Two employees on the October 2014 email chain submitted declarations stating
11 that their “work supported only LinkedIn’s own hiring and retention efforts,” that and “did not
12 support or work on LinkedIn’s external facing products.” (Maurath Decl. at ¶ 3; Docket No. 358-
13 2 (Rigano Decl.) at ¶ 3.)

14 On the other hand, a reasonable factfinder could find that the LinkedIn employees
15 implicitly had a duty to report suspected scraping, especially when LinkedIn appears to have no
16 functioning anti-scraping program or enforcement team as of October 2014. (*See* LinkedIn’s
17 Supp. Resp. to Interrogatory 8 (“When hiQ was subsequently identified by email to Scraper
18 Council in October 2015, at the time the cross-functional group was still working out its internal
19 processes and there were not yet clear lines of responsibility or a playbook on how to proceed with
20 reports made to the Scraper Council.”); Docket No. 386 Ex. D (LinkedIn April 2015 slide deck on
21 third party scraping stating that it was “investing very little into stopping 3rd party scraping” and
22 that the team working on scraping prevention consisted of “1 data scientist, 1 infra engineer, 0.25
23 of a person in legal, and very minimal support from TnS/BD”).) Given such limited resources, it
24 is reasonable to infer that employees not explicitly designated to report scraping nonetheless had
25 such a responsibility. A factfinder may also infer such a duty from the fact that Mr. Maurath
26 volunteered to “request to attend [hiQ’s conference]” when Mr. Gaker recommended someone “to
27 go to make sure [hiQ] isn’t accessing [LinkedIn’s] data without [its] permission,” even though no
28 one did so. (Docket No. 356 Exs. C, D; Lawit Dep. (8/26/22) at 72:18-73:3; Maurath Decl. ¶ 4.)

1 Because a genuine dispute exists as to the scope of employment of the LinkedIn's
2 employees on the October 2014 email chain, a factfinder may draw more than one reasonable
3 inference regarding whether LinkedIn knew or should have known about hiQ's scraping then.
4 Summary judgment in hiQ's favor based on the October 2014 LinkedIn email chain thus would be
5 improper. *See Miniace v. Pac. Mar. Ass'n*, No. C 04-03506 SI, 2006 WL 648732, at *2 (N.D. Cal.
6 Mar. 13, 2006) (denying summary judgment on statute of limitations defense where, under
7 California agency law, factual questions remained as to whether Director of Human Resources had
8 obligation to report amendment to executives' life insurance to impute knowledge to corporation).

9 C. The December 2014 Email Chain

10 On December 15, 2014, Bob Rosin, LinkedIn's Vice President of Business Development,
11 forwarded an email to Lee Womer, LinkedIn's then Director of Business Development. (Docket
12 No. 356-7 Ex. H at 3.) The email was from a third-party venture capital investor who had looked
13 into hiQ and "[wasn't] sure that LinkedIn would look favorably at a company that is analyzing
14 profiles." (*Id.*) In response, Mr. Womer expressed concern that hiQ might not be a "members'
15 first use case." (*Id.* at 2.) He defined "members' first use" as "one of LinkedIn's corporate values
16 that guides decision making, which is that the interest of LinkedIn members on the platform need
17 to take first priority amongst a range of priorities." (Docket No. 356-8 Ex. I⁴ at 55:11-15.)

18 There is a material factual dispute as to whether the LinkedIn employees on the December
19 2014 email chain had notice of hiQ's scraping activity. The email did not expressly mention the
20 term "scraping." And both Mr. Womer and Mr. Rosin testified that they could not specifically
21 remember if they suspected hiQ of scraping when they received the email. (Docket No. 358-3 Ex.
22 7 (Womer Dep. Tr.) at 54:11-16; Docket No. 356-5 Ex. F (Rosin Dep. Tr.)⁵ at 126:25-127:4.) hiQ
23 argues that a January 12, 2015, email that Mr. Rosin received shows that he knew about third

24 _____
25 ⁴ The Court overrules LinkedIn's objection to this exhibit because it is not properly authenticated.
26 For the purpose of this motion, the Court considers this exhibit because it can be presented in a
27 form admissible at trial. *See Fraser*, 342 F.3d at 1036 ("At the summary judgment stage, we do
28 not focus on the admissibility of the evidence's form. We instead focus on the admissibility of its
contents."); *see also Faulks v. Wells Fargo & Co.*, 231 F. Supp. 3d 387 (N.D. Cal. 2017).

⁵ LinkedIn objects to hiQ's Exhibit F because it is not properly authenticated. The Court overrules
this objection for the same reason as above.

1 parties scraping LinkedIn and that LinkedIn did not approve of it. (HCE Ex. 22.) That 2015 email
 2 involves a discussion about another company that was scraping LinkedIn data, but it makes no
 3 mention of hiQ. (*Id.*) Thus, even if Mr. Rosin knew about third parties scraping LinkedIn
 4 generally, there is a genuine dispute as to whether Messrs. Womer and Rosin knew hiQ was
 5 “analyzing profiles” through scraping.

6 Additionally, there is a material factual dispute as to whether Messrs. Womer and Rosin’s
 7 knowledge was imputable to LinkedIn. Mr. Rosin testifies that he was not involved with anti-
 8 scraping in 2014. (Rosin Dep. Tr. at 108:2-109:1, 117:15-118:1, 152:16-25.) And Mr. Womer
 9 did not take on responsibility for scraping-related issues until 2015. (Womer Dep. Tr. at 30:11-
 10 31:1.) For the same reasons as explained for the October 2014 email chain, it is for the jury to
 11 decide whether they had a duty to report suspected scraping to LinkedIn.

12 Even if Messrs. Womer and Rosin knew hiQ was scraping LinkedIn and their knowledge
 13 can be imputed to LinkedIn, there is still a factual dispute as to “whether a reasonable person in
 14 [LinkedIn’s] situation would have been expected to inquire about the cause of [its] injury.”
 15 *O’Connor*, 311 F.3d at 1150. LinkedIn provided evidence that it received over one hundred
 16 recorded reports of scraping every year between 2015 and 2021 and that it “did not have the
 17 resources to investigate every single report of potential abuse.” (Lawit Decl. at ¶¶ 14-15.) Mr.
 18 Womer testified that there was nothing about the December 2014 email that suggested he should
 19 prioritize an investigation into hiQ’s potential scraping activity. (Womer Dep. Tr. at 57:13-24.)
 20 Thus, the Court cannot conclude as a matter of law that LinkedIn had or should have had notice of
 21 hiQ’s scraping from the December 2014 email chain.

22 In sum, because more than one reasonable inference can be drawn as to whether LinkedIn
 23 knew or should have known that hiQ scraped LinkedIn’s site before June 7, 2015, the Court
 24 **DENIES** hiQ’s motion for summary judgment.

25 **VI. LINKEDIN’S MOTION FOR SPOILIATION SANCTIONS (DOCKET NO. 337)**

26 LinkedIn requests evidentiary sanctions applied coincident with its pending summary
 27 judgment and *Daubert* motions, and to the extent necessary thereafter, as jury instructions against
 28 hiQ for the destruction of two categories of electronically stored information. Besides monetary

1 sanctions, it seeks (1) various adverse inference jury instructions, and (2) dismissal of all of hiQ's
2 claims that involve its relationships with its customers and prospective, or in the alternative, an
3 order precluding hiQ from offering any evidence or argument attributing its loss of customers or
4 potential customers to any action by LinkedIn, including preclusion of its expert report calculating
5 "business value" based on implied customer relationships.

6 A. The Evidence At Issue

7 This sanctions motion concerns the evidence hiQ stored with three cloud service
8 providers—Salesforce, Splunk, and Amazon Web Services ("AWS"). Salesforce hosted hiQ's
9 "Customer Relationship Management Database" or "CRM Database." Splunk and AWS both
10 hosted hiQ's scraping activity records. Because the data stored in Salesforce CRM Database only
11 relate to hiQ's UCL and tortious interference claims on which the Court has granted motion for
12 summary judgment for LinkedIn, the Court only analyzes data stored with Splunk and AWS.

13 hiQ issued a company-wide litigation hold notice on June 20, 2017, about a month after
14 LinkedIn's C&D letter and two weeks after hiQ's filing of this action. (LCE Ex. 93.) After that,
15 hiQ's employees "started to leave the business rather quickly." (Docket No. 368-1 Ex. P (Weidick
16 Dep. Tr.) at 51:11.) In 2018, hiQ had 13 individuals left on the payroll, "barely half the personnel
17 on its payroll the year prior." (Docket No. 368 at 3.) hiQ went into hibernation that year. (Docket
18 No. 335-3 at 5.) By January 2019, no personnel remained on hiQ's payroll. (*Id.*) hiQ went in
19 debt. (*Id.*) At times, hiQ's CEO and its employees put their personal credit cards on accounts to
20 keep the accounts active. (Docket No. 368-1 Ex. P (Weidick 3/8/22 Dep. Tr.) at 23:12-20.)

21 1. hiQ's AWS Account

22 hiQ lost the data stored in its AWS account in or around September 2020 after AWS
23 terminated the account earlier that year for non-payment. (Docket No. 368 at 4.) AWS housed a
24 computer database program called MongoDB that stored several collections of hiQ data. (Docket
25 No. 355-3 at 3-4.) The "Raw Scrape" collection contained the actual information hiQ scraped
26 from LinkedIn member profiles. (*Id.* at 4.) The "scrapus" and "scrapus2" collections
27 (collectively, the "Scrapus Collections") contained scraping information for each target LinkedIn
28 profile URL, including whether the last request that hiQ's scrapers made on LinkedIn's servers for

1 each profile was successful or blocked. (*Id.*) The “Proxies Collection” organized data around
2 each IP address that hiQ’s scrapers were using to evade LinkedIn’s general technical defenses.
3 (*Id.* at 4–5.) MongoDB also housed data related to hiQ’s use of “mechanical turkers”—
4 contractors who logged into LinkedIn’s platform, sometimes using fake accounts, to collect profile
5 data not publicly available. (*Id.*; Docket No. 368 at 4.)

6 For all the data stored in its AWS account, hiQ archived only the “Raw Scrape” collection
7 in 2018, the year when hiQ started receiving suspension notices from AWS due to non-payment.
8 (Docket No. 368 at 4.) It maintains that the other collections remained in hiQ’s AWS account for
9 several years thereafter (*id.*), but LinkedIn points to hiQ internal communications between 2017
10 and 2018 referencing plans to affirmatively delete AWS data as part of a migration of its data to
11 save money (Docket No. 335-3 at 6). In March 2020, a month before AWS permanently
12 suspended hiQ’s account, hiQ’s CEO sent an email to its litigation funder that hiQ was \$895,000
13 in debt, \$22,600 of which was owed to AWS. (LCE 1255 (3/2/20 Weidick email).) The email
14 chain mentioned a few potential options to preserve AWS and the fact that hiQ’s AWS’s account
15 would “shut down and delete immediately” if not paid. (*Id.*) After AWS’s deletion and after
16 LinkedIn sought information from AWS beyond what had been achieved, hiQ, through counsel,
17 attempted to recover the lost Salesforce data without success. (Docket No. 368 at 4.)

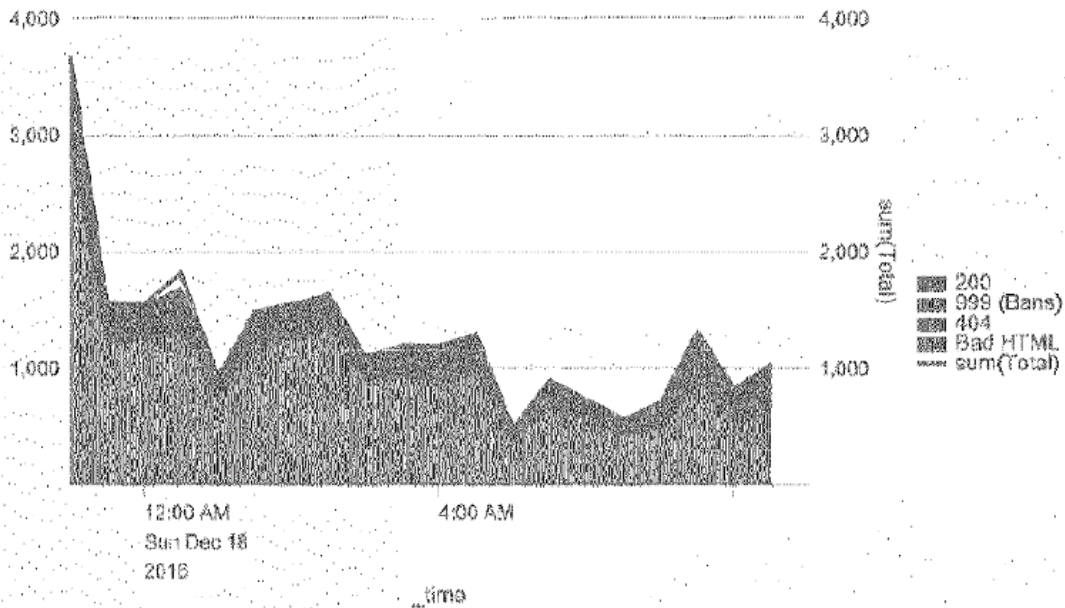
18 2. hiQ’s Splunk Account

19 hiQ lost most of its data stored with Splunk, a company that provided specialized software
20 to hiQ. (Docket No. 335-3 at 7.) Splunk logged and kept for analysis data about every hiQ scrape
21 attempt and the failure rate of those attempts. (*Id.*) In July 2018, when discussing hiQ’s winding
22 down of storage management services, a hiQ software developer noted that hiQ should not delete
23 the 580 gigabytes Splunk data as it could “be important for legal issues.” (*Id.*) hiQ did not
24 affirmatively delete those data, but did let its Splunk account become inactivated. (Docket No.
25 335-3 (“The lost data was completely accessible to hiQ until the point at which Splunk
26 discontinued its services to hiQ.”) (citing Devorakonda dep.)) hiQ initially did not disclose to
27 LinkedIn the existence of Splunk when the parties had detailed discussions regarding ESI from
28 August to November 2021. (*Id.* at 8.) After LinkedIn discovered the existence of Splunk and

United States District Court
Northern District of California

1 inquired about it, hiQ “learned that it was unable to access its Splunk account.” (*Id.*; Docket No.
2 368 at 4.) Splunk advised hiQ that all of its data would remain available in the event of
3 reactivation, but upon reactivation, hiQ discovered that only less than one month of data in 2020
4 remained in the account. (*Id.*)

5 hiQ has produced over 600 daily Splunk scraping dashboards and other documentation
6 concerning hiQ’s scraping efforts. (Docket No. 368 at 22.) The scraping dashboards were created
7 in the normal course of business between November 11, 2016, and July 7, 2020. (*Id.*) These
8 dashboards showed various statistics relating to hiQ’s technology, including the general trend of
9 requests hiQ made to LinkedIn’s servers and ban rates of those requests. (Docket No. 368-1 Exs.
10 A-H.) LinkedIn observes that the produced dashboards consist of barely legible line graphs.
11 (Docket No. 387 at 9.) And its expert testifies that it is difficult to discern the precise number of
12 requests made. (Schmidt Decl. at ¶ 13.) Examples of the dashboards are shown below.



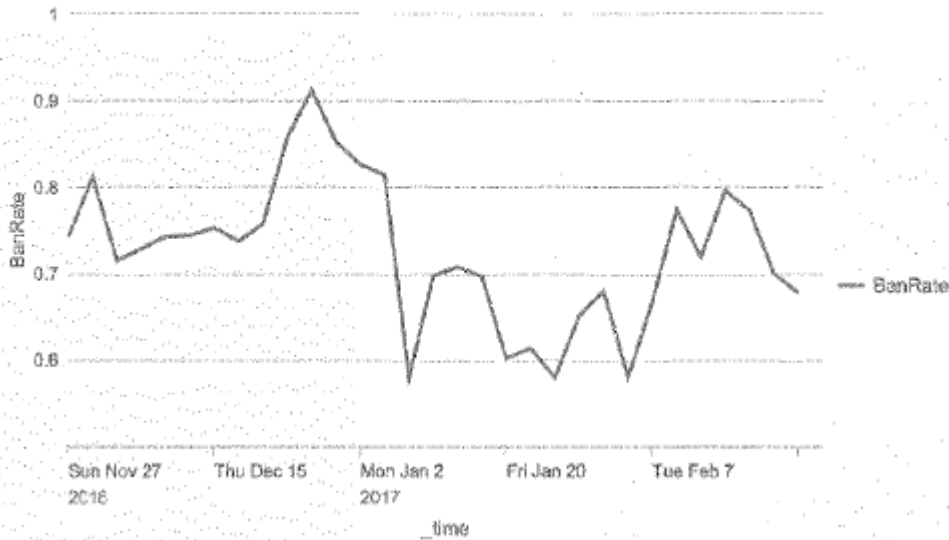
23 (Docket No. 368-1 Ex. B.)

24 ///

25 ///

Ban Rate

Ban Rate over last 3 months -- sampled 1:10, 3 day average



(*Id.* Ex. C.)

hiQ has also produced communications among its engineers regarding the success rate of hiQ’s scraping attempts of LinkedIn during the relevant time period. (*See* LCE 0051 (“Ban rate continues to fluctuate between .90 and 1.0. Often[,] we see ban rate stick at close to 1.0 for several days in a row.”), 0770 (“we can no longer scan LinkedIn, ban rate is > 99%.”), 1173 (“I am shutting down scraping for the time being. We’re only getting a trickle of data, and we could be in danger of hitting our proxies too hard and creating a situation.”), 1174 (“Need path to scrape [LinkedIn] better & faster (e.g.,) from 100K per day to 500K per day.”), 1258 (“The first order of business is to get scraping back up and running to some viable pace.”), 1259 (“The ban rate has increased to the point where it [is] no longer working again.”), 1616 (“unfortunately, Luminati has told me they can’t deliver any help for ~2 weeks.”), 1626–27 (discussing scraping LinkedIn via proxy).)

B. Legal Standard

Federal Rule of Civil Procedure 37(e), as amended in 2015, provides in full as follows:

(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed

1 to take reasonable steps to preserve it, and it cannot be restored or
replaced through additional discovery, the court:

2 (1) upon finding prejudice to another party from loss of the
3 information, may order measures no greater than necessary to cure
the prejudice; or

4 (2) only upon finding that the party acted with the intent to deprive
5 another party of the information's use in the litigation may:

6 (A) presume that the lost information was unfavorable to the
party;

7 (B) instruct the jury that it may or must presume the
8 information was unfavorable to the party; or

9 (C) dismiss the action or enter a default judgment.

10 Fed. R. Civ. P. 37(e).

11 Rule 37(e) therefore provides two levels of sanctions. Under Rule 37(e)(1), upon finding
12 that the loss of ESI that the offending party had a duty to preserve has prejudiced the moving
13 party, a court “may order measures no greater than necessary to cure the prejudice.” If the court
14 further finds that the offending party “acted with the intent to deprive another party of the
15 information’s use in the litigation,” the court may presume (or instruct the jury to presume) that
16 the lost information was unfavorable to the offending party, dismiss the action, or enter a default
17 judgment. Fed. R. Civ. P. 37(e)(2).

18 The Advisory Committee Notes emphasize that the “remedy should fit the wrong.” Fed.
19 R. Civ. P. 37(e) advisory committee’s note to 2015 amendment. A finding of breach and
20 prejudice under Rule 37(e)(1) is sufficient for the court to “allow[] the parties to present evidence
21 to the jury concerning the loss and likely relevance of information and instructing the jury that it
22 may consider that evidence, along with all the other evidence in the case, in making its decision,”
23 as long as this is “no greater than necessary to cure prejudice.” *Id.*

24 C. Analysis

25 hiQ does not dispute that it had a duty to preserve the ESI evidence at issue here. (Docket
26 No. 368 at 3 (“hiQ understood that data on its MongoDB and AWS accounts should be preserved
27 for this litigation.”); *id.* at 4 (“Splunk data should not be deleted as it ‘can be important for legal
28 issues.’”) (quoting hiQ employee); *id.* at 5 (“hiQ understood that it should maintain the data from

1 its Salesforce account for the purposes of litigation.”.)

2 Nor does hiQ dispute that it has permanently lost the evidence at issue. (Docket No. 368-1
3 Ex. Z (Weidick Decl.) at ¶ 3 (“With respect to AWS and Salesforce, despite our best efforts, we
4 were not able to recover any data from those accounts and were advised that the data had been
5 permanently deleted after hiQ’s accounts had been closed due to non-payment.”), ¶ 4 (“[O]nly a
6 subset of the data still existed in hiQ’s Splunk account, and that older data was no longer
7 available.”).)

8 On the merits, the Court therefore analyzes (1) whether hiQ “acted with the intent to
9 deprive [LinkedIn] of the information’s use in the litigation” under Federal Rule of Civil
10 Procedures 37(e)(2), (2) whether the loss of the evidence prejudiced LinkedIn under Rule 37(e)(1),
11 and (3) what sanctions, if any, are appropriate.

12 1. There Is Insufficient Evidence To Find hiQ Acted With The Requisite Intent To
13 Warrant Rule 37(e)(2) Sanctions

14 Unlike Rule 37(e)(1), Rule 37(e)(2) “does not include a requirement that the court find
15 prejudice to the party deprived of the information.” Fed. R. Civ. P. 37(e) advisory committee’s
16 note to 2015 amendment. “This is because the finding of intent required by the subdivision can
17 support not only an inference that the lost information was unfavorable to the party that
18 intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss
19 of information that would have favored its position.” *Id.*

20 a. A Knowing Failure To Preserve Per Se Does Not Establish An “Intent To
21 Deprive”

22 The parties do not dispute that hiQ knowingly failed to preserve the evidence at issue, but
23 disagree whether that amounts to an “intent to deprive [LinkedIn] of the information’s use in the
24 litigation.” Fed. R. Civ. P. 37(e)(2). Rule 37(e)(2) requirement of a specific “intent to deprive”
25 may be inferred from a knowing failure to preserve when combined with other circumstances.

26 LinkedIn argues that a knowing failure to preserve qualifies as an “intent to deprive” per
27 se, primarily relying on *Fourth Dimension Software v. DER Touristik Deutschland GmbH*, No. 19-
28 cv-05561-CRB, 2021 WL 5919821, at *10 (N.D. Cal. Dec. 15, 2021). In that case, the court cited

1 the standard that “a party’s deletion of information qualifies as intentional ‘if the party has some
2 notice that the documents were potentially relevant to the litigation before they were destroyed.’”
3 *Id.* (quoting *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 959 (9th Cir. 2006)). But the quoted authority,
4 *Leon*, concerns willful spoliation under a court’s inherent authority. 464 F.3d at 958. The Ninth
5 Circuit has indicated that Rule 37(e) “foreclose[s] reliance on inherent authority.” *Newberry v.*
6 *Cty. of San Bernardino*, 750 F. App’x 534, 537 (9th Cir. 2018) (quoting Fed. R. Civ. P. 37
7 Advisory Committee Notes to the 2015 Amendment); *but see Meta Platforms*, 2022 WL 1990225,
8 at *7 (holding party’s negligence in failing to preserve ESI could support adverse inference
9 instruction under Court’s inherent authority). And the *Fourth Dimensions* court did not seem to
10 have actually relied on the *Leon* standard. Instead, the court found the plaintiff to have acted with
11 an intent to deprive under Rule 37(e)(2) “based on the timing and circumstances of the deletion.”
12 *Id.*, 2021 WL 5919821, at *10. *Ottoson v. SMBC Leasing and Fin., Inc.* which relies on inherent
13 authority therefore is also inapplicable. 268 F. Supp. 3d 570, 580 (S.D.N.Y. 2017).

14 The court in *Moody v. CSX Transp., Inc.* inferred a specific “intent to deprive” under Rule
15 37(e)(2) from a knowing failure to preserve when “mere negligence” was “implausible.” 271 F.
16 Supp. 3d 410, 424, 427 (W.D.N.Y. 2017). That case concerns the loss of data from a train data
17 recorder, “highly relevant—if not the most important objective evidence”—to determine liability
18 in a train accident where plaintiff lost a limb. *Id.* at 422, 431. The train company’s foreman
19 downloaded the data to a computer and was supposed to then transmit the data to a centralized
20 server, but appeared to have transmitted the wrong file. *Id.* at 422. His computer then crashed and
21 the company lost the computer without ever trying to retrieve the data. *Id.* at 423. The court held
22 that the company acted with “intent to deprive” because it could not “credibly explain[]” its
23 “failure to make any effort over the course of four years to confirm that the data was properly
24 preserved.” *Id.* at 431. Additionally, had the defendants made a reasonable inquiry as required by
25 Rules 11 and 26(a), they would have noticed that the data was missing at a time when it was still
26 capable of being retrieved. *Id.* at 427. Hence, the court found more than mere negligence.

27 LinkedIn’s other cases suggest that courts require conduct akin to bad faith to infer a
28 specific “intent to deprive.” *See Sines v. Kessler*, No. 3:17-CV-00072, 2021 WL 4943742, at *11

1 (W.D. Va. Oct. 22, 2021), *order approved*, No. 3:17-CV-00072, 2021 WL 5492826 (W.D. Va.
 2 Nov. 19, 2021) (finding intent to deprive based on defendant’s “inability to recall almost *any* fact
 3 about the steps he took (or did not take) to preserve or recover this ESI, combined with his
 4 occasionally flippant or dismissive answers to opposing counsel’s questions at his court-ordered
 5 deposition, demonstrates a contempt for his discovery obligations . . . that further reinforces this
 6 conclusion”) (emphasis in original); *O’Berry v. Turner*, No. 7:15-CV-00064-HL, 2016 WL
 7 1700403, at *4 (M.D. Ga. Apr. 27, 2016) (finding defendants’ “irresponsible and shiftless
 8 behavior,” including having no written policy on proper procedure to preserve evidence and
 9 failing to collect the documents at issue after numerous requests by the Plaintiff to do so, “can
 10 only lead to one conclusion—that [they] acted with the intent to deprive Plaintiff of the use of this
 11 information at trial”). In sum, these authorities appear to require a specific intent to deprive, rather
 12 than a mere knowing failure to preserve.

13 b. Direct And Circumstantial Evidence Suggests That hiQ Lost The Evidence
 14 At Issue Negligently Or With An Intent To Cut Cost

15 The circumstances in this case suggest that hiQ destroyed, or allowed to be destroyed, the
 16 evidence at issue either negligently or with an intent to cut cost, but not with a specific “intent to
 17 deprive [LinkedIn] of the information’s use in the litigation.” Fed. R. Civ. P. 37(e)(2). **First**,
 18 LinkedIn seems to agree that any *affirmative* deletion of the evidence by hiQ is “part of a
 19 migration of [hiQ’s] data in order to save money.” (Docket No. 335-3 at 6.) hiQ attempted to cut
 20 costs in 2018 by migrating all of its MongoDB operations from California and Oregon to Virginia.
 21 (*Id.*; LCE 1535 (2/02/18 hiQ email regarding “All-hands AWS cleanup” to “strip down any
 22 systems that [we]re defunct or should be . . . to reduce [its] AWS costs by several thousand
 23 dollars”).) In that process, hiQ’s employees discussed deleting some AWS data, including data
 24 that made up the Scrapus Collections and the Proxies Collection. (LCE 1614 (7/6/18 hiQ Chat
 25 Tr.) (discussing deletion of three “AWS volumes”); LCE 1618 (5/16/18 hiQ Chat Tr.) (“Scrapus2
 26 we dont [sic] need to backup”); LCE 1634 (8/22/17 hiQ Chat Tr.) (discussing deleting “Mongo-
 27 Scraper”).)

28 **Second**, there is no dispute that hiQ has struggled financially and that it lost its Salesforce

1 and AWS accounts because it was unable to pay the bills. (*See* LCE 1391 (hiQ Second Supp.
2 Resp. to LinkedIn’s Interrogatory No. 16) (“Salesforce deleted the raw data from hiQ’s Salesforce
3 instance at some point in or around January 2020 after hiQ had been unable to pay its Salesforce
4 bills AWS delet[ed] hiQ’s data for non-payment.”).) Although hiQ received repeated
5 suspension notices from AWS and consciously let its AWS account lapse, the decision was driven
6 by financial considerations. In March 2020, a month before AWS permanently suspended hiQ’s
7 account, hiQ’s CEO wrote to its litigation funder detailing the accounts receivable to “prevent any
8 creditor from pushing the company into a receivership situation and thereby take control of [its]
9 litigation.” (LCE 1255 (3/2/20 Weidick email).) To be sure, hiQ’s financial situation does not
10 absolve its duty of preservation, but it does suggest the driving factor was not an intent to deprive
11 LinkedIn of evidence.

12 **Third**, the timing of the evidence’s loss indicates a lack of such intent. “The most decisive
13 factor [in the ‘intent’ analysis] is the timing” of the offending conduct. *Fed. Trade Comm. v.*
14 *Noland*, No. CV-20-00047-PHX-DWL, 2021 WL 3857413, at *12 (D. Ariz. Aug. 30, 2021)
15 (finding “intent to deprive” where defendants installed “elaborate encrypted privacy-focused apps
16 immediately after discovering they were the subject of an FTC investigation”); *accord Fourth*
17 *Dimensions*, 2021 WL 5919821, at *10 (finding party to have intentionally destroyed records
18 where it affirmatively destroyed records “shortly after receiving notice that [plaintiff] was
19 prepared to file suit”); *Brittney Gobble Photography, LLC v. Sinclair Broad. Grp., Inc.*, No. SAG-
20 18-3403, 2020 WL 1809191, at *10 (D. Md. Apr. 9, 2020) (“more than a month” delay of routine
21 deletion of emails after receiving subpoena suggested that defendant “did not intend to deprive
22 [plaintiff] of evidence for litigation but merely allowed the routine e-mail deletion to proceed”).
23 Here, hiQ deleted, or allowed to be deleted, the evidence at issue years *after* the litigation began.
24 There was no rush to delete relevant evidence.

25 **Fourth**, there was no selective preservation of evidence from the lost hiQ accounts aimed
26 at depriving LinkedIn of the relevant information. LinkedIn argues that hiQ selectively archived
27 some “raw scrape” data from AWS that “supported [hiQ’s] story,” but discarded the remaining
28 scraping activity records that supported LinkedIn’s defense or undermined hiQ’s claims. (Docket

1 No. 335-3 at 17–18.) However, hiQ’s CEO testified that he instructed and expected hiQ’s CTO to
 2 archive on a hard drive all the raw data within MongoDB in its existing form. (Docket No. 368-1
 3 Ex. P at 94:24-95:7.) LinkedIn did not point to any evidence that the CTO’s failure to carry out
 4 the instruction was due to an intent to deprive LinkedIn of that information. Amidst hiQ’s dire
 5 financial situation and intense employee turnover, negligence is the more likely explanation to its
 6 failure to preserve evidence.

7 **Finally**, hiQ did attempt to recover the data from AWS, Splunk, and Salesforce. (Docket
 8 No. 368 at 16.) Although largely unsuccessful, such attempts, coupled with the partial production
 9 of Salesforce exports, the Splunk dashboards, and hiQ internal communications on scraping,
 10 indicate a lack of intent to deprive LinkedIn of evidence. *See Gaina v. Northridge Hosp. Med.*
 11 *Ctr.*, No. CV 18-00177-DMG (RAOx), 2018 WL 6258895, at *5 (C.D. Cal. Nov. 21, 2018).
 12 LinkedIn argues that hiQ is not an unsophisticated individual who spoliated evidence, which goes
 13 to show that hiQ should not have lost the evidence in the first place. (Docket No. 387 at 7.) But it
 14 does not diminish the inference from hiQ’s salvation efforts that hiQ did not intend to hide the
 15 evidence from LinkedIn.

16 In sum, although hiQ should have informed LinkedIn and the Court about the impending
 17 closure of its accounts—particularly the AWS account, hiQ’s loss of evidence was not driven by
 18 an intent to deprive LinkedIn of evidence. It was more akin to negligence. “Negligence—even
 19 gross negligence—in failing to retain relevant evidence is not sufficient to support an adverse
 20 inference under Rule 37(e)(2).” *Meta Platforms, Inc. v. BrandTotal Ltd.*, --- F. Supp. 3d. ---, No.
 21 20-CV-07182-JCS, 2022 WL 1990225, at *6 (N.D. Cal. June 6, 2022). Thus, there is insufficient
 22 evidence to find hiQ acted with the requisite intent to warrant harsh Rule 37(e)(2) sanctions.

23 2. hiQ’s Loss Of The Evidence At Issue Has Prejudiced LinkedIn Under Rule
 24 37(e)(1)

25 “Prejudice exists where ‘the [spoiling party’s] actions impaired [the moving party’s] ability
 26 to go to trial or threatened to interfere with the rightful decision of the case.’” *RG Abrams Ins. v.*
 27 *L. Offs. of C.R. Abrams*, 2022 WL 3133293, at *29 (C.D. Cal. July 1, 2022) (quoting *United States*
 28 *ex rel. Wiltec Guam, Inc. v. Kahaluu Constr. Co.*, 857 F.2d 600, 604 (9th Cir. 1988)).

1 Rule 37(e)(1) “does not place a burden of proving or disproving prejudice on one party or
2 the other,” but instead “leaves judges with discretion to determine how best to assess prejudice in
3 particular cases.” Fed. R. Civ. P. 37(e)(1) advisory committee’s note to 2015 amendment. The
4 Committee Notes acknowledge that, in some circumstances, determining the content of lost ESI
5 will be difficult and placing the burden of proving prejudice on the moving party may be unfair.
6 *Id.* Courts have discretion under Rule 37(e)(1) to determine how to assess prejudice on a case-by-
7 case basis. *Id.* “Proving that lost evidence is relevant can be a difficult task, however, because the
8 evidence no longer exists. To show prejudice resulting from the spoliation, therefore, courts have
9 held that a party must only come forward with plausible, concrete suggestions as to what [the
10 destroyed] evidence might have been.” *Fast v. GoDaddy.com LLC*, 340 F.R.D. 326, 339 (D. Ariz.
11 2022) (citations omitted, internal quotation marks omitted).

12 LinkedIn argues that the lost AWS and Splunk data inform the factual questions of (1)
13 “how many requests hiQ’s scraping bots made to LinkedIn’s servers” that “goes directly to hiQ’s
14 argument that LinkedIn cannot show the requisite harm to its system,” and (2) the failure rate (or
15 “ban rate”) of hiQ’s scraping attempts that rebut hiQ’s claim that LinkedIn’s C&D caused hiQ’s
16 business’ downfall. (Docket No. 355-3 at 19, 21.) LinkedIn’s expert explained that “[d]uring the
17 time that hiQ was using Splunk, the deleted data showed the full scope of hiQ’s scraping activity.”
18 (*Id.* (citing Schmidt Decl. at ¶ 13).) And based on hiQ’s source code, the deleted AWS “would
19 have provided enough information to make a much more precise estimate of all the scraping
20 requests from the period before hiQ started using Splunk.” (*Id.* at 19–20 (citing Schmidt Decl. at ¶
21 9).) hiQ responds that hiQ’s produced daily Splunk scraping dashboards and internal
22 communications provide the evidence LinkedIn seeks. (Docket No. 368 at 22.)

23 **Prejudice.** The loss of hiQ’s scraping data prejudiced LinkedIn because it interfered with
24 the accurate determination of the number of hiQ’s scraping requests and the ban rates. Without
25 the lost scraping activity records, LinkedIn had to estimate those numbers by (1) extracting into a
26 table the timestamp, URL, and scrape ID from the raw scrape data produced by hiQ (Schmidt
27 Decl. at ¶ 6), (2) comparing the URL and timestamp to LinkedIn’s activity logs to identify the IP
28 addresses that made the scraping requests, and (3) locating requests in LinkedIn’s server logs

1 associated with the IP addresses. (Docket No. 335-3 at 20.) “The results showed that activity
2 associated with the hiQ IP addresses totaled over 50 billion requests in an 18-month period.” (*Id.*)
3 hiQ avers that LinkedIn could have determined the number of hiQ bot requests to LinkedIn’s
4 server from existing data, but does not explain how to do so. The Court therefore credits
5 LinkedIn’s expert’s testimony that “he would have been able to make a much more precise
6 estimate of the number of scrape attempts, and the success rate of those attempts” from the lost
7 data “than [he] could with the data that was produced.” (Schmidt Decl. at ¶ 9.)

8 The lost scraping records also prejudiced LinkedIn financially. Instead of directly
9 assessing hiQ’s scraping requests from its AWS and Splunk data, LinkedIn had to pay its outside
10 experts and consultants to analyze hiQ’s raw data and use its internal employee time and resources
11 to estimate the numbers. (Docket No. 335-3 at 21.)

12 **Sanctions.** For the destruction of the scraping activity records relating to the number of
13 hiQ scraping attempts, LinkedIn requests that the Court (1) presume that LinkedIn’s expert
14 Xiaofeng Wu’s analysis is correct and that hiQ’s scrapers made at least fifty billion requests on
15 LinkedIn’s servers, (2) issue mandatory adverse inference jury instructions to that effect, and (3)
16 preclude hiQ from offering any evidence to the contrary or otherwise disputing that analysis in
17 connection with summary judgment, Rule 702 motions, and trial. (Docket No. 335-3 at 24.)
18 LinkedIn also seeks costs associated with analysis directed by Mr. Wu, which would have been
19 unnecessary had hiQ retained its scraping activity records and produced them. (*Id.* at 25.)

20 Although LinkedIn was not able to directly assess the number of hiQ’s scraping attempts
21 and the ban rates, it was able to estimate those statistics using other means. Therefore, the
22 prejudice likely does not warrant “the quite extraordinary relief . . . of mandatory adverse
23 inference instructions.” *Chinitz v. Intero Real Est. Servs.*, No. 18-cv-05623-BLF, 2020 WL
24 7389417, at *3 (N.D. Cal. May 13, 2020). The Court therefore will issue *permissive* adverse
25 inference instructions that the jury may presume that (1) LinkedIn’s expert Xiaofeng Wu’s
26 analysis is correct and that hiQ’s scrapers made at least fifty billion requests on LinkedIn’s
27 servers, and that (2) prior to hiQ’s receipt of the C&D letter, LinkedIn’s general technical defenses
28 had blocked hiQ’s anonymous scraping from collecting data to such a degree that hiQ could no

1 longer effectively scrape LinkedIn profiles. LinkedIn’s request for the Court to presume the same
2 in the context of summary judgment is moot as these facts are not necessary to the Court’s ruling
3 on the motions for summary judgment.

4 Additionally, the Court grants LinkedIn’s requests for costs associated with the analysis
5 directed by Mr. Wu that would have been unnecessary but for hiQ’s loss of evidence. The Court
6 also grants LinkedIn’s attorney fees for bringing this motion that would not have been necessary
7 had hiQ carried out its duty to preserve. hiQ opposes based on its “precarious financial position”
8 and that an attorney fee award would be a case-ending sanction—a windfall not appropriate under
9 Rule 37(e)(1). (Docket No. 369 at 24.) But hiQ could have satisfied its duty by notifying
10 LinkedIn of the closure of its various accounts at issue.

11 At this juncture, the Court instructs the Clerk of the Court to file this order, in its entirety,
12 under seal. The Court orders the parties to meet and confer to determine which portions of this
13 order may be publicly filed. The parties shall jointly file their request to file under seal within a
14 week of the date of this order.

15 This order disposes of Docket Nos. 336, 337, 338, 339, and 355.

16
17 **IT IS SO ORDERED.**

18
19 Dated: October 27, 2022

20
21 

22 EDWARD M. CHEN
23 United States District Judge
24
25
26
27
28