COOLEY LLP
SIMONA AGNOLUCCI (246943)
(sagnolucci@cooley.com)
EDUARDO SANTACANA (281668)
(esantacana@cooley.com)
3 Embarcadero Center, 20th Floor
San Francisco, California 94111-4004
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

COOLEY LLP
NATALIE PEELISH *(Appearance Pro Hac Vice)*
(npeelish@cooley.com)
1700 Seventh Avenue, Suite 1900
Seattle, Washington 98101-1355
Telephone: +1 206 452 8700
Facsimile: +1 206 452 8800

Attorneys for Defendant
LINKEDIN CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

NICHOLAS FARRELL, individually and on behalf of all other persons similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

JEFF GANAN, on behalf of himself and all others similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Related Cases:
No. 3:26-cv-02953-VC
No. 3:26-cv-02968-VC

DEFENDANT LINKEDIN CORPORATION'S MOTION TO DISMISS PLAINTIFFS NICHOLAS FARRELL AND JEFF GANAN'S COMPLAINTS

Date: September 3, 2026
Time: 10:00 a.m.
Location: 17th Floor, Courtroom 3
Judge: Hon. Vince Chhabria

Date Action Filed: April 6, 2026

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	BACKGROUND	4
	A. LinkedIn's anti-abuse systems examine browser extension data.	4
	B. LinkedIn's terms prohibit browser add-ons that scrape or copy data from LinkedIn.	4
	C. Farrell's allegations rely on the BrowserGate website.	5
	D. Ganan's allegations substantially replicate the BrowserGate website.	6
III.	LINKEDIN MOVES TO DISMISS FOR LACK OF ARTICLE III STANDING.	7
	A. Plaintiffs factually lack standing.	7
	B. Plaintiffs facially lack standing.	9
IV.	LINKEDIN MOVES TO DISMISS FOR FAILURE TO STATE A CLAIM.	10
	A. Plaintiffs consented to the alleged conduct, defeating all their claims.	11
	B. Plaintiffs fail to allege that LinkedIn unlawfully collected or used any personal information, communication contents, or routing data.	14
	C. Plaintiffs fail to allege plausible invasion of privacy	16
	D. Plaintiffs fail to plead plausible CDAFA claims.	18
	E. Farrell fails to plead a plausible right to publicity claim.	19
	F. Ganan fails to plead a plausible CIPA claim.	20
	1. Ganan's Section 631 allegations are insufficient.	20
	2. Ganan's Section 638.50 and 638.51 allegations are insufficient.	23
	G. Ganan fails to plead a plausible ECPA claim.	24
V.	CONCLUSION	24

TABLE OF AUTHORITIES

Page(s)

Cases

Ambrozewicz v. 6Sense Insights, Inc.,
804 F.Supp.3d 1026 (N.D. Cal. 2025) 20

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....10

Bowen v. Energizer Holdings, Inc.,
118 F.4th 1134 (9th Cir. 2024) 7

Brodsky v. Apple Inc.,
445 F. Supp. 3d 110 (N.D. Cal. 2020) 24

Calhoun v. Google, LLC,
113 F.4th 1141 (9th Cir. 2024) 11, 12

California v. Greenwood,
486 U.S. 35 (1988).....16

Callahan v. Ancestry.com Inc.,
2021 WL 783524 (N.D. Cal. 2021) 10

Cody v. Ring LLC,
718 F. Supp. 3d 993 (N.D. Cal. 2024) 20

Cottle v. Plaid Inc.,
536 F. Supp. 3d 461 (N.D. Cal. 2021) 18

Crano v. Sojern, Inc.,
2026 WL 1670136 (N.D. Cal. 2026) 8

Dellasala et al. v. Samba TV, Inc.,
2026 WL 1138358 (N.D. Cal. Apr. 21, 2026) 19, 21

Doe 1 v. Google LLC,
741 F. Supp.3d 828 (N.D. Cal. 2024) 14, 18, 19

Doe v. Eating Recovery Ctr. LLC,
806 F. Supp. 3d 1109 (N.D. Cal. 2025) 22

Doe v. Tenet Healthcare Corp.,
789 F. Supp. 3d 814 (E.D. Cal. 2025).....18

Esparza v. Kohl's, Inc.,
723 F. Supp. 3d 934 (S.D. Cal. 2024).....9

TABLE OF AUTHORITIES
(continued)

Page(s)

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 16

Goldstein v. Rumble Inc.,
2026 WL 1406766 (C.D. Cal. 2026)....21

Gonzalez v. Planned Parenthood of Los Angeles,
759 F.3d 1112 (9th Cir. 2014) 10

In re Google Location Hist. Litig.,
428 F. Supp. 3d 185 (N.D. Cal. 2019) 16

In re Google, Inc. Priv. Pol'y Litig.,
58 F. Supp. 3d 968 (N.D. Cal. 2014) 17

Hammerling v. Google LLC,
2024 WL 937247 (9th Cir. 2024) 13, 21

Hammerling v. Google, LLC,
615 F. Supp. 3d 1069,1091 (N.D. Cal. 2022) 18

Harrill v. Emanuel Med. Ctr.,
2025 WL 1635428 (E.D. Cal. 2025)....16

Heiting v. HP Inc.,
2025 WL 2993673 (Cal. Super. Ct. 2025)....24

Heiting v. Taro Pharms. USA, Inc.,
709 F. Supp. 3d 1007 (C.D. Cal. 2023) 18, 21, 23

Heiting v. Taro Pharms. USA, Inc.,
728 F. Supp. 3d 1112 (C.D. Cal. 2024) 21

Hernandez v. Hillsides, Inc.,
47 Cal. 4th 272 (2009) 17

Jones v. Peloton Interactive, Inc.,
720 F. Supp. 3d 940 (S.D. Cal. 2024)....23

Lakes v. Ubisoft, Inc.,
777 F.Supp.3d 1047 (N.D. Cal. 2025) 11, 13

Leite v. Crane Co.,
749 F.3d 1117 (9th Cir. 2014) 7

Lineberry v. AddShopper, Inc.,
2025 WL 551864 (N.D. Cal. 2025) 10, 19

TABLE OF AUTHORITIES
(continued)

Page(s)

Love v. Ladder Fin., Inc.,
2024 WL 2104497 (N.D. Cal. 2024) 22

Martin v. Sephora USA, Inc.,
2023 WL 2717636 (E.D. Cal. 2023).....23

Mastel v. Miniclip SA,
549 F. Supp. 3d 1129 (E.D. Cal. 2021).....22

Maya v. Centex Corp.,
658 F.3d 1060 (9th Cir. 2011) 10

Mitchener v. CuriosityStream, Inc.,
815 F. Supp. 3d 845 (N.D. Cal. 2025) 20

Palacios v. Fandom, Inc.,
2024 WL 5494527 (Cal. Super. Ct. 2024).....23

Perez v. Romantix Online, Inc.,
2025 WL 3085786 (N.D. Cal. 2025) 11

Popa v. Microsoft Corp.,
153 F.4th 784 (9th Cir. 2025) 7, 17, 19

Price v. Headspace, Inc.,
2025 WL 1237977 (Cal. Super. Ct. 2025).....20

Rodriguez v. Culligan Int'l Co.,
2025 WL 3064113 (S.D. Cal. Nov. 3, 2025) 17

Rodriguez v. Ford Motor Co.,
722 F. Supp. 3d 1104 (S.D. Cal. 2024).....23

Rodriguez v. Sparc Grp., LLC,
2025 WL 2993671 (Cal. Super. Ct. 2025).....24

Safe Air for Everyone v. Meyer,
373 F.3d 1035 (9th Cir. 2004) 7

Sisti v. Bosley Inc.,
2026 WL 1223927 (C.D. Cal. 2026).....14

Smith v. Facebook, Inc.,
262 F. Supp. 3d 943 (N.D. Cal. 2017 17

Smith v. Facebook, Inc.,
745 F. App'x 8 (9th Cir. 2018) 11, 12

TABLE OF AUTHORITIES
(continued)

Page(s)

Smith v. United States,
2024 WL 2941365 (D. Or. May 31, 2024), *R&R adopted*, 2024 WL 3203287
(D. Or. June 27, 2024) 13, 14

Spokeo, Inc. v. Robins,
578 U.S. 330 (2016).....9

Swarts v. Home Depot, Inc.,
689 F. Supp. 3d 732 (N.D. Cal. 2023) 22

Torres v. SeatGeek, Inc.,
2026 WL 1495202 (N.D. Cal. 2026) 8, 16, 17

TransUnion LLC v. Ramirez,
594 U.S. 413 (2021).....7

Tsao v. Desert Palace, Inc.,
698 F.3d 1128 (9th Cir. 2012) 14

Washington v. Flixbus, Inc.,
2025 WL 1592961 (S.D. Cal. 2025).....11

In re Zynga Priv. Litig.,
750 F.3d 1098 (9th Cir. 2014) 24

Statutes

Cal. Civ. Code § 3344.....11, 19

Cal. Penal Code
§ 502.....11
§ 631..... *passim*
§ 638.50.....20, 23
§ 638.51.....20, 23, 24

California Comprehensive Computer Data Access and Fraud Act 3, 10, 18, 19

Electronic Communications Privacy Act.....3, 11, 24

Other Authorities

Federal Rules of Civil Procedure
8.....19
12(b)(1) 1, 3, 7, 24
12(b)(6) 1, 3, 10, 24

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that the following Motion to Dismiss will be heard on September 3, 2026 at 10:00am PT, or as soon thereafter as counsel may be heard, in Courtroom 3, on the 17th Floor, of the United States District Court for the Northern District of California, located at 450 Golden Gate Avenue, San Francisco, California, 94102, with the Honorable Vince Chhabria presiding. Defendant LinkedIn Corporation will and hereby does move the Court pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for an order dismissing the complaints filed in the related cases *Farrell v. LinkedIn Corp.*, 3:26-cv-02953-VC, ECF 1, and *Ganan v. LinkedIn Corp.*, 3:26-cv-02968-VC, ECF 1. The Motion is based on the pleadings filed herewith, all pleadings and other papers on file in this action, and any other evidence or argument that may be presented to the Court.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

LinkedIn is a social network where members can find jobs, showcase their resumes, and connect with other professionals. Its rich platform and robust community make LinkedIn a target for opportunistic software developers who seek to scrape its data for their own purposes. To protect against unauthorized scraping, fraud, and abuse, LinkedIn deploys multi-layered security systems, including browser-extension (or "add-on") detection systems that identify user software that could scrape or automate behavior on LinkedIn.

Teamfluence, an Estonian platform, is one of those groups that traffics in scraping. It markets a Google Chrome browser plug-in designed to "[i]dentify 100% of your LinkedIn traffic."[1] LinkedIn caught it and banned its CEO from the platform, leading to a legal dispute in Germany. A German tribunal recently determined that "[t]he 'Teamfluence' software violates [LinkedIn's User Agreement]," and that LinkedIn's "suspending the Claimants' user accounts is objectively justified overall and not arbitrary."[2]

---

[1] *See* Peelish Decl., Ex. 5, www.teamfluence.com, at 2. All numbered exhibits refer to those attached to the Declaration of Natalie Peelish in support of LinkedIn's contemporaneously filed Request for Incorporation by Reference and/or Judicial Notice.

[2] *See* Peelish Decl., Ex. 9 (certified translation of Landgericht München I, Mar. 11, 2026, 37 O 104/26 (Ger.)) at 23, 31.

Within a month of the German court order, a shadowy entity dubbed "Fairlinked," which describes itself as an "advocacy group of commercial LinkedIn users,"[3] posted on its website an "investigation" titled "BrowserGate" that proclaims "LinkedIn is running a massive, global, and illegal spying operation on every computer that visits their website."[4] The gist of the so-called "investigation" is that LinkedIn observes whether site visitors are operating certain browser extensions, which Fairlinked claims is a "privacy violation."

No surprise: the founder of Teamfluence sits on Fairlinked's board. Having been caught for scraping, and held to have violated LinkedIn's terms, he has now embarked on an international retaliation campaign by manufacturing a fake privacy controversy. But it is Teamfluence that is scraping data without consent.

These lawsuits are part and parcel of Teamfluence's sour-grapes campaign. The first-filed complaint, by Plaintiff Nicholas Farrell, relies almost entirely on the BrowserGate website, alleging that LinkedIn's self-defense systems violate privacy rights. Farrell additionally contends that LinkedIn shares browser-extension data with third parties who then use it commercially. The second complaint, by Plaintiff Jeff Ganan, represented by Fairlinked's U.S. counsel, essentially copies the BrowserGate website, with a sprinkling of self-contradicting wiretapping and pen register claims on top.

The narrative is false. As LinkedIn has publicly explained, "this is a case of an individual who lost in the court of law, but is seeking to re-litigate in the court of public opinion, without regard for accuracy"—or as one online expert put it, a "nothingburger."[5]

As is evident both from the face of the complaints and from evidence LinkedIn submits with this motion, neither Plaintiff suffered a cognizable injury. As LinkedIn explained to the German court, browser extensions can degrade website function and enable fraud and abuse, harming the site and its members. The purpose of LinkedIn's systems is to identify whether a visitor to the platform is operating a browser extension that could threaten the security and integrity

[3] *See* Peelish Decl., Ex. 6, www.fairlinked.eu, at 1.
[4] *See* Peelish Decl., Ex. 1, www.browsergate.eu, at 3.
[5] Gintaras Radauskas, *Security analyst calls LinkedIn's BrowserGate scandal a giant nothingburger, urges calm*, CYBERNEWS (Apr. 14, 2026), https://cybernews.com/security/linkedin-browsergate-sensationalism-clickbait-debunking/.

of the platform. To accomplish this, LinkedIn detects information that browser extensions openly provide to all websites in order to interact with them. The information is publicly available and in no way private. And LinkedIn's right to detect this information is disclosed and agreed to by all its members. So is LinkedIn's right to use security-focused vendors to detect and prevent potential abuse.

Nothing in either complaint supports a plausible inference that LinkedIn or its vendors use personal data purportedly derived from browser extension detection information to generate profits—nor that any users suffered an invasion of privacy. LinkedIn's evidence in support establishes the opposite. Thus, these complaints fail under Rule 12(b)(1) of the Federal Rules of Civil Procedure.

Moreover, neither Plaintiff has stated a claim under Rule 12(b)(6). The complaints fail to allege that LinkedIn or its vendors use Plaintiffs' data beyond the lawful scope provided for by the consent LinkedIn receives from each of its members. The gravamen of each complaint is that Plaintiffs don't like the specific ways LinkedIn has exercised this consent and chosen to protect itself. But Plaintiffs (and Teamfluence) have no basis to second-guess the implementation of security measures LinkedIn duly disclosed and to which users affirmatively consented.

Plaintiffs' claims suffer from a raft of other defects as well. They fail to plead a reasonable privacy expectation, let alone a highly offensive violation of one. As for their California Comprehensive Computer Data Access and Fraud Act ("CDAFA") claims, both Plaintiffs fall far short of pleading the requisite damage, loss, or unauthorized access. Farrell's right to publicity claim fails to allege a plausible commercial nexus, while Ganan's claims under the California Invasion of Privacy Act ("CIPA") and the federal Electronic Communications Privacy Act ("ECPA") fail to demonstrate that the at-issue data is covered by either statute. Also fatal to all of these claims is that neither Plaintiff offers plausible allegations supported by anything beyond Teamfluence's BrowserGate propaganda and their own information and belief.

It is unfortunate that Teamfluence's machinations have resulted in this wasteful litigation. The Court should dismiss both cases, with prejudice.

II. BACKGROUND

A. LinkedIn's anti-abuse systems examine browser extension data.

Farrell and Ganan base their allegations on LinkedIn's alleged scanning of Chrome browser extensions. Farrell Compl. ¶ 11; Ganan Compl. ¶¶ 4–5. A browser extension is a "small software module[] that can be added onto a web browser for enhanced functionality." Farrell Compl. ¶ 13. Examples of browser extensions include "AI JobScraper," which "[e]xtract[s] job listings from LinkedIn, Upwork and other job boards with ease," "Academic Job Market Scraper," which "[e]xtract[s] job market data for academic research, salary, requirements, location data from job sites," and "Deep Scraper," an "AI-powered browser automation for deep web scraping."[6]

Chrome browser extensions typically include "web_accessible_resources," which are files inside an extension that can be accessed by webpages.[7] In other words, extension developers can voluntarily make certain information inside of their extensions publicly available to webpages. Ganan Compl. ¶ 198 (explaining that "web_accessible_resources" are "exposed to webpages").

Chrome extensions may act as scraping tools or "bots" to scrape or extract data from LinkedIn, often at a cost to LinkedIn's platform and members. Specifically, scraping tools "harvest member data for unauthorized redistribution, generate artificial engagement signals that degrade platform quality, [] execute automated connection requests and messages that can constitute spam," and "consum[e] server capacity and degrad[e] service for legitimate members." Declaration of Tyler Seymour ISO Def. Mot. to Dismiss (Seymour Decl.) ¶ 4.

"To combat the threat of automated scraping and bot activity, LinkedIn deploys multi-layered anti-abuse systems, including browser extension detection systems." *Id.* ¶ 9. LinkedIn also works with security vendors, including HUMAN Security, to assess whether traffic on LinkedIn derives from bots or bad actors. *Id.* ¶¶ 21–23.

B. LinkedIn's terms prohibit browser add-ons that scrape or copy data from LinkedIn.

When any web user (visitor or signed-in member) uses LinkedIn, they agree to LinkedIn's User Agreement. Peelish Decl., Ex. 2 at 2 ("When you use our Services, you agree to all of these

[6] *See* Peelish Decl., Ex. 1 at 26; *see also* https://browsergate.eu/extensions/.
[7] Ex. 1 at 8 (Chrome browser extensions "can expose internal files to web pages through the web_accessible_resources field").

terms"). In so doing, they agree not to "[d]evelop, support or use software … (such as crawlers, **browser plugins and add-ons** or any other technology) to scrape or copy the Services" or "[u]se bots or other unauthorized automated methods to access [LinkedIn's] Services." *Id.* at 8–9 (emphasis added). They also agree not to "[o]verride any security feature or bypass or circumvent any access controls or use limits of the Services." *Id.* at 8.

In addition to prohibiting security threats such as use of bots and scraping, the UA provides that LinkedIn users are subject to LinkedIn's Privacy Policy, Peelish Decl., Ex. 3, and Cookie Policy, Peelish Decl., Ex. 4, which describe how LinkedIn may "collect, use, share, and store [user] personal information." Peelish Decl., Ex. 2 at 2. The Privacy Policy referenced in the User Agreement expressly discloses that, when users "visit or otherwise use [its] Services," LinkedIn may access "device information and internet protocol ('IP') addresses to identify you and log your use," Peelish Decl., Ex. 3 at 4, as well as "information about your network and device (e.g., IP address, proxy server, operating system, **web browser and add-ons**, device identifier and features, cookie IDs and/or ISP, or your mobile carrier)." *Id.* (emphasis added).

LinkedIn discloses it may use such information, including about a user's browser and add-ons, to "prevent or investigate possible fraud or other violations of the law, [its] User Agreement and/or attempts to harm [its] Members, Visitors, company, Affiliates, or others," *id.* at 8; "detect malicious activity and violations of our User Agreement" Peelish Decl., Ex. 4 at 2; and "[i]nvestigate … complaints and for Service issues," Peelish Decl., Ex. 3 at 8.

LinkedIn also tells users that it "may use others to help [it] with [its] Services," including "fraud detection [and] customer support," and that they "will have access to your information … as reasonably necessary to perform these tasks on [LinkedIn's] behalf and are obligated not to disclose or use it for other purposes." *Id.* at 10. It further discloses that it may use data to "conduct research and development for our Services in order to provide our Members and Customers a better, more intuitive, and personalized experience, drive membership growth and engagement on our Services, and help connect professionals to economic opportunity." *Id.* at 7.

C. Farrell's allegations rely on the BrowserGate website.

Farrell unabashedly rests nearly his entire complaint on the BrowserGate "investigation."

Farrell Compl. ¶¶ 12–25. He alleges that he is a "regular user of LinkedIn" and that he "has long had several browser extensions installed" on a Chrome browser from which he accessed LinkedIn, *id.* ¶¶ 23–24, yet he fails to mention which extensions he had installed at the time. Parroting the BrowserGate website and on "information and belief," Farrell alleges that LinkedIn (1) "surreptitiously executed a fingerprinting script, looking for known browser extension identifiers within Farrell's computer and computer systems," (2) without his consent, (3) in order to "amass a profile and build a dossier on [him]," (4) so that LinkedIn "could use his name and likeness in advertising or selling its products to him, or soliciting purchases of products, merchandise, goods, or services by him," *id.* ¶¶ 24–25. Farrell identifies no such advertisements. Farrell claims LinkedIn has not disclosed the alleged conduct in its Privacy Policy. *Id.* ¶ 19. He seeks to represent a proposed class of "all persons in the United States who logged into LinkedIn using a Chrome browser." *Id.* ¶ 26.

D. Ganan's allegations substantially replicate the BrowserGate website.

Ganan's allegations effectively mirror the BrowserGate website. *Compare* Peelish Decl., Ex. 1 at 7–14, *with* Ganan Compl. ¶¶ 1–10. His counsel also represents the group behind BrowserGate. *See* Ganan Opp. re Mot. to Consolidate at 7–8, No. 3:26-cv-02968-VC, ECF 25. Ganan generally claims that LinkedIn collected information about browser extensions that were linkable to LinkedIn members, "package[d] those results into a session-linked anti-abuse fingerprint," sent the data to "LinkedIn-controlled telemetry endpoints," and shared "source-identifying session metadata" with third parties. Ganan Compl. ¶¶ 4, 5, 9, 61, 62, 73. Ganan alleges that these third parties used the information they received to, *inter alia*, "enhance their own products" and "support offerings provided or sold to other clients." *Id.* ¶ 73.

According to his complaint, Ganan used the Chrome browser to access LinkedIn's website; he does not, however, allege whether he had any extensions installed, or if so, which ones. *Id.* ¶ 11. He claims, regardless, that he did not consent to the security measures taken by LinkedIn. *Id.* ¶¶ 11, 21. Ganan does not allege that this information was used for targeted advertising; instead, he alleges that the security measures taken by LinkedIn were more intrusive than necessary to accomplish the goals disclosed by the Privacy Policy. *Id.* ¶ 77. Ganan brings claims on behalf of a

proposed nationwide class and California subclass of "[a]ll Chrome browser users with a LinkedIn account who accessed LinkedIn.com." *Id.* ¶ 138–39.

III. LINKEDIN MOVES TO DISMISS FOR LACK OF ARTICLE III STANDING.

Plaintiffs lack Article III standing to bring any of their claims because (1) LinkedIn's evidence demonstrates that Plaintiffs could not have suffered the harms they allege to have suffered; and (2) even taking the complaints on their own, they fail to plausibly allege those harms.

To establish standing, a plaintiff must show "that he suffered an injury in fact that is concrete, particularized, and actual or imminent." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). Defendants may challenge standing via Rule 12(b)(1), which permits dismissal for lack of subject matter jurisdiction, "in one of two ways." *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). "A factual attack on jurisdiction 'contests the truth of the plaintiff's factual allegations, usually by introducing evidence outside the pleadings.'" *Bowen v. Energizer Holdings, Inc.*, 118 F.4th 1134, 1142 n.6 (9th Cir. 2024) (internal citation omitted). By contrast, a "facial" attack accepts the truth of the plaintiff's allegations but asserts that they "are insufficient on their face to invoke federal jurisdiction." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Here, LinkedIn brings both attacks.

A. Plaintiffs factually lack standing.

"*TransUnion* requires a court to assess whether an individual plaintiff has suffered a harm that has traditionally been actionable in our nation's legal system." *Popa v. Microsoft Corp.*, 153 F.4th 784, 791 (9th Cir. 2025). Plaintiffs' pleadings primarily assert standing based on an alleged invasion of their reasonable expectation of privacy. *See* Farrell Compl. ¶¶ 67–69, 80; Ganan Compl. ¶¶ 185, 218, 246, 274, 287, 297. They also claim to have suffered economic harm because of alleged use of the data by LinkedIn and third parties. *See, e.g.*, Farrell Compl. ¶¶ 51, 53, 54; Ganan Compl. ¶¶ 179, 192, 252. The Declaration disproves Plaintiffs' allegations.

LinkedIn's Declaration in support of this motion demonstrates that Plaintiffs suffered no injury and therefore lack Article III standing. ***First***, there can be no reasonable expectation of privacy over the browser extension data LinkedIn observes. Users voluntarily choose to download browser extensions for "enhanced functionality" while browsing the web. Farrell Compl. ¶ 13. In

other words, they want to change how their browser interacts with websites. To effectuate this, browser extension developers tell websites, like LinkedIn, which extensions are installed; LinkedIn merely looks at the extension's publicly accessible files designated as "web_accessible_resources." *See* Ganan Compl. ¶ 198; Seymour Decl. ¶¶ 10-14. The browser extension data is intentionally exposed to websites by the user's browser; it cannot reasonably be expected to remain private. As a result, Plaintiffs could not have suffered a privacy harm.

As for the "fingerprinting" data Ganan alleges to be transmitted to third parties—i.e., "content-bearing page-context fields such as href, pathname, hash, and related location or page-state values," Ganan Compl. ¶¶ 71, 116—it is the sort of information that courts have found to be "routine browser information" that does not fall within a reasonable expectation of privacy. *See, e.g.*, *Torres v. SeatGeek, Inc.*, 2026 WL 1495202, at *4 (N.D. Cal. 2026). Ganan "identifies no embarrassing, invasive, or otherwise private information collected by [LinkedIn]." *Crano v. Sojern, Inc.*, 2026 WL 1670136, at *3 (N.D. Cal. 2026) (quoting *Popa*, 153 F.4th at 791 and dismissing complaint for lack of standing). As in *Sojern*, Ganan fails to allege anyone "actually collected Plaintiff's personal information." *Id.*

Second, Plaintiffs could not have suffered an economic injury because no party used the data to generate financial gains. Setting aside Plaintiffs' (and the BrowserGate website's) wild speculation, the truth is that LinkedIn never used and does not use browser extension detection data for revenue-generating, marketing, or advertising purposes; nor does it link those data to member identities, except in furtherance of servicing the member's account or securing the platform. Seymour Decl. ¶¶ 16–18. Browser extension data are retained only for the anti-abuse analysis and customer support services disclosed in LinkedIn's Privacy Policy. *Id.* ¶ 16. There is no basis for crediting unsupported allegations about "dossiers" or any other economic benefits LinkedIn purportedly derived from the at-issue data.

As for its security vendors, LinkedIn uses them to enforce its clearly disclosed terms and policies (to which Plaintiffs consented, *see infra* § IV.A.), not for any revenue-generating purpose. LinkedIn does not share browser extension detection results with *any* third party. Seymour Decl. ¶ 20. Plaintiffs accuse LinkedIn of "surreptitiously" transmitting data to one vendor in particular,

HUMAN Security, *see, e.g.*, Farrell Compl. ¶ 17, Ganan Compl. ¶ 56. But HUMAN can only use the data sent from LinkedIn for the purpose of distinguishing bot traffic from genuine human traffic. Seymour Decl. ¶¶ 22–23 & Ex. A at 20 (LinkedIn-HUMAN Data Processing Agreement) ("[HUMAN] hereby certifies that it does not … derive value from the processing or use of LinkedIn Personal Data … [I]t does not and will not sell LinkedIn Personal Data … it may not retain, use or disclose LinkedIn Personal Data except as is necessary to provide services to LinkedIn."). And, in fact, the transmitted data *does not include browser extension detection results*, but only record information about web traffic. There can be no harm caused by sharing basic data with a vendor who uses it solely in furtherance of purposes to which Plaintiffs expressly agreed.

B. Plaintiffs facially lack standing.

Even accepting Plaintiffs' allegations as true, their complaints fail to state a cognizable Article III injury. As a threshold deficiency that dooms their complaints, neither Plaintiff alleges a concrete, particularized privacy injury that *they* suffered. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (a cognizable injury must be "particularized," meaning it "affect[s] the plaintiff in a personal and individual way") (citation omitted).

Where a complaint "does not plead any facts to suggest Defendant collected intimate or sensitive personally identifiable information," generally alleging that software captures "personal details and browsing history, and IP address[es], is insufficient to demonstrate the Defendant's conduct constituted a serious invasion of a protected privacy interest." *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 946 (S.D. Cal. 2024) (cleaned up). Plaintiffs' complaints do not establish collection of their data, let alone that any collected data was intimate or sensitive. They therefore fail to show any privacy harm actionable at common law.[8]

For his part, Ganan does not allege he has any extensions installed at all, much less one

[8] Farrell quotes the BrowserGate website for the allegation that LinkedIn searches extensions that correlate to religious or political beliefs. Farrell Compl. ¶ 22. The cited extensions are designed to modify social media sites like LinkedIn. *See, e.g.*, Peelish Decl., Ex. 7, PordaAI (depicting blurring on social media websites); Peelish Decl., Ex. 8 at 1, Anti-Woke Tag (explaining that the extension "[s]hows warnings about woke companies"). LinkedIn may search for such extensions because their web accessible resources file indicates that they interact with social media sites in ways that could extract data. Seymour Decl. ¶¶ 10-14. At any rate, knowing that a user does or does not have a particular extension installed fails to establish anything private about them.

that would be private. Ganan Compl. ¶ 50 (alleging LinkedIn searched for "extension-related … absence information"). He further concedes that extension information is web accessible. *Id.* ¶ 198.

Farrell alleges only that he has "long had several browser extensions installed," without identifying a single one by name. Farrell Compl. ¶ 23. Neither LinkedIn nor the Court can assess whether anyone ever learned anything about him, much less something private. And, indeed, LinkedIn doesn't detect every extension; it could be that none of Farrell's extensions are among those LinkedIn detects.

Nor does either Plaintiff explain how there could be any economic value to whatever data is allegedly used by third parties—kneecapping their claims of economic loss. *See, e.g.*, Farrell Compl. ¶ 81, Ganan Compl. ¶ 302. To plead cognizable injury, a complaint must "articulate that theory of loss in a concrete way." *Lineberry v. AddShopper, Inc.*, 2025 WL 551864, at *2 (N.D. Cal. 2025). But these complaints do not "allege[] that there is a market for individual people's browsing activity, nor anything about what the actual value of the plaintiffs' data could be … [nor] whether a person can still sell their data if [LinkedIn already has it], nor how the value of a person's data decreases when their data is misappropriated." *Id.*; *see also Callahan v. Ancestry.com Inc.*, 2021 WL 783524, at *4–*5 (N.D. Cal. 2021) (a "plaintiff must do more than point to the dollars in a defendant's pocket; he must sufficiently allege that in the process he lost dollars of his own"). As in *Callahan* and *Lineberry*, neither Plaintiff alleges any sort of concrete economic injury.[9]

IV. LINKEDIN MOVES TO DISMISS FOR FAILURE TO STATE A CLAIM.

Rule 12(b)(6) requires dismissal of a cause of action that fails to state a claim upon which relief can be granted. A plaintiff must plead factual allegations that "plausibly (not merely conceivably) entitle plaintiff to relief." *Maya v. Centex Corp.*, 658 F.3d 1060, 1067–68 (9th Cir. 2011). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The Court may disregard "allegations that contradict matters properly subject to judicial notice or by exhibit." *Gonzalez v. Planned Parenthood of Los Angeles*, 759 F.3d 1112, 1115 (9th Cir. 2014) (citations omitted).

[9] As an additional claimed injury, Ganan regurgitates an element of his CDAFA claim verbatim to assert actual harm to his data or computer. Ganan Compl. ¶ 219. Ganan also alleges having spent $100 on investigating and/or repairing the harms he discovered (none of which he identifies). *Id.* ¶ 218. These conclusory allegations are implausible. *See* § IV.D. *infra*.

A. Plaintiffs consented to the alleged conduct, defeating all their claims.

Plaintiffs strive mightily to suggest that they did not consent to LinkedIn "scann[ing] its users' devices in order to detect what browser extensions they had installed" and "shar[ing] that data with third parties." *See, e.g.*, Farrell Compl. ¶¶ 45–47, 63, 76, 87; Ganan Compl. ¶¶ 10, 180, 192, 217, 240, 264, 284, 294. *For good reason:* if they consented, their claims fail. *See Lakes v. Ubisoft, Inc.*, 777 F.Supp.3d 1047, 1054 (N.D. Cal. 2025) (consent defeats CIPA, ECPA, invasion of privacy/ intrusion upon seclusion claims); *see also* Cal. Penal Code § 502 (CDAFA) (requiring alleged violations be "unauthorized"), Cal. Civ. Code § 3344 (requiring action "without such person's prior consent").

In assessing consent, courts consider "whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization." *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8 (9th Cir. 2018). The key questions are whether "the person alleging harm consented 'to the particular conduct, or to substantially the same conduct'" and whether "the alleged tortfeasor did not exceed the scope of that consent." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024) (quoting *Tsao v. Desert Palace, Inc.*, 698 F.3d 1128, 1149 (9th Cir. 2012)). In disputing consent, Plaintiffs must allege more than bare assertions. *See Perez v. Romantix Online, Inc.*, 2025 WL 3085786, at *2–*3 (N.D. Cal. 2025) (dismissing claims because plaintiffs failed to allege "what they knew of the [privacy] policy [on the website], when they knew it, and whether that information had any effect on their decisions related to the site").

Farrell. Farrell asserts that he has been a "regular" user of LinkedIn for over ten years. Farrell Compl. ¶ 23. As explained *supra*, this means that he agreed to LinkedIn's User Agreement, which incorporates the Privacy Policy and Cookie Policy. *See* Peelish Decl., Ex. 2 at 2. His continued use constitutes repeated consent to those terms. Unable to ignore this fact, Farrell relies on identical conclusory statements that he did not consent to the alleged conduct because LinkedIn "has not disclosed this practice in its Privacy Policy" and that "there is no mention of extension scanning in any public-facing document" of LinkedIn. Farrell Compl. ¶¶ 3, 24, 53, 63, 76, 85.

Farrell pleads nothing to support those statements and his conclusory allegations cannot sustain his claims. *See Washington v. Flixbus, Inc.*, 2025 WL 1592961, at *3 (S.D. Cal. 2025)

(refusing to accept as true the "legal conclusion" that plaintiff "did not consent to the data practices at issue in the complaint.").

In any event, the relevant policies flatly contradict his no-consent allegations. Browser extensions are, by definition and as alleged by both Plaintiffs, add-ons to a web browser, and LinkedIn discloses that it collects information about members' "**web browser and add-ons**." Peelish Decl., Ex. 3 at 4 (emphasis added). Because Plaintiff consented "to substantially the same conduct" that he alleges—i.e., collecting information about browser add-ons—he fails to state any of his claims. *See Calhoun*, 113 F.4th at 1147. He also consented to having LinkedIn "use your data (including your communications) for security purposes or to prevent or investigate possible fraud or other violations of the law." Peelish Decl., Ex. 3 at 8. And he consented to letting LinkedIn "use cookies to enable and support our security features, keep your account safe and to help us detect malicious activity and violations of our User Agreement." Peelish Decl., Ex. 4 at 2. In other words, LinkedIn discloses that it may use data derived from member browsing sessions to prevent fraud and abuse of its platform. In this respect, "the practice complained of falls within the scope of Plaintiffs' consent to [LinkedIn's] Terms and Policies." *Smith*, 745 F.App'x at 9.

The policies also defeat Farrell's allegation that LinkedIn shares his information with third parties without his consent. *See, e.g.*, Farrell Compl. ¶ 50. LinkedIn discloses that it "use[s] others to help us provide our Services," including, *inter alia*, "fraud detection," and that these third parties "will have access to your information … as reasonably necessary to perform these tasks." Peelish Decl., Ex. 3 at 10. In other words, LinkedIn told users—who necessarily agreed to the User Agreement in the first place—that it may share data with third parties like HUMAN to provide its services. Farrell's characterization of the HUMAN pixel as a secret, undisclosed transmission cannot survive this provision. *See Smith*, 745 F. App'x at 9.

Finally, Farrell's commercial exploitation theory cannot stand where LinkedIn explains that it uses data about members to "conduct research and development for our Services in order to provide our Members and Customers a better, more intuitive, and personalized experience, drive membership growth and engagement on our Services, and help connect professionals to economic opportunity." Peelish Decl., Ex. 3 at 7. It is telling that the complaint cites this very "growth and

engagement" language as supposed evidence of wrongdoing. If this is all the support he can identify, it cannot amount to behavior beyond the scope of his consent. Farrell Compl. ¶ 25.[10]

Ganan. Ganan concedes he consented to LinkedIn's use of web browser add-ons to detect and combat fraud and abuse. *See, e.g.*, Ganan Compl. ¶ 90 (acknowledging "acceptance of broad terms of service" and "awareness that LinkedIn receives routine browser information"). Yet he claims that LinkedIn's actual anti-abuse conduct went beyond the scope of that consent. *See id.* ¶ 270 ("General references to … add-ons … did not amount to consent to the covert contents-interception scheme alleged herein"); *see also id.* ¶¶ 74, 76, 97, 240.

These allegations are insufficient in light of the policies to which he agreed. As explained *supra*, LinkedIn expressly discloses that when members "visit or otherwise use [its] Services," it gains access to "device information and internet protocol ('IP') addresses to identify and log your use," as well as "information about your … web browser and add-ons [and] device identifier and features[.]" Peelish Decl., Ex. 3 at 4.

Courts routinely reject arguments that, for consent to be valid, implementation and related details must be specified at the level Ganan suggests—particularly in the pixel tracking context. *Smith*, 745 F. App'x at 8–9 (affirming dismissal in part because Facebook's terms and policies contained numerous disclosures related to information collection on third-party websites); *Hammerling v. Google LLC*, 2024 WL 937247, at *3 (9th Cir. 2024) (affirming dismissal of invasion of privacy claim because there is "no reasonable expectation of privacy in that data" collection which a "[p]olicy … expressly disclosed").

In *Lakes v. Ubisoft, Inc.*, the court reasoned that user consent warranted dismissal of claims that a website's use of the Meta Facebook pixel violated all the laws cited here (excepting the right to publicity statute). *See* 777 F. Supp. 3d at 1057. The court emphasized that there was no support for the high specificity standard that the plaintiffs had invoked. *See id.* (rejecting claims that consent required some sort of "highly granular disclosure" about a tracking pixel that could allegedly identify an individual users' web activity). This is especially true here, where Ganan fails

[10] Farrell quotes the BrowserGate website for an allegation that LinkedIn also tracks "Do Not Track" browser preferences. Farrell Compl. ¶ 16. Yet he fails to allege whether his browser featured such a preference or what, specifically, that preference would mean. This stray sentence is too flimsy to support any of his claims.

to explain *how* or *why* the data collection supposedly exceeded necessity. Where such "important allegations [a]re conclusory," dismissal is warranted. *See Doe 1 v. Google LLC*, 741 F. Supp.3d 828, 849 (N.D. Cal. 2024).

To the extent Ganan alleges that LinkedIn's integration of third-party security vendors was undisclosed, he is wrong. LinkedIn explicitly highlights that it uses "cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) … We also allow some others to use cookies as described in our Cookie Policy[.]" Peelish Decl., Ex. 3 at 4. Ganan's fingerprinting allegations describe precisely the security technology and third-party activity that LinkedIn discloses. *See, e.g.*, Ganan Compl. ¶ 270. He therefore consented "to the particular conduct" alleged. *Tsao*, 698 F.3d at 1149; *see also Sisti v. Bosley Inc.*, 2026 WL 1223927, at *6 (C.D. Cal. 2026) (holding consent defeated privacy claims where plaintiff consented to "exactly the practice" complained of in the complaint).

While Ganan may have preferred that LinkedIn used his data in a different way to combat fraud and abuse, that is not for him to decide. LinkedIn provided reasonable disclosures about its data collection and use, and Ganan, in choosing to use LinkedIn's services, consented to the alleged conduct. He cannot now dictate how LinkedIn conducts its security or anti-fraud efforts.

B. Plaintiffs fail to allege that LinkedIn unlawfully collected or used any personal information, communication contents, or routing data.

The crux of Plaintiffs' complaints is the theory that (1) LinkedIn unlawfully collected browser extension data that was linked to personal identities, and (2) LinkedIn, or third parties with whom it shared data, used that personal information. Yet neither complaint offers *any* plausible allegations that LinkedIn unlawfully collected, let alone unlawfully used, or shared with a third party, Plaintiff's browser-related extension data, or any other data. These failures undergird each Plaintiffs' claims, and each must fall for the same reason.

Farrell. Farrell bases his allegations on "information and belief." But "conclusory allegations based on information and belief are insufficient, they must be supported by factual assertions allowing a plausible inference." *Smith v. United States*, 2024 WL 2941365, at *4 (D. Or. May 31, 2024), *R&R adopted*, 2024 WL 3203287 (D. Or. June 27, 2024) (citation omitted). The only "factual" predicate for Farrell's 19-page complaint is the BrowserGate website: an

unsubstantiated, made-for-litigation report published by an advocacy group that seeks revenge on LinkedIn for having suffered the consequences of violating LinkedIn's policies. Ganan Decl. ISO Opp. re Mot. To Consolidate Ex. A, No. 3:26-cv-2968-VC (N.D., Cal. June 4, 2026), ECF 25-3 (press release). Rather than substantiate the so-called "investigation" with plausible factual allegations of his own, Farrell's investigation concededly consisted of reviewing "numerous reports and articles" and "reviewing the publicly-available code" of LinkedIn's website. Drury Decl. ISO Pl.'s Mot. Appt. of Interim Counsel at 4, ECF 26-1. Such bare-bones allegations cannot withstand Rule 12.

Ganan. Despite its wrappings of technical jargon, Ganan's complaint suffers from the same deficiency as Farrell's: It fails to allege with any particularity that LinkedIn *actually* caused any privacy or economic harm. Empty inferences are not plausible pleadings, but they are all Ganan offers. He alleges the collected data "were ***linkable*** to identified or identifiable California users, including" himself, Ganan Compl. ¶ 9 (emphasis added), yet he fails to allege that they were, in fact, ***linked*** to his (or anyone else's) identity. *See also id.* ¶ 93 (alleging the signals LinkedIn examines "were reasonably *capable of* identifying, singling out, or being linked to a particular user"), ¶ 94 ("the resulting data … *supported* ready inference about" user characteristics); ¶ 95 ("LinkedIn itself *possessed* the contextual data necessary to make such inferences"); ¶ 96 ("LinkedIn's own internal collection and inference systems *could* nevertheless reveal or support inferences about a member's job-seeking or other sensitive interests.") (emphases added).

Ultimately, Ganan relies on implausible inferential leaps. For example, he alleges that LinkedIn secretly shared browser extension data with third parties—i.e., LinkedIn's "anti-fraud partners" and "anti-abuse partners," *id.* ¶ 72—then jumps to the conclusion that these partners may use such data "not merely to assist LinkedIn in a single fraud or abuse decision," but also to, "enhance their own products and services, improve analytics and predictive models, generate benchmarking outputs, and support offerings provided or sold to other clients." *Id.* ¶ 73. This conclusory assertion is based not on plausible facts but rather uncited, conditional statements made by a single, ***unidentified*** alleged data "recipient," about ***some*** product (it is unclear which) that collects some subset of data. *Id.* Such vague, unsupported speculation falls well beneath Rule 12's

plausibility bar.

C. Plaintiffs fail to allege plausible invasion of privacy.

Plaintiffs allege that the collection of browser extension data combined with other LinkedIn account data amounts to an invasion of privacy and intrusion upon seclusion. *E.g.*, *id.* ¶¶ 93, 281; Farrell Compl. ¶ 63. These claims fail because neither Plaintiff plausibly alleges a reasonable expectation of privacy in browser extension data or the other routine data collected, nor that the alleged intrusion was highly offensive. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (identifying elements of the claims). Courts analyze the "effectively identical" claims together. *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 196 (N.D. Cal. 2019).

No reasonable expectation of privacy. In browser privacy cases, plaintiffs must plead that "browsing information was embarrassing or sensitive data." *Torres*, 2026 WL 1495202, at *7. Vague "allegations regarding … browsing activity" do not "sufficiently allege[] a reasonable expectation of privacy." *Harrill v. Emanuel Med. Ctr.*, 2025 WL 1635428, at *6 (E.D. Cal. 2025).

Here, for all their bluster, neither Plaintiff plausibly alleges that any purportedly sensitive information, e.g., about a user's membership of a protected class, was actually linked to any identifiable user or that any of their own allegedly sensitive data was at issue. This is fatal. Ganan himself concedes that the information purportedly shared with third parties is "*not* sensitive." Ganan Compl. ¶ 264. As for Farrell, even if he were to elaborate about the extensions he allegedly used, he would still need to explain why they reveal anything other than unprotected general activity. Learning that Ganan, for example, used the Teamfluence extension to scrape LinkedIn (unlawfully) and "track profiles," is hardly the stuff of LinkedIn invading his privacy. Plaintiffs ask the Court to take it on faith that private information was taken. The laws, however, punish actual conduct, not theoretical harms.

Further, "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *California v. Greenwood*, 486 U.S. 35, 41 (1988). Ganan acknowledges that "extension developers expose particular resources as web-accessible." Ganan Compl. ¶ 49; *see also id.* ¶ 198. Farrell, for his part, relies on the BrowserGate website, which in turn concedes

that "Chrome extensions can expose internal files to web pages through the web_accessible_resources field in their manifest.json." Because both complaints (or the documents on which they are based) acknowledge that this information is publicly web accessible, neither demonstrates a legitimate expectation of privacy. *See supra* § III.A.

Finally, beyond extension data, Plaintiffs can hardly claim that they have a reasonable expectation of privacy in routine identifiers of the ilk alleged here—e.g., "browser-resident traces, device-resident characteristics, session-linked identifiers, and other browser and device information." Ganan Compl. ¶ 280. Courts have consistently held that internet users have no expectation of privacy in "IP addresses, device make/model/OS, browser type, and cookie identifiers," *Torres*, 2026 WL 1495202, at *4, or in their "email address or webpage username," "in their IP addresses," or in the "metadata of their internet communications." *Rodriguez v. Culligan Int'l Co.*, 2025 WL 3064113, at *4–*5 (S.D. Cal. Nov. 3, 2025) (collecting cases).

At any rate, Plaintiffs' consent to LinkedIn's clear disclosures underscores the extent to which Plaintiffs lack a reasonable expectation of privacy. *See* § IV.A., *supra.* They were on notice of and agreed to the alleged activity. *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("He who consents to an act is not wronged by it." (citation omitted)).

No highly offensive intrusion. Sufficiently pleading a "highly offensive" invasion of privacy or intrusion requires pleading an action that is "so serious in nature, scope and actual or potential impact as to constitute an egregious breach of the social norms." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009) (internal quotes omitted). "Courts … have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." *In re Google, Inc. Priv. Pol'y Litig.,* 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014). If Plaintiffs "identif[y] no embarrassing, invasive, or otherwise private information collected … the monitoring of [their] interactions with [a] website seems most similar to a store clerk's observing shoppers in order to … spot problems[.]" *Popa*, 153 F.4th at 791.

Neither complaint pleads highly offensive activity to the level California law requires. Plaintiffs allege that LinkedIn detected publicly exposed browser extension information while

collecting routine (and disclosed) browser, device, and session-related data, without plausibly alleging that any of it was *actually* linked to any specific user for any undisclosed purpose. Indeed, nothing in either complaint suggests that information about either Plaintiff's religious, political affiliations and beliefs, or personal health information was collected, shared, or used. Nor that any data about their own extensions was revealed at all, if they even used them while visiting LinkedIn's website. Accordingly, Plaintiffs have failed to allege any highly offensive intrusion. *See Hammerling v. Google, LLC*, 615 F. Supp. 3d 1069,1091 (N.D. Cal. 2022) (privacy claims failed because "Plaintiffs do not allege that the data allegedly collected … is sufficiently specific or personal, and its collection sufficiently harmful, to be highly offensive.").

D. Plaintiffs fail to plead plausible CDAFA claims.

Plaintiffs claim that LinkedIn violated CDAFA because it knowingly and without authorization scanned its users' devices to detect what browser extensions they had installed, and then allegedly shared that browser extension data with third parties. Farrell Compl. ¶¶ 46–48; Ganan Compl. ¶ 190. These allegations fail to state a CDAFA claim for several reasons.

Neither Plaintiff plausibly pleads that they "suffer[ed] damage or loss," as required to confer standing under the statute. *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1020 (C.D. Cal. 2023). Neither one sufficiently alleges physical damage to their "computer system, network, program, or data contained on that computer." *Id.* at 1021. *See also Doe v. Tenet Healthcare Corp*., 789 F. Supp. 3d 814, 845 (E.D. Cal. 2025) (dismissing CDAFA claim because "Plaintiffs have failed to plead any measurable decrease in storage, memory, or any other impairment to their computing devices' functioning"); *Doe I*, 741 F. Supp. 3d at 846 (dismissing CDAFA claim because "plaintiffs' alleged damage [of] reduced storage, disk space, and performance of their computers" did not establish standing); *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 487 (N.D. Cal. 2021) (similar).

While Ganan includes boilerplate allegations that he spent $100 to "protect his devices and identity after learning of these data breach and extraction issues," *e.g.*, Ganan Compl. ¶ 218, these conclusory allegations are insufficient to support a claim for compensatory loss, particularly where there is no allegation Ganan undertook any investigation to verify that his device was not

impacted by the alleged conduct, nor any allegation of what damage he supposedly discovered.

Plaintiffs do not plausibly plead economic loss, either. Farrell, for his part, claims that LinkedIn "profited by appropriating Plaintiff's and Class members' valuable data without sharing those profits with Plaintiff and Class members." Farrell Compl. ¶¶ 53–54. But he never alleges how he supposedly suffered an "economic loss" from any misappropriation: He does not allege any market for individual browser extension data, that he would have participated in that market, nor that the value of his data decreased because it was allegedly misappropriated. *Lineberry, Inc.*, 2025 WL 551864, at *2 (dismissing CDAFA claims for lack of statutory standing where complaint failed to adequately plead economic loss); *see also Dellasala et al. v. Samba TV, Inc.*, 2026 WL 1138358, at *9 (N.D. Cal. Apr. 21, 2026).[11]

In any event, allegations that the conduct was without authorization fail for the reasons discussed *supra*, § IV.A.

E. Farrell fails to plead a plausible right to publicity claim.

The right to publicity statute that Farrell invokes requires showing that a person "knowingly uses another's name … or likeness … for purposes of advertising or selling or soliciting purchases … without that person's prior consent[.]" Cal. Civ. Code § 3344. Farrell baldly alleges that LinkedIn sought "to amass profiles and build dossiers" so that it could "advertise its products to Plaintiff and Class members." Farrell Compl. ¶ 87.

Yet Farrell could not marshal a single allegation that any advertisement ***actually*** "use[d]" his identity, falling short of the plausibility bar. A complaint must do more than merely "identif[y] potential harms that *might* be associated with [a] technology." *See Popa*, 153 F. 4th at 791 n.5. Vague, metaphysical allegations that LinkedIn "could" use browser extension information to potentially build some kind of profile fails to pass Rule 8's pleading threshold, let alone Rule 12's plausibility bar. *See Doe I*, 741 F. Supp. 3d at 839 ("instead of offering factual allegations … plaintiffs allege hypothetical examples").

Moreover, even if it were true that LinkedIn creates profiles or dossiers based on extension data (and it is not true), Farrell fails to allege any plausible facts that suggest such dossiers have

[11] Ganan's aside that third parties engaged in "nonconsensual monetization" of user data, Compl. ¶ 192, is a vague, generalized assertion that does not suffice to establish plausible economic loss.

a commercial purpose. "In right to publicity statutes, the context concerns the commercial use of an individual's identity. Plaintiffs' allegations, on the other hand, present no commercial nexus between any one individual identity and" LinkedIn's commercial activity. *Ambrozewicz v. 6Sense Insights, Inc.*, 804 F.Supp.3d 1026, 1035 (N.D. Cal. 2025).

F. Ganan fails to plead a plausible CIPA claim.

CIPA contains a section about intercepting or eavesdropping on contents of a communication, Cal. Penal Code § 631(a), and a different section about tracking or collecting routing information (e.g., a phone number), *id.* § 638.50(b). By definition, these two categories of information are distinct: data could be contents or routing information (or something else), but they cannot be both. *See id.* (explaining that a pen register captures "dialing, routing, addressing, or signaling information … but not the contents of a communication.").

Ganan quizzically alleges that the same data are both: "contents" under Section 631 and "routing information" under Section 638.51. Courts don't allow that. *Mitchener v. CuriosityStream, Inc.*, 815 F. Supp. 3d 845, 852 (N.D. Cal. 2025) (dismissing Section 638.51 claim where plaintiff alleged that the technology at issue captured content information); *Price v. Headspace, Inc.*, 2025 WL 1237977, at *3 (Cal. Super. Ct. 2025) (pen registers provide information about the "'who,' 'when,' and 'where' of communications—but not the 'what'"). The data in question are neither.

1. Ganan's Section 631 allegations are insufficient.

Ganan appears to base his California Penal Code Section 631 allegations that LinkedIn caused his data, including "duplicated content-bearing href, pathname, hash, and related page-context fields" "to be transmitted to" "undisclosed third-party data partners, anti-fraud partners, anti-abuse partners" who then "use[] that content data for their own purposes." Ganan Compl. ¶ 263, *see also id.* ¶¶ 258–59. He limits this claim to only Section 631(a)'s fourth clause—that LinkedIn aided and abetted "undisclosed" third parties in CIPA violations. *Id.* ¶¶ 252, 254; *see* Cal. Penal Code § 631(a). As a result, he must plausibly allege an "underlying third-party violation" of the preceding three clauses in order to state his claim. *See Cody v. Ring LLC*, 718 F. Supp. 3d 993, 1003 (N.D. Cal. 2024). Section 631(a)'s first three clauses prohibit intentionally

making an unauthorized wire connection, reading or attempting to read the contents of a message while it is in transit over a wire, or using any information so obtained. *Id.* As outlined below, Ganan fails to plausibly allege a third-party predicate violation, so his aiding and abetting theory fails.

Not contents. Ganan's CIPA claim fails because the data at issue—e.g., "href values, pathnames, hashes, and related page-context fields," *see* Ganan Compl. ¶¶ 258–59—are not the "contents" of a communication. Under Section 631(a), only "information concerning the substance, purpose, or meaning of [a] communication" is protected. *Heiting v. Taro Pharms. USA, Inc.*, 728 F. Supp. 3d 1112, 1123 (C.D. Cal. 2024) (citation omitted). "[C]ontent does not include 'record information,' or the "characteristics of the message that is generated in the course of the communication." *Id.*; *see also Dellasala v. Samba TV, Inc.*, 2026 WL 1138358, at *6 (N.D. Cal. 2026). Only "the intended message conveyed by the communications" is protected contents. *Id.* (citation omitted).

Ganan's vacuous allegations concern contextual signals, not contents. He says so himself, alleging that said data "conveyed the contents or meaning … of the communications" because they "relayed" what Plaintiffs "were doing, viewing, and/or requesting," Ganan Compl. ¶ 258. In other words, Ganan asserts generalized allegations that information *about* his internet activity was intercepted, *not* any specific information about *what* messages were being conveyed. He does not allege any specific actions, pages viewed, or requests that were transmitted to LinkedIn or a third party. *See Hammerling*, 615 F. Supp. 3d at 1093 ("To constitute contents, the information intercepted by Google needs to identify the *specific videos or document* that the user views within Instagram or Facebook.") (emphasis added); *Heiting*, 709 F. Supp. 3d at 1018 (finding "personal identifiers, device identifiers, commercial information, electronic and sensory data, browser information, operating system information" did not include "any substantive communications"). Compare with *Goldstein v. Rumble Inc.*, 2026 WL 1406766, at *4 (C.D. Cal. 2026) (allegations that a pixel obtained "a full-string URL which includes the *descriptive title of the exact video viewed*, in addition to the user's Facebook ID" satisfied the contents requirement (emphasis added)).

Nor are browser "extension-related signal[s] … the contents of a communication," as Ganan himself seems to concede. *See* Ganan Compl. ¶ 269. Though Ganan does not appear to allege that LinkedIn "aids and abets" third parties in accessing browser extension detection results, *id.*, it is ultimately immaterial—none of the data he describes in his complaint could constitute the "contents" of any messages between him and LinkedIn.

Not in transit. Ganan also fails to allege sufficiently that any third party read or attempted to read contents while in transit—i.e., before the communication reached an intended recipient. *See Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1137 (E.D. Cal. 2021); *Swarts v. Home Depot, Inc.*, 689 F. Supp. 3d 732, 746 (N.D. Cal. 2023). Ganan's complaint identifies LinkedIn as the intended recipient of the communications at issue. Ganan Compl. ¶¶ 256, 260, 262. Any data that HUMAN receives necessarily flows *after* those communications have already arrived at LinkedIn, given that its iframe loads only *after* a user's browser initiates a connection to LinkedIn's servers. *Doe v. Eating Recovery Ctr. LLC*, 806 F. Supp. 3d 1109, 1117 (N.D. Cal. 2025) (Chhabria, J.) (in-transit element not met where third party receives data "after the communication has already traveled from the website visitor to the website operator").

Nor does Ganan plausibly allege that HUMAN was even reading or learning the meaning of his data (let alone reading it while it was in transit). *See* Ganan Compl. ¶ 73. Under virtually identical facts, this Court held that a security vendor's public statements about how it may use data do not make it plausible that the vendor is "accessing or reading" specific user information entered into a customer's website. *Love v. Ladder Fin., Inc.*, 2024 WL 2104497, at *2 (N.D. Cal. 2024). "Merely quoting these lines from the [public statement] and then making broad assertions about use is not enough to state a claim under the second clause of § 631(a)." *Id.* And unlike in *Love*, Ganan fails to even allege that HUMAN made these statements. Ganan's allegations to the contrary lack plausibility.

No predicate. The third clause prohibiting the use of information obtained through an unauthorized interception presupposes a valid violation of the first or second clause. Ganan has not pleaded either, so his third-clause claim fails. Conclusory allegations that a third party "used" the data "to enhance its own products and services" and "for corporate marketing," Ganan Compl.

¶ 264, cannot substitute for the predicate interception he has failed to allege.

No aiding and abetting. Even if he had sufficiently alleged a predicate violation, Ganan's aiding and abetting claim would still fail because LinkedIn cannot have aided conduct that it expressly forbids. A vendor that acts as an extension of the website operator, providing a tool that allows the operator to analyze its own data, is not a third-party eavesdropper subject to Section 631. *Jones v. Peloton Interactive, Inc.*, 720 F. Supp. 3d 940, 946 (S.D. Cal. 2024); *see also Martin v. Sephora USA, Inc.*, 2023 WL 2717636, at *13 (E.D. Cal. 2023) (vendor not a third-party eavesdropper where it acted "as an extension of the company"). Moreover, HUMAN's contract with LinkedIn restricts HUMAN, as the vendor, to security and anti-fraud purposes and prohibits use of LinkedIn member data for any other purpose. *See supra* § III.A. To the extent HUMAN may have used data beyond that contracted mandate, such conduct would be prohibited by contract and unknown to LinkedIn. Indeed, LinkedIn has not seen evidence that this is the case, and neither Plaintiff has alleged anything beyond threadbare conclusions. Where a vendor's alleged misconduct is expressly forbidden by the parties' agreement, it defies logic (and defeats the required element of knowing assistance) to impute it to the contracting party. *Heiting*, 709 F. Supp. 3d at 1019 (allegations that defendant paid vendor to intercept messages did not demonstrate defendant "acted with the requisite knowledge or intent to aid and abet" a CIPA violation); *Rodriguez v. Ford Motor Co.*, 722 F. Supp. 3d 1104, 1124 (S.D. Cal. 2024) ("Plaintiff has not alleged that Defendants knew [its vendor's] conduct constituted a breach of some duty."). Speculative allegations that HUMAN deviated from its contracted role should not be entertained.

2. Ganan's Section 638.50 and 638.51 allegations are insufficient.

Ganan also brings a claim under CIPA's "pen register" provision. As explained *supra*, the pen register claims under California Penal Code Sections 638.50(b) and 638.51 are incompatible with his claim under Section 631(a). They therefore may not proceed in parallel.

In any event, the allegedly detected or shared data do not meet the definition of routing information, either. Routing information—dialing, addressing, signaling—identifies the server or destination a device is connecting to; it does not describe the user's device state or a list of features of that device. *Palacios v. Fandom, Inc.*, 2024 WL 5494527, at *3 (Cal. Super. Ct. 2024). The

href values, pathnames, and page-context fields at issue here are context; they cannot be used to identify or contact Ganan, and they say nothing about incoming communications to him. Nor does browser extension data. Courts have sustained demurrers on this exact ground. *Rodriguez v. Sparc Grp., LLC*, 2025 WL 2993671, at *4 (Cal. Super. Ct. 2025) ("This is all information about Plaintiff's device—not information about incoming communications to the device of Plaintiff, who is alleged to be the privacy victim."); *Heiting v. HP Inc.*, 2025 WL 2993673, at *3 (Cal. Super. Ct. 2025) (sustaining demurrer where plaintiff made "no allegation that Defendant's website puts any sort of wiretap or tracker on Plaintiff that allows Defendant to monitor who else contacts Plaintiff"). The same logic governs here. These data are neither contents nor routing information, so neither Section 631 nor Section 638.51 applies. Both claims must be dismissed.

G. Ganan fails to plead a plausible ECPA claim.

For the reasons Ganan's CIPA Section 631(a) claim fails, *see supra* § IV.F., his ECPA claim also fails. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."). The information he describes "do[] not meet the definition of 'contents'" under the cited statute. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014).

V. CONCLUSION

For the foregoing reasons, LinkedIn respectfully requests that this Court dismiss both complaints in their entirety, with prejudice, under Rules 12(b)(1) and 12(b)(6). The core deficiencies in each complaint—the absence of any allegation linking LinkedIn's conduct to a specific extension on a specific plaintiff's browser, each plaintiff's consent to the disclosed conduct, and the structural incompatibility of Plaintiffs' theories with the elements of each cause of action—cannot be cured by amendment. Leave to amend should be denied.

Dated: June 30, 2026

COOLEY LLP

By: */s/ Simona Agnolucci*
Simona Agnolucci
Eduardo Santacana
Natalie Peelish *(Appearance Pro Hac Vice)*

Attorneys for Defendant
LINKEDIN CORPORATION

ATTESTATION

Pursuant to Civil Local Rule 5-1(i)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: June 30, 2026

By: */s/ Eduardo Santacana*
Eduardo Santacana

Attorney for Defendant
LINKEDIN CORPORATION