J.R. HOWELL (State Bar No. 268086)
jr@lojrh.com
LAW OFFICE OF J.R. HOWELL
2219 Main Street
Suite 436
Santa Monica, CA 90405
Tel: (323) 897-8656

ATTORNEY FOR PLAINTIFF
AND THE PROPOSED CLASS

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiff,

vs.

LINKEDIN CORPORATION,

Defendant.

CLASS ACTION COMPLAINT

Jury Demand Endorsed Hereon

I. INTRODUCTION

1. Can a company tell its website users that its systems are fighting fraud and abuse while secretly rifling through the software installed on their computers, extracting data from that private space, copying contents, and profiling users far beyond anything reasonably necessary to stop either fraud or abuse?

2. LinkedIn crossed the line by using anti-abuse justifications as cover for massive covert browser surveillance on a global scale that far exceeded both necessity and any iteration of consent.

3. Plaintiff Jeff Ganan brings this action on behalf of himself and all others similarly situated against Defendant LinkedIn Corporation for covert and overbroad browser surveillance carried out through LinkedIn's website and web-based application.

4. During the relevant period, LinkedIn served client-side code to Plaintiff's browser in California that, on information and belief, actively probed his browser for installed extensions, scanned the page's DOM for extension traces, assembled a browser and device fingerprint, encrypted that fingerprint, transmitted the resulting data to LinkedIn-controlled telemetry endpoints, and reused browser-derived identifiers in subsequent requests during the same session.

5. LinkedIn did not clearly disclose to Plaintiff that it would interrogate his personal browser and home computer in this manner. LinkedIn did not clearly disclose that it would attempt to enumerate installed browser extensions by requesting extension-internal resource paths, crawl the DOM for extension-related traces, and package those results into a session-linked anti-abuse fingerprint. LinkedIn did not disclose the role of third parties involved in this data extraction—nor what those parties or their subprocessors or clients could or would do with that data.

6. LinkedIn has publicly portrayed its challenged systems as part of anti-fraud, anti-abuse, anti-scraping, and security efforts. Plaintiff does not allege that LinkedIn has no legitimate interest in protecting its platform from scraping, bots, fraud, or other abusive behaviors. Plaintiff alleges that LinkedIn used those legitimate interests as cover for a materially broader browser-interrogation regime than was reasonably necessary or proportionate to narrow anti-abuse needs.

7. The challenged practices were not limited to data that users voluntarily entered into LinkedIn. They reached browser-resident and device-resident information that users reasonably expected LinkedIn would not probe, enumerate, classify, and transmit absent clear notice and informed authorization.

8. The challenged practices were also overinclusive. On information and belief, the target list of browser extensions was not confined to tools facially associated with scraping or automation. It extended to many categories of software whose detection served little or no narrow anti-abuse

purpose, including privacy and security tools, job-search tools, and commercially sensitive competitor tools.

9. Because LinkedIn operates the world's largest professional networking platform and knows, or can readily determine, a member's identity, employer, role, network, and use history, the collected signals were not abstract technical artifacts. They were linkable to identified or identifiable California users, including Plaintiff, as well as users around the United States.

10. Plaintiff seeks relief under the federal Electronic Communications Privacy Act, California law for invasion of privacy under article I, section 1 of the California Constitution, intrusion upon seclusion, and violations of California Penal Code §§ 502, 631, and 638.51.

II. PARTIES

11. Plaintiff Jeff Ganan is, and at all relevant times was, a natural person who used LinkedIn's relevant website while physically present at and residing in Los Angeles County, California, during the limitations period. While accessing the relevant website, Plaintiff accessed LinkedIn's product and services using the Chrome browser. At all times relevant, Plaintiff was subjected to the invasions of privacy, surveillance, and data collection, interception, retrieval, transmission, and re-use as alleged in this complaint. Plaintiff consented to none of these actions nor were they disclosed to Plaintiff by LinkedIn or any of its third party partners. Whatever consent LinkedIn may have thought was given absolutely did not include the privacy invasions alleged herein—and no reasonable user of LinkedIn's services would have believed such consent was given.

12. At all relevant times, Plaintiff worked remotely as a sales professional, including work in Los Angeles County where he accessed LinkedIn's website through a personal computer and Chrome web browser.

13. Defendant LinkedIn Corporation is, on information and belief, a Delaware corporation that maintains and operates substantial offices, including its headquarters campus, in California, and does substantial business throughout the State of California, including Los Angeles County. For users such as Plaintiff located outside LinkedIn's designated countries, LinkedIn's own user agreement states that the relevant contracting entity is LinkedIn Corporation.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and the provisions of the Class Action Fairness Act in 28 U.S.C. § 1332. Additionally, a contract between Defendant and Plaintiff and Defendant and the putative class members contains a choice of law and forum selection clause designating the state superior court and the federal court in this district as the exclusive adjudicative fora for disputes of this type.

15. This Court has personal jurisdiction over Defendant because Defendant is headquartered or maintains substantial principal operations in California, purposefully avails itself of the privilege of conducting business in California, directs its services and challenged conduct to California residents, and caused the injuries alleged herein in California.

IV. FACTUAL ALLEGATIONS

A. LINKEDIN'S SERVICES AND RELATIONSHIP WITH USERS

16. LinkedIn operates linkedin.com and related web-based services used by professionals to maintain profiles, build networks, search for work, message other users, identify business opportunities, and use recruiting, sales, advertising, learning, and related features.

17. LinkedIn encourages users to maintain profiles using their real names and real professional histories. Through those profiles and related account data, LinkedIn knows or can readily determine a member's name, location, employer, job title, work history, connections, and use of LinkedIn's services.

18. LinkedIn's public-facing privacy and contract materials state in substance that when users visit or leave LinkedIn's services, LinkedIn receives URLs, timing, and network and device information, including web browser and add-ons, device identifiers, and device features, and that LinkedIn uses data for security, fraud prevention, investigations, automated systems, and inferences.

19. LinkedIn's public-facing help and contract materials also prohibit third-party software, bots, browser plug-ins, and browser add-ons that scrape, automate, or modify the appearance of LinkedIn's services, and state that LinkedIn continues to improve technical measures and defenses against such tools.

20. Plaintiff does not challenge LinkedIn's right to police unlawful scraping, fraud, or abuse. Plaintiff challenges the covert, overbroad, and underdisclosed means by which LinkedIn implemented those efforts.

21. LinkedIn did not disclose, and neither Plaintiff nor the class members consented to, the role of third parties as alleged in this Complaint and/or to the uses of their data to which those third parties could or did perform.

B. PLAINTIFF'S CALIFORNIA USE OF LINKEDIN

22. Plaintiff created and maintained a LinkedIn member account.

23. At all relevant times, Plaintiff used LinkedIn in California, from Los Angeles County, through a personal computer and a Chromium browser-based LinkedIn experience.

24. Plaintiff used LinkedIn in the ordinary course of his work and professional life, including to maintain professional relationships, review profiles, communicate with other users, and identify business or career opportunities.

25. When Plaintiff used LinkedIn in the ordinary course, LinkedIn knew or could readily determine his identity, employer, and professional role through his member account, profile, cookies, and session state.

26. Plaintiff continues to use, or needs to use, LinkedIn as part of his profession and thus faces a continuing risk of being subjected to the challenged practices absent judicial relief.

C. LINKEDIN'S ASSERTED ANTI-ABUSE RATIONALE

27. LinkedIn has elsewhere described its anti-abuse systems as multi-layered technical systems developed to detect and mitigate scraping, automation, and related platform abuse.

28. On information and belief, LinkedIn has represented under oath through a senior manager in software engineering and machine learning that tools such as scraper-oriented browser extensions can generate disproportionately high request volume, burden LinkedIn infrastructure, impair service availability, and contribute to outages or degradation.

29. On information and belief, LinkedIn has also represented that it invested in extension-detection mechanisms because, in its view, those mechanisms helped it trace causes of service disruptions and outages associated with scraping and automation.

30. At the same time, LinkedIn has also represented that its broader abuse models do not treat the use of any particular extension alone as dispositive, and that users were not acted against merely because they had a particular extension installed.

31. Those representations show two things at once: first, LinkedIn had a real anti-abuse objective; and second, LinkedIn's challenged extension-detection processes swept in more information than was necessary to determine whether any specific extension alone justified user enforcement action, while exposing user data to nonpermissioned third parties.

32. Plaintiff does not allege that LinkedIn cannot use technical means to protect its site. Plaintiff alleges that LinkedIn exceeded the bounds of reasonable necessity, proportionality, and user authorization when it covertly probed personal browsers and devices in a mass surveillance program as alleged below.

D. LINKEDIN'S CHALLENGED CLIENT-SIDE CODE

33. Plaintiff's investigation, including review of LinkedIn-served JavaScript bundles and related technical materials, reflects that LinkedIn delivered a production JavaScript bundle that contained a coordinated browser-interrogation system.

34. In representative inspected builds, the relevant bundle was identified as a Webpack package commonly referenced as chunk.905, and the extension-detection logic appeared in a module identified as module 75023. The hashed filename of the bundle changed between deployments, but the stable module, strings, internal names, and endpoint references remained searchable.

35. In representative inspected builds, LinkedIn's extension-detection architecture included at least two material mechanisms: an active extension-probing system and a passive DOM-scanning system. It also included a broader device-fingerprinting system discussed below.

36. On information and belief, the active extension-probing system used a hardcoded list containing thousands of extension identifiers paired with specific internal file paths for each targeted extension. In inspected builds from late 2025 and early 2026, that hardcoded list contained more than five thousand entries and later more than six thousand entries.

37. Each targeted entry paired a 32-character browser-extension identifier with a specific internal resource path such as a popup file, icon, manifest, script, or similar file. That pairing was not incidental. It reflected prior identification by LinkedIn of a particular extension-internal resource to be probed.

38. LinkedIn's code then attempted requests to URLs of the form chrome-extension://{id}/{file} in order to determine whether the targeted extension was installed and exposed a web-accessible resource.

39. In one execution mode, LinkedIn's code launched these requests in parallel and used the success of each request to infer that the corresponding extension was installed.

40. In another execution mode, LinkedIn's code launched the extension-resource requests sequentially, one by one, with a configurable delay between requests.

41. On information and belief, LinkedIn could also defer execution of the probing logic until browser idle time through requestIdleCallback, making the process less visible to users and less likely to create a noticeable performance spike.

42. Failed extension-resource requests were silently caught and discarded. The code did not require any visible user interaction before performing the scan.

43. Separate from the active resource probing, LinkedIn also operated a passive DOM-based detection mechanism referred to in inspected materials as Spectroscopy.

44. That DOM-based mechanism recursively traversed the document tree and inspected both text nodes and element attributes for strings beginning with chrome-extension://.

45. When the code found such a string, it extracted the extension identifier embedded in the URL and added that identifier to a collection of detected extensions.

46. This passive DOM scan could detect extension traces left by browser extensions that altered LinkedIn's page or inserted extension-specific elements, even if such extensions were not limited to a smaller prebuilt list.

47. On information and belief, LinkedIn controlled deployment of the challenged systems through internal experimentation and feature-flag controls, but served the challenged architecture broadly to Chromium-based browsers, including the browser used by Plaintiff.

48. The challenged probing and scanning were not required to render LinkedIn profiles, feeds, messages, search results, job pages, or other ordinary user-requested content.

49. The fact that some extension developers expose particular resources as web-accessible does not mean that LinkedIn users authorized LinkedIn to query their browsers for the existence of thousands of extensions, to compile the results, or to tie those results to account-linked anti-abuse profiles.

50. Whether or not each targeted extension was actually installed on Plaintiff's browser, LinkedIn's code still caused Plaintiff's browser and computer to test for, reveal, and process extension-related presence or absence information.

E. LINKEDIN'S BROADER APFC OR DNA FINGERPRINTING SYSTEM

51. On information and belief, the extension-detection system was not a standalone feature. It was one component of a broader device-fingerprinting and anti-fraud system referred to in inspected materials as APFC, or Anti-fraud Platform Features Collection, and also as DNA, or Device Network Analysis.

52. In representative inspected builds, the APFC or DNA system collected numerous browser and device characteristics, including WebRTC or local IP information, enumerated input and output devices, browser and operating system identifiers, CPU and memory characteristics, language and time zone data, the user agent, webdriver status, private-browsing indicators, screen properties, storage availability, canvas output, WebGL characteristics, network information, battery information, audio-context features, automation indicators, plugins and MIME types, and font data.

53. LinkedIn's code packaged the extension-detection results together with or alongside broader fingerprinting data and caused that data to be transmitted to LinkedIn-controlled telemetry systems.

54. In representative inspected builds, the resulting payload was serialized and encrypted using a public key identifier referred to as apfcDfPK, stored in the browser context on globalThis.apfcDf, and transmitted to telemetry destinations including LinkedIn's li/track endpoint and APFC-related collection endpoints.

55. On information and belief, LinkedIn also reused the resulting fingerprint by injecting it into subsequent API requests during the same user session, so that the collection did not occur merely once and disappear. It became part of the session-level telemetry tied to the user's actions on LinkedIn.

56. In representative inspected builds, LinkedIn's surrounding anti-abuse systems also included a hidden HUMAN Security iframe loaded from li.protechts.net, a separate fingerprinting script from merchantpool1.linkedin.com, and reCAPTCHA bot-detection code.

57. LinkedIn's use of multiple additional anti-abuse technologies is significant because it shows that LinkedIn already maintained several layers of technical protection before, during, and alongside the challenged browser probing and fingerprinting.

F. LINKEDIN'S COVERT SESSION-PERSISTENT FINGERPRINT SIGNALING SYSTEM: INTENTIONAL CIRCUMVENTION OF CHROME'S SECURITY FEATURES

58. On information and belief, LinkedIn's APFC process did not merely collect a static set of browser traits and send them once. In representative inspected builds, LinkedIn serialized the APFC fingerprint, encrypted it with the public key identifier apfcDfPK, stored the resulting encrypted value on globalThis.apfcDf, transmitted it to /platform-telemetry/li/apfcDf and /apfc/collect, and then reused that same value during the balance of the session.

59. In representative inspected builds, LinkedIn's code used SyncCollectionHandler and related synchronization logic to inject, append, or otherwise propagate the APFC value, or an equivalent session-linked signaling value derived from it, into subsequent API requests during the same browsing session. On information and belief, this allowed the same device- and session-linked identifier to accompany later searches, profile views, message actions, feed loads, and other requests after the initial page load.

60. On information and belief, LinkedIn's own internal feature flags further confirm that this was a network-level signaling system, not a one-time background measurement. Those flags included, among others, sync.apfc.headers and pemberly.tracking.apfc.network.interceptor, reflecting a design in which APFC-derived identifiers were synchronized into headers and related network-interceptor flows during the same session.

61. The APFC process collected and encoded non-content dialing, routing, addressing, and signaling information used to identify and correlate the source of subsequent communications. In representative inspected builds, that information included WebRTC-derived local-network IP signals, user-agent and browser-identification strings, protocol, hostname, port, origin, timezone and

language signals, automation-detection signals, storage-capability signals, device-memory and hardware-concurrency signals, and other source-identifying session metadata.

62. On information and belief, the APFC process thereby transformed ordinary LinkedIn sessions into a persistent signaling stream in which the same source-identifying value or values were attached to repeated requests and responses over time. This process enabled LinkedIn, and any linked recipient of the same signaling values, to recognize, correlate, and monitor the same browser and device across repeated electronic communications during the session.

63. LinkedIn did not deploy this system in isolation. In representative inspected builds, the same process also included a concealed cross-origin iframe, a separate fingerprinting script, and reCAPTCHA or similar anti-bot integrations. On information and belief, those auxiliary components were positioned to receive, process, or act upon the same session-linked identifiers and signaling values as part of a broader coordinated surveillance system.

64. The challenged process was also not implemented in a transparent manner. On information and belief, LinkedIn deferred portions of the scan to browser idle time, staggered requests over time rather than firing them in one visible burst, silently handled failures, concealed outside-recipient infrastructure in an off-screen zero-by-zero iframe, and encrypted the resulting fingerprint before transmission. These implementation choices reduced user visibility and made the persistence, scope, and network propagation of the process harder to detect.

65. LinkedIn already maintained multiple anti-fraud and anti-abuse tools, including separate anti-bot and fraud integrations, yet still chose to operate the APFC process as a high-entropy, session-persistent signaling system tied to logged-in accounts. The challenged process was therefore broader than reasonably necessary to operate, maintain, or test a communications service or to address any narrow anti-abuse need.

66. On information and belief, the overbreadth of the APFC process is further shown by its coexistence with LinkedIn's extension-detection systems, which probed for thousands of extensions and extracted browserExtensionIds arrays, including extensions unrelated to narrow scraping prevention. Plaintiff does not rely in the pen-register count on those extension outputs as "contents," but does allege that their inclusion in the same system shows that the challenged process was designed for identity-linked surveillance and profiling rather than a narrow, transaction-specific technical safeguard.

G. LINKEDIN'S CONCEALED THIRD-PARTY AUXILIARY CHANNEL

67. On information and belief, LinkedIn did not confine the challenged surveillance system to code operating only within linkedin.com. In representative inspected builds, LinkedIn embedded

concealed auxiliary integrations sourced from domains distinct from linkedin.com and caused those integrations to operate during users' live LinkedIn sessions.

68. One such integration was loaded into the active LinkedIn page as a hidden cross-origin iframe. The iframe was concealed from ordinary users by being rendered invisible at zero by zero pixels, positioned in a negative space off-screen, and marked hidden from assistive technologies. It did not appear as part of any user-requested LinkedIn feature and was not disclosed in LinkedIn's consumer-facing privacy or consent materials.

69. LinkedIn's code passed session-linked values into that concealed outside-recipient environment, including a timestamp, a page-tree or request identifier, a hashed session cookie, an application identifier, and a use-context string associated with scraping or anti-abuse review. The concealed outside-recipient environment also read and set its own cookies and identifiers through cross-origin exchanges. Those cookies and identifiers were distinct from LinkedIn's ordinary first-party cookies and gave the outside recipient its own persistent foothold within the user's live browser session. But, those distinct third party cookies were coded to appear as though they were LinkedIn's to avoid detection.

70. The concealed auxiliary integration did not merely host inert content. It operated during the same live sessions in which LinkedIn's APFC and DNA systems collected browser and device data, assembled telemetry payloads, and propagated session-linked identifiers into subsequent requests. On information and belief, LinkedIn used URL parameters, cross-origin messaging, and related browser mechanisms to pass or make available session-linked data from the parent LinkedIn page into that concealed outside-recipient environment while the session was ongoing.

71. Because the concealed outside-recipient environment was cross-origin and separate from linkedin.com, it could not independently read the LinkedIn parent page absent LinkedIn's assistance. LinkedIn therefore had to create and maintain a bridge by which data extracted from the live LinkedIn session could be furnished to, received by, or made available for interception or acquisition by the outside recipient. On information and belief, through that bridge LinkedIn routed, duplicated, transmitted, or made available data extracted from the live session, including content-bearing page-context fields such as href, pathname, hash, and related location or page-state values that relayed what Plaintiff and class members were doing, viewing, and/or requesting during their LinkedIn sessions.

72. LinkedIn's APFC and DNA systems were designed to collect, package, serialize, encrypt, store, transmit, and propagate those page-context values together with other session-linked data. In representative inspected builds, LinkedIn stored the resulting encrypted fingerprint in the browser

context, transmitted it to LinkedIn telemetry endpoints, and reused it by propagating it into later API requests during the same session. On information and belief, the same covert system also enabled that content-bearing information, or the meaning of that information, to be transmitted to, disclosed to, or made available to LinkedIn's undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, and similar outside recipients.

73. One such outside recipient publicly states that its product uses client-side JavaScript and/or pixels placed on webpages or across domains to collect information about web and mobile visits; that it stores customer data including IP address, connection metadata such as request headers, browser identification strings, TLS information, mouse interaction events, and in some products user identifiers; and that "Processor Data may be integrated into the Product and shared with other clients to enhance the Product's anti-fraud functionality," may be used for analytics "to detect behavior patterns in order to enhance the Product," and may be aggregated for "general corporate marketing and industry benchmarking purposes." On information and belief, LinkedIn knew, intended, or recklessly disregarded that its undisclosed third-party data partners would use or derive value from session-linked data obtained through these integrations 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.

74. In this way, LinkedIn's concealed outside-recipient channel was not limited to ordinary first-party website functionality. It created a covert second stream through which user-session data could be duplicated, transmitted, received, analyzed, stored, reused, and monetized by outside recipients without clear disclosure or informed consent.

75. LinkedIn's extension-probing and DOM-scanning systems further confirm the deliberate and non-innocent character of that architecture. LinkedIn's code actively probed thousands of extensions and recursively scanned the DOM for extension traces, then transmitted the resulting detections through internal tracking events. Plaintiff does not allege that every extension-related signal, standing alone, independently constitutes the contents of a communication. Plaintiff alleges that these systems were part of the same covert surveillance apparatus and demonstrate that LinkedIn's outside-recipient architecture was designed to harvest semantically rich, identity-linkable user information rather than merely to receive innocuous routing data.

76. LinkedIn did not clearly disclose that users' live LinkedIn sessions would include a concealed cross-origin outside-recipient environment; that such an environment would maintain its own cookies, identifiers, and cross-origin messaging channel; that LinkedIn would pass or make

available session-linked data into that environment; or that outside recipients could use or derive value from such data to enhance their own anti-fraud products, analytics, benchmarking, or other commercial offerings. General references to URLs, browser data, device features, security, anti-abuse, fraud prevention, add-ons, cookies, or automated systems did not disclose the concealed outside-recipient channel alleged herein and did not obtain informed consent to it.

H. THE CHALLENGED CONDUCT EXCEEDED WHAT WAS REASONABLY NECESSARY FOR NARROW ANTI-ABUSE PURPOSES

77. Plaintiff does not allege that anti-scraping or anti-bot measures are inherently unlawful. Plaintiff alleges that LinkedIn's actual implementation was broader than reasonably necessary and exceeded the scope of what a user would reasonably authorize by using LinkedIn.

78. On information and belief, the extension target list was not limited to tools facially associated with scraping or automation. It included many categories of software whose relevance to a narrow anti-abuse purpose was weak, remote, or nonexistent.

79. Those categories included, on information and belief, privacy and security tools, job-search tools, sales and prospecting tools, tools associated with companies that compete with LinkedIn's own commercial offerings, and other extensions that reveal intimate or commercially sensitive details when tied to a real-name LinkedIn identity.

80. LinkedIn's own representation that its broader abuse models do not rely on the use of any particular extension alone underscores that the challenged extension scans were not limited to a narrowly tailored pass-fail check for a single identified threat.

81. The challenged systems were also overinclusive because they reached ordinary users engaged in routine LinkedIn activity from personal and household computers, including users who were not scraping LinkedIn or automating activity. The data retrieval could even scan information related to religion, political views, and disability status.

82. The existence of less intrusive technical tools already in use, including bot-detection services and other fingerprinting measures, further demonstrates that LinkedIn's extension probing and session-linked reuse of the results went beyond what was reasonably necessary or proportionate to narrow anti-abuse needs.

I. LINKEDIN'S DISCLOSURES DID NOT CLEARLY DISCLOSE THE CHALLENGED CONDUCT OR OBTAIN INFORMED CONSENT

83. LinkedIn's public-facing privacy and contract materials did not clearly inform Plaintiff that LinkedIn would interrogate his browser for installed extensions and extension traces in the manner alleged herein.

84. LinkedIn's public-facing privacy materials stated in substance that when users visit or leave its services, LinkedIn receives URL, timing, and network and device information, including web browser and add-ons, device identifiers, and device features.

85. LinkedIn's public-facing privacy materials also stated in substance that LinkedIn uses data for security, fraud prevention, investigations, automated systems, and inferences.

86. LinkedIn's public-facing cookie materials later referred to anti-abuse or extension-related cookies, including a cookie called spectroscopyId used to catch malicious activity through browser extensions, and cookies such as li_bapfcc, li_apfcdc, and li_odapfcc used to control or trigger abuse-prevention features on a member device.

87. Those generalized references did not clearly tell a reasonable user that LinkedIn would attempt to enumerate installed extensions by making targeted requests to chrome-extension:// resource paths, recursively scan the page's DOM for extension traces, collect a browserExtensionIds array, encrypt the resulting fingerprint, store it within the browser context, and attach it to later API requests.

88. Nor did LinkedIn clearly tell users that its anti-abuse probing extended across thousands of targeted extensions, including categories facially unrelated to narrow scraping prevention.

89. LinkedIn's user agreement and help materials prohibited third-party scraping, bots, browser plug-ins, and browser add-ons that scrape or modify LinkedIn's services. Those prohibitions may explain why LinkedIn would pursue technical defenses, but they did not inform Plaintiff that LinkedIn itself would engage in covert browser-resource probing, DOM scanning, and session-linked fingerprinting of users' devices.

90. Any purported consent arising from ordinary use of LinkedIn, acceptance of broad terms of service, or awareness that LinkedIn receives routine browser information did not amount to informed authorization for the covert, overinclusive, and session-linked browser interrogation alleged herein.

J. THE COLLECTED OR INFERRED INFORMATION WAS PERSONAL, PROTECTED, AND LINKABLE TO IDENTIFIED USERS

91. The information LinkedIn collected or derived was personal information and protected browser-resident or device-resident information.

92. Installed-extension presence or absence, extension-related DOM traces, and extension identifiers are facts about software installed in, or interacting with, the user's browser environment and personal computer.

93. When combined with LinkedIn account data, cookies, session identifiers, IP addresses, user agents, device fingerprints, and the user's own profile, those signals were reasonably capable of identifying, singling out, or being linked to a particular user, including Plaintiff.

94. For at least some targeted extension categories, the resulting data also revealed, or supported ready inference about, a user's job-seeking activity, privacy or security practices, use of competitor tools, or other sensitive or intimate interests.

95. LinkedIn itself possessed the contextual data necessary to make such inferences because LinkedIn knew or could readily determine the member's name, employer, role, network, and site activity.

96. Even where LinkedIn publicly says it does not show an employer the member's job searches or personal messages, LinkedIn's own internal collection and inference systems could nevertheless reveal or support inferences about a member's job-seeking or other sensitive interests to LinkedIn itself.

97. Plaintiff had a reasonable expectation that LinkedIn would not covertly interrogate his personal browser and home computer for this class of information absent clear disclosure and informed consent.

K. PLAINTIFF'S AND CLASS MEMBERS' INJURIES

98. LinkedIn's conduct invaded Plaintiff's privacy and deprived him of control over browser-resident and device-resident information that he did not intend to disclose to LinkedIn in this manner.

99. As a result of learning about these invasions of privacy, Plaintiff spent approximately one hundred dollars on services to protect his data and personal devices.

100. LinkedIn's conduct also caused Plaintiff's computer and browser to expend processing time, network resources, storage interactions, and other computer services to perform the challenged probes, scans, and fingerprinting tasks.

101. Plaintiff has spent time and effort investigating, understanding, and responding to LinkedIn's conduct, including reviewing his LinkedIn use, browser behavior, LinkedIn disclosures, and the nature of the challenged collection.

102. Plaintiff and class members private data has been published by LinkedIn to third parties.

103. Plaintiff faces an ongoing risk of repeated future exposure because LinkedIn has operated the challenged architecture as part of ongoing anti-abuse systems and Plaintiff continues to need LinkedIn for professional reasons.

104. Plaintiff's injuries are concrete, particularized, and not merely speculative. They arise from the covert interrogation of his personal browser and computer, the extraction and use of browser-resident information, the creation and reuse of an account- or session-linked fingerprint, the associated loss of privacy and control, and the unauthorized use of his computer resources.

105. Class members were injured in materially similar ways through common code, common telemetry systems, common or substantially similar disclosures, and a common anti-abuse rationale asserted by LinkedIn.

L. CHOICE OF LAW

106. California's substantive laws apply to every member of the Classes, regardless of where in the United States the Class member resides, or to which Class the Class member belongs.

107. At all relevant times, LinkedIn required users nationwide, including Plaintiff and members of the proposed classes to agree to LinkedIn's user agreement by creating an account or by accessing or using LinkedIn's services. This agreement stated that it applies to both "Members" and "Visitors" and to LinkedIn.com, LinkedIn-branded apps, and other LinkedIn-related sites, apps, communications, and services, including offsite collection of data for those Services.

108. The agreement further provides that, for users residing outside the "Designated Countries," the contracting party is LinkedIn Corporation. For those users, LinkedIn selected the laws of the State of California, excluding its conflict-of-laws rules, to exclusively govern any dispute relating to the Contract and/or the Services, and required that all claims and disputes be litigated only in the federal or state courts in Santa Clara County, California: "You and LinkedIn agree that the laws of the State of California, U.S.A., excluding its conflict of laws rules, shall exclusively govern any dispute relating to this Contract and/or the Services." This clause applies to the dispute by Plaintiff and the class members against LinkedIn.

109. Plaintiff and members of the proposed Nationwide Class used LinkedIn's Services outside the Designated Countries, including throughout the United States, and did so subject to the same User Agreement and the same California governing-law and forum provisions. The challenged conduct alleged herein arose from and related to LinkedIn's provision, design, deployment, operation, and monetization of those Services, including the covert code, telemetry, collection, transmission, reuse, and related partner-enabled processing carried out through LinkedIn's website and associated Services.

110. By drafting and enforcing a User Agreement that applies to Members and Visitors, selecting LinkedIn Corporation as the contracting entity for users outside the Designated Countries, and mandating California law and Santa Clara County courts for disputes relating to the Contract and/or

the Services, LinkedIn elected to have a single California-centered legal regime govern disputes arising from its provision and operation of those Services for users nationwide outside the Designated Countries, including Plaintiff and members of the proposed Nationwide Class.

111. By choosing substantive California law for the resolution of disputes pertaining to "Services" covered by its User Agreement, LinkedIn concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. The User Agreement defines services to include LinkedIn.com generally and data collection activities specifically: "This Contract applies to LinkedIn.com, LinkedIn-branded apps, and other LinkedIn-related sites, apps, communications, and other services that state that they are offered under this Contract ('Services'), including the offsite collection of data for those Services, such as via our ads and the "Apply with LinkedIn" and "Share with LinkedIn" plugins."

112. As such, LinkedIn specifically contracted to the application of California law with respect to the claims by class members nationwide, including the below claims arising under California's Penal Code.

113. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiff and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Classes and California has the greatest interest in applying its laws here.

114. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

M. LACK OF DISCLOSURE AND ABSENCE OF CONSENT

115. Neither Plaintiff nor class members knowingly, expressly, or impliedly consented to the challenged privacy invasions, covert browser surveillance, extraction of browser-resident or device-resident information, creation of session-linked fingerprints, or the transmission, disclosure, or making available of such information to undisclosed third parties.

116. At no point before or during the challenged sessions did LinkedIn provide Plaintiff or class members with a clear, specific, and timely disclosure that LinkedIn would cause hidden code to probe browsers for installed extensions and extension traces, scan the DOM for extension-related artifacts, extract href, pathname, hash, and related page-context fields, assemble an APFC or DNA fingerprint, encrypt and store that fingerprint in the browser context, and inject or propagate it into subsequent requests during the same session.

117. Nor did LinkedIn clearly disclose that the challenged conduct would extend beyond LinkedIn's own internal receipt of ordinary first-party traffic and would include transmitting, disclosing, or making available session-linked data and related information to undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, or other outside recipients operating through concealed auxiliary integrations, separate identifiers, cookies, or cross-origin communication channels.

118. On information and belief, LinkedIn also did not disclose that such outside recipients could use or derive value from Plaintiff's and class members' data for purposes beyond a one-time service to LinkedIn, including enhancing or training their own products and services, improving analytics and behavioral or predictive models, supporting cross-client anti-fraud or anti-abuse functionality, benchmarking, marketing, and other commercial exploitation or monetization.

119. Plaintiff and class members were not told that the challenged collection extended to information they did not voluntarily furnish to LinkedIn, including browser-resident and device-resident information, extension-related presence or traces, and content-bearing page-context fields that relayed what they were doing, viewing, and/or requesting during live LinkedIn sessions.

120. Plaintiff and class members likewise were not told that the challenged systems would operate silently in the background, without any visible prompt, separate opt-in, session-specific authorization, or meaningful opportunity to refuse the conduct while still using LinkedIn's ordinary website functions.

121. Whatever generalized disclosure LinkedIn may contend it provided, and whatever generalized consent LinkedIn may contend it obtained through privacy policies, cookie materials, terms of service, help pages, or ordinary use of the site, a reasonable user would not have understood those generalized statements to authorize the challenged conduct alleged herein.

122. No reasonable user would read generalized references to URLs, browser data, add-ons, device features, cookies, automated systems, security, anti-abuse, fraud prevention, or similar matters and understand that LinkedIn would covertly interrogate the user's browser, enumerate or infer installed extensions, scan the DOM for extension traces, extract href, pathname, hash, and

related page-context values, create an encrypted session-linked fingerprint, propagate that fingerprint across subsequent requests, and transmit, disclose, or make such information available to undisclosed third parties for their own reuse, analytics, model improvement, benchmarking, marketing, or other commercial monetization.

123. The challenged surveillance, extraction, reuse, and outside-recipient exploitation therefore exceeded the scope of any disclosure or authorization LinkedIn may claim existed. Any purported consent was, at most, consent to ordinary first-party website functionality and conventional security measures as a reasonable user would understand them, not to the covert, overbroad, identity-linked, and third-party-enabled practices alleged in this Complaint.

124. Had Plaintiff and class members been clearly told that LinkedIn would engage in the challenged surveillance and data extraction, or that outside recipients could receive, reuse, or commercially benefit from the resulting data, they would not have understood themselves to be consenting to such conduct merely by visiting, logging into, or using LinkedIn's services.

125. LinkedIn's omissions were material. In light of the sensitivity, breadth, persistence, and third-party reuse alleged herein, a reasonable user deciding whether and how to use LinkedIn's services would have considered these undisclosed practices important.

N. TOLLING OF THE STATUTE OF LIMITATIONS

126. Any applicable statutes of limitations have been tolled under, among other doctrines, the doctrines of fraudulent concealment and delayed discovery.

127. Throughout the applicable period, LinkedIn knowingly concealed the challenged conduct from Plaintiff and class members. LinkedIn did not present the challenged surveillance and data extraction practices to users through any clear, specific, and timely disclosure. Instead, LinkedIn served hidden client-side code that operated in the background of users' live LinkedIn sessions and silently interrogated users' browsers and devices.

128. The challenged conduct was self-concealing. In representative inspected builds, LinkedIn's code did not require any visible user interaction before performing the scan, could defer execution until browser idle time through requestIdleCallback to make the process less noticeable, and silently caught and discarded failed requests. The challenged probing and scanning did not appear as an ordinary user-facing LinkedIn feature and were not required to render the ordinary content that users requested.

129. LinkedIn further concealed the challenged conduct by serializing and encrypting the resulting fingerprint payload, storing it in the browser context, transmitting it to telemetry endpoints, and reusing it by injecting it into subsequent API requests during the same session. Because the

challenged payload was encrypted and transmitted through technical telemetry channels rather than through visible user-facing interfaces, ordinary users had no reasonable way to perceive the nature, scope, or persistence of the collection.

130. LinkedIn's public-facing privacy materials, cookie materials, user agreement, and help materials did not clearly disclose that LinkedIn would attempt to enumerate installed extensions by making targeted requests to chrome-extension:// resource paths, recursively scan the DOM for extension traces, collect a browserExtensionIds array, encrypt the resulting fingerprint, store it within the browser context, attach it to later API requests, and otherwise engage in covert, session-linked browser interrogation as alleged herein.

131. Instead of clearly disclosing the challenged conduct, LinkedIn described its practices only in generalized terms, such as receiving URL, timing, browser, add-on, and device information and using data for security, fraud prevention, investigations, automated systems, and inferences. Those generalized statements omitted the specific mechanics, breadth, persistence, and sensitivity of the conduct alleged herein and were insufficient to place a reasonable user on notice of the challenged practices.

132. LinkedIn also publicly framed its systems in terms of anti-abuse, anti-fraud, anti-scraping, and security, thereby reinforcing the impression that any technical activity occurring in the background was limited to ordinary, proportionate, and disclosed site-protection measures. A reasonable user would not have understood those generalized descriptions to mean that LinkedIn was covertly probing the user's browser for thousands of extensions, scanning the DOM for extension traces, generating a fingerprint from browser- and device-resident information, and propagating that fingerprint across subsequent requests during the same session.

133. Plaintiff and class members did not know, and could not reasonably have known, of the facts giving rise to their claims until shortly before the filing of this action. The challenged conduct was not apparent from ordinary use of LinkedIn, did not generate any visible prompt or notification, and could not be discovered without specialized technical investigation, including review of LinkedIn-served JavaScript bundles, telemetry behavior, and related technical artifacts.

134. Plaintiff and class members acted with reasonable diligence. They used LinkedIn in the ordinary course, reviewed or were exposed to LinkedIn's public-facing disclosures, and had no reason to suspect that LinkedIn was engaging in the covert browser surveillance, encrypted telemetry, and session-linked fingerprinting alleged herein. Nothing in LinkedIn's user-facing materials or ordinary site behavior would have alerted a reasonable user to the existence of the challenged conduct.

135. Plaintiff first discovered, or could reasonably have discovered, the challenged conduct only after specialized investigation and technical review brought LinkedIn's concealed code and telemetry practices to light. Plaintiff thereafter acted diligently in investigating the facts, evaluating his claims, and bringing this action.

136. Because LinkedIn concealed the challenged conduct, omitted material facts necessary to make its generalized public statements not misleading, and structured the challenged practices in a manner that ordinary users could not reasonably detect, any otherwise applicable limitations periods were tolled and this action is timely.

V. CLASS ACTION ALLEGATIONS

137. Plaintiff brings this action pursuant to Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of himself and the following classes.

138. The Nationwide Class:

> All Chrome browser users with a LinkedIn account who accessed LinkedIn.com from the United States while using such a Chrome browser during the Class Period.

139. The California Class:

> All Chrome browser users with a LinkedIn account who accessed LinkedIn.com while using such a Chrome browser from California during the Class Period.

140. Excluded from the classes are Defendant, Defendant's officers and directors, Defendant's legal representatives, successors and assigns, and any judicial officer to whom this case is assigned, together with that officer's immediate family, and Plaintiff's counsel.

141. Plaintiff is a member of the proposed classes.

142. Each class member has suffered injury or damage as alleged herein and, on a class-wide basis, seeks damages and injunctive and declaratory relief as allowed by law.

143. There are questions of law and fact common among Plaintiff and the proposed classes.

144. Common questions include whether LinkedIn served materially similar client-side code to class members' browsers, including code that probed chrome-extension:// resources, scanned the DOM for extension traces, or built APFC or DNA fingerprints.

145. Common questions also include whether LinkedIn collected browserExtensionIds or similar extension-detection results, whether LinkedIn transmitted those results to li/track or related telemetry destinations, and whether LinkedIn reused or attached encrypted fingerprints to subsequent requests during a user session.

146. Common questions further include whether the challenged conduct was reasonably necessary or proportionate to any legitimate anti-abuse, anti-fraud, or anti-scraping purpose and whether LinkedIn already employed less intrusive technical alternatives.

147. Common questions also include whether LinkedIn's disclosures adequately informed class members of the specific conduct alleged herein, whether class members gave informed authorization for that conduct, and whether generalized references to browser add-ons, device features, cookies, or anti-abuse processes were sufficient. Common questions include what a reasonable user would have believed with respect to the privacy and security of their data on LinkedIn's syststems.

148. Common questions also include whether the conduct alleged herein invaded a legally protected privacy interest, whether it would be highly offensive to a reasonable person, and whether it constituted a serious invasion of privacy under applicable law.

149. Common questions also include whether LinkedIn knowingly and without permission accessed, caused to be accessed, used, or caused to be used class members' computers, computer services, data, or related resources within the meaning of Penal Code section 502.

150. The class is so numerous that joinder is impracticable. LinkedIn is used by large numbers of California users and users across the United States, and the challenged practices were deployed through common LinkedIn code and telemetry systems.

151. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Requiring the numerous affected California users to pursue their claims individually would create duplicative proceedings, duplicated evidence and expert work, inconsistent results, and burdens disproportionate to many individual claims.

152. The classes are ascertainable from Defendant's records and data, including account records, login and session records, cookies, browser and user-agent data, bundle-delivery records, feature-flag or experimentation records, telemetry logs, and records reflecting AedEvent, SpectroscopyEvent, APFC, or related collection. LinkedIn also possesses class member names and email addresses.

153. Plaintiff's claims are typical of the classes. Plaintiff, like other class members, used LinkedIn in through a personal or household computer and Chrome browser, was subjected to the challenged conduct, and seeks relief under the same legal theories based on materially similar facts.

154. Plaintiff will fairly and adequately protect the interests of the classes. Plaintiff has no interests antagonistic to the classes. Plaintiff has retained counsel experienced in privacy, technology, and class-action litigation. Plaintiff's counsel has previously served as class counsel in nationwide class action litigation, recognized as a privacy expert by the United States District Court

for the Central District of California, and has previously litigated from pleading to verdict a California privacy law matter.

155. The questions of law and fact common to the class predominate over any individualized questions. Any variation in the exact extensions installed, the precise browser configuration, or particular feature-flag assignment does not defeat predominance because the central issues concern common code, common design, common disclosures, common anti-abuse rationale, and common categories of injury.

156. Class treatment is especially appropriate because the challenged practices were implemented through centralized LinkedIn engineering decisions and common telemetry systems, and because Defendant's liability can be established or disproved largely through common documentary, technical, and expert proof.

VI. CAUSES OF ACTION

157. To the extent any of the causes of action set forth below are perceived to duplicate any other cause of action, Plaintiff alleges any such perceived duplicative cause of action as an alternative form of relief to be consolidated, if applicable, before trial or submission to the jury as alternative counts subject to an appropriate instruction.

158. To the extent any theory of liability set forth below is perceived as inconsistent with or contradictory of any other theory of liability, or perceived as inconsistent with or contradictory of any allegation of fact, Plaintiff alleges any such perceived inconsistent or seemingly contradictory cause of action as an alternative form of relief, or fact supporting such an alternative form of relief, to be consolidated, if applicable, before trial or submission to the jury as alternative counts subject to an appropriate instruction.

FIRST CAUSE OF ACTION
VIOLATION OF THE FEDERAL ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. §§ 2511 AND 2520

159. Plaintiff repeats and realleges each and every preceding allegation as though fully set forth herein.

160. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, Plaintiff asserts this cause of action on behalf of himself and the California Class.

161. The Federal Electronic Communications Privacy Act prohibits intentionally intercepting, endeavoring to intercept, or procuring another person to intercept the contents of any wire, oral, or electronic communication through the use of an electronic, mechanical, or other device. The Act further prohibits intentionally using or disclosing the contents of any wire, oral, or electronic

communication, knowing or having reason to know that the information was obtained through an interception in violation of the Act.

162. The statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication [] while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. §§ 2511(3)(a).

163. Section 2520 provides a civil cause of action to a person whose electronic communication is intercepted, disclosed, or intentionally used in violation of the Act.

164. LinkedIn's website at issue is and was an electronic communications service within the meaning of the statute. As described herein, the site at issue enabled users like Plaintiff and the class members to send or receive wire or electronic communications within the meaning of the Wiretap Act. Through those services, users including Plaintiff and class members had the ability to send and receive electronic communications, including direct messages, connection requests, invitations, search requests, profile requests, job-related requests, notification data, and the corresponding server responses and session communications necessary to operate LinkedIn's platform.

165. During Plaintiff's and class members' live sessions, those electronic communications were transmitted between users' browsers and devices, on the one hand, and LinkedIn's site, servers, and related session infrastructure, on the other. The challenged APFC and related code executed during those transmissions and, as alleged herein, contemporaneously duplicated and transmitted content-bearing href, pathname, hash, and related page-context fields that relayed what Plaintiff and class members were doing, viewing, and/or requesting on LinkedIn

166. At all relevant times, Plaintiff Jeff Ganan used LinkedIn in California, from a computer at a residence in Los Angeles County, through a Chrome browser to request, receive, render, and interact with pages, feeds, profiles, searches, messages, job-related pages, and other features on linkedin.com. The transmissions between Plaintiff's browser and device, on the one hand, and LinkedIn's site, servers, and related session infrastructure, on the other, were electronic communications, including the signs, signals, writing, data, and intelligence exchanged as part of live page requests, page responses, and associated page-context and session communications.

167. During those live sessions, LinkedIn served and executed hidden client-side JavaScript and related code in Plaintiff's browser contemporaneously with page loads, user interactions, page rendering, and related requests and responses and thereby caused harm to Plaintiff and the class members as alleged below. In representative inspected builds, that code included APFC and DNA

fingerprinting logic, telemetry logic, and associated auxiliary integrations operating in parallel with the user's ordinary session.

168. LinkedIn's APFC code collected a feature internally identified as "location," which included fields including protocol, hostname, port, origin, href, hash, and pathname. By capturing href, pathname, hash, and related page-context field data, LinkedIn caused more than abstract addressing or routing information to be duplicated. Those duplicated fields included an array of content categories of the site, an array of content categories that describe the current section of the site the user is actively using or communicating with or through, URL of the page where the impression will be shown, referrer URL that caused navigation to the current page, details about the publisher object of the site, details about the content within the site, a list of keywords about the site, an array of behaviors undertaken by the user on the site, and other content information.

169. In other words, this data was content. Those fields relayed what Plaintiff and class members were doing, viewing, and/or requesting during their live LinkedIn sessions, including the specific page or feature being used, the context of the interaction, and the nature of the activity occurring during the session.

170. Plaintiff does not allege that every URL-related field is contents in every context. Plaintiff alleges that the descriptive page-context fields captured here, including href, pathname, hash, and related page-state values, conveyed the substance, purport, or meaning of Plaintiff's and class members' communications because those fields disclosed what those users were doing, viewing, and/or requesting during their live LinkedIn sessions.

171. LinkedIn's hidden code operated while Plaintiff's browser communications with LinkedIn were being sent, received, processed, and rendered in real time. The challenged acquisition was not limited to a later review of stored information. Instead, LinkedIn's code contemporaneously duplicated, extracted, and transmitted content-bearing page-context fields through a covert, separate, but simultaneous surveillance and telemetry channel during Plaintiff's live sessions.

172. On information and belief, LinkedIn packaged those duplicated content-bearing page-context fields together with other session-linked information, serialized and encrypted the resulting payload, stored the encrypted payload in the browser context, transmitted the payload to LinkedIn-controlled telemetry destinations including li/track and APFC-related collection endpoints, and propagated the resulting APFC value into subsequent API requests during the same session.

173. In representative inspected builds, LinkedIn also embedded concealed auxiliary integrations, including a hidden cross-origin iframe and related anti-fraud and anti-abuse scripts, that operated

during the same live sessions, received session-linked values, and engaged in cross-origin exchanges while the session was ongoing.

174. LinkedIn secretly caused a content-bearing duplicate to be furnished to a nonparty through a separate but simultaneous channel, and is therefore liable for procuring, aiding, using, or disclosing the interception. On information and belief, through the hidden scripts mentioned above, auxiliary integrations, and covert transmission paths, LinkedIn intentionally procured, caused, enabled, facilitated, and/or made possible the contemporaneous duplication, transmission, and interception of the contents of Plaintiff's and class members' electronic communications, including the content-bearing href, pathname, hash, and related page-context fields alleged herein, by LinkedIn's undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, and similar outside recipients.

175. Those outside recipients were not parties to Plaintiff's and class members' ordinary communications with LinkedIn for use of LinkedIn's services. Plaintiff and class members did not knowingly direct or send the duplicated content-bearing page-context communications to those outside recipients and did not authorize LinkedIn to create and route a separate copied stream of such contents to them.

176. The devices used to accomplish the interceptions, endeavors to intercept, and procurement of interception included, at a minimum, LinkedIn's hidden JavaScript and related code modules, Plaintiff's browser and computer as commandeered by that code, LinkedIn's telemetry transport and collection infrastructure, LinkedIn's APFC encryption and session-reuse mechanisms, and the concealed iframe, script, and cross-origin messaging components used to duplicate, transmit, and propagate the captured contents to outside recipients.

177. LinkedIn's extension-probing and DOM-scanning systems were part of the same covert architecture. Plaintiff does not allege that every extension-related signal, standing alone, independently constitutes Wiretap Act contents. Plaintiff alleges that those systems further show the intentional, sensitive, overbroad, and non-innocent design of the overall scheme through which LinkedIn caused content-bearing page-context communications to be duplicated, transmitted, and made available to undisclosed outside recipients.

178. LinkedIn's procurement of interception, endeavors to intercept, and related use and disclosure were intentional. LinkedIn designed, deployed, maintained, and executed APFC, DNA, related telemetry logic, and the associated auxiliary integrations for the purpose of acquiring, packaging, transmitting, reusing, and sharing the information described herein. The challenged conduct was not accidental and was not a passive or inevitable byproduct of ordinary page rendering.

179. LinkedIn knowingly embedded a concealed access and transmission point in users' live sessions. This concealed point was used by a third party to intercept, access, or to receive the contents of user communications. That third party maintained its own undisclosed cookies and cross-origin messaging channel. Either LinkedIn routed session-linked content data to that third party or the third party intercepted said data. This third party then went on to use that content data, Plaintiff's content data and the content data of the class members, including sensitive information about the behavior and personal information concerning Plaintiff and the class members, to enhance its own products and services, to share with the third party's other clients, to perform analytics to improve behavior prediction models, and for corporate marketing. When integrated into the products and services, this data and/or the information derived from the use of this data, the third party sells those products and services to other clients. In this sense, the third party monetizes the class member data at issue. All of this is done without disclosure or consent.

180. Plaintiff did not expressly or impliedly consent to LinkedIn's creation of a covert, separate, but simultaneous channel through which content-bearing page-context communications would be duplicated, transmitted, intercepted, used, disclosed, or made available to LinkedIn's undisclosed third-party data partners and similar outside recipients. LinkedIn did not clearly disclose that hidden code on linkedin.com would read, duplicate, and transmit href, pathname, hash, and related page-context fields from Plaintiff's live sessions, encrypt the resulting payload, propagate the resulting APFC value across later requests, and transmit or make those contents available to undisclosed outside recipients. General references to URLs, browser data, device features, security, anti-abuse, fraud prevention, add-ons, cookies, or automated systems did not amount to consent to the covert interception scheme alleged herein.

181. After the contents of Plaintiff's and class members' electronic communications were intercepted as alleged herein, LinkedIn intentionally used those contents and, on information and belief, intentionally disclosed them to, or made them available for use by, LinkedIn's undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, and similar outside recipients, knowing or having reason to know that the information had been obtained through the interceptions alleged herein.

182. LinkedIn used the intercepted contents to generate, encrypt, store, transmit, and session-reuse APFC and related telemetry tied to Plaintiff's and class members' browsers, accounts, sessions, and activities.

183. The challenged interceptions were not necessary to render the LinkedIn pages Plaintiff requested and were not limited to ordinary service functionality. LinkedIn already employed

multiple anti-fraud and anti-abuse measures, yet nonetheless chose to duplicate and transmit content-bearing page-context data and related live-session information through hidden code and auxiliary integrations to undisclosed outside recipients. The conduct alleged herein exceeded the scope of any purported authorization.

184. Plaintiff is informed and believes, and on that basis alleges, that the same acts were carried out through materially similar code, telemetry architecture, auxiliary integrations, and disclosures with respect to members of the proposed class while they used LinkedIn in California and/or elsewhere in the United States.

185. As a direct and proximate result of LinkedIn's violations of 18 U.S.C. § 2511, Plaintiff suffered injury, including invasion of privacy, unlawful interception, use, and disclosure of the contents of his electronic communications, loss of control over content-bearing session information and related browser-resident data, unauthorized use of his browser and computer resources, and the need to take protective measures against continued eavesdropping and surveillance. After learning of the challenged conduct, Plaintiff spent approximately $100.00 on a service to help protect his computer and device environment from further eavesdropping or surveillance.

186. Plaintiff is a person whose electronic communications were intercepted, disclosed, and/or intentionally used in violation of the Federal Wiretap Act and is therefore entitled to relief under 18 U.S.C. § 2520, including appropriate equitable and injunctive relief, statutory damages, actual damages to the extent proven, punitive damages as permitted by law, reasonable attorney's fees and litigation costs, and such other relief as the Court deems just and proper.

187. LinkedIn's conduct was willful, knowing, malicious, oppressive, and in conscious disregard of Plaintiff's and class members' rights under federal law.

SECOND CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE SECTION 502

188. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

189. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, he asserts this cause of action on behalf of himself and the California Class.

190. The California Legislature enacted the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"), to "expand the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to (including the extraction of data from) lawfully created computer data and computer systems," finding and declaring that "the proliferation

of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions . . . ." Cal. Penal Code § 502(a).

191. Plaintiff and the class members were owners of the data at issue and the compromised hardware, computers, and computer systems in question.

192. Direct Liability. As set forth above, LinkedIn directly violated California Penal Code § 502(c)(6) and (7). Among the ways LinkedIn is directly liable, LinkedIn knowingly and without permission provided third parties with access to and/or assisted third parties in accessing or causing to be accessed a computer, computer system, or computer network in violation of CDAFA, as alleged above. LinkedIn made false statements or deceptive omissions alleged at length above that induced Plaintiff and the class members to use the computer interface, provided to them by LinkedIn and to which third parties were given access by LinkedIn, for the purpose of allowing those third parties access to intercept, transmit, or receive private data, including personal information and behavioral information, without any disclosure thereof and without consent. These third parties went on to subject this stolen data to the non-permissioned secondary uses alleged above, including the undisclosed, nonconsensual monetization of their data.

193. LinkedIn had full knowledge of the third parties' wrongful access to Plaintiff's and class members' computers and data and was fully knowledgeable that the access was entirely without consent.

194. LinkedIn directly violated California Penal Code § 502(c)(8), which creates a cause of action against any person who "knowingly introduces any computer contaminant into any computer, computer system, or computer network."

195. A "computer contaminant" means "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network."

196. Within the meaning of CDAFA, LinkedIn's website introduced a computer contaminant to computers, computer systems, and computer networks that caused injury or damage to Plaintiff and

the class members as alleged herein—namely the interception, retrieval, and/or transmission of private data alleged above. This contaminant overcame Chrome's natural code-based security protocols and hid the existence thereof from Plaintiff and the class members.

197. LinkedIn's surreptitious injection of the code at issue constitutes a computer contaminant within the meaning of the law and was for the purpose of overcoming the technical and code-based barriers erected by the Chrome browser and adopted by Plaintiff and the class members to protect their private information and to keep that information secure, information that was within their computers, computer systems, and/or computer networks.

198. Chrome's extension architecture is designed to separate ordinary websites from the internal code and resources of users' installed browser extensions. Chrome's developer documentation explains that extensions and content scripts run in isolated execution worlds, that webpages cannot access the context and variables of those extension contexts, that webpages cannot connect to an extension unless the extension expressly permits such contact through externally_connectable, and that extension resources are not exposed to webpages unless the developer expressly declares them as web_accessible_resources. Chrome's own documentation further warns that making extension resources web-accessible can make an extension detectable by websites and attackers.

199. On information and belief, LinkedIn and/or its third party partners designed the challenged codes to route around those code-based separations. Rather than rely on any ordinary, user-facing browser feature, LinkedIn and/or its third party partners served hidden code that tested for the existence of installed extensions by attempting direct extension contact where possible, then falling back to resource probing, and then falling back again to DOM-based trace detection when the earlier methods failed. This behavior is designed and intended to avoid detection. It overcomes Chrome's code-based security protocols to protect user data by engaging in the processes alleged herein. And, it obtains user data, in part, by injecting code onto user computers that alters the code to transmit data and to avoid detection. It is coded like malware and it is nonpermissioned by the unsuspecting user—it is a computer contaminant the CDAFA protects against.

200. In representative inspected builds, LinkedIn's active extension-detection system used a hardcoded array containing thousands of extension identifiers paired with specific internal file paths. That system issued requests to URLs of the form chrome-extension://{id}/{file} for the purpose of determining whether the corresponding extension was installed and whether the targeted internal resource was exposed to the web page. The targeted file path was not incidental. It reflected prior identification by LinkedIn of a specific internal extension resource to be used as the probe target.

201. On information and belief, LinkedIn used that technique because Chrome does not provide ordinary webpages with a general-purpose mechanism to enumerate a user's installed extensions. Instead, LinkedIn tested thousands of candidate extension identifiers and known internal resource paths until the browser disclosed a positive response. In this way, LinkedIn exploited the narrow and conditional exposure created by web_accessible_resources to infer facts about software installed in the user's browser environment that Chrome's extension code system otherwise keeps separated from the host website.

202. LinkedIn's code also attempted direct extension communication as part of the same detection chain. Chrome's developer documentation states that, if an extension does not declare externally_connectable, webpages cannot connect to it. On information and belief, when a targeted extension did not permit such contact, LinkedIn treated that restriction not as a stopping point, but as a condition triggering fallback detection methods intended to arrive at the same answer by other means.

203. Even when an extension did not expose a probeable resource or did not permit direct webpage contact, LinkedIn employed a separate passive fallback mechanism referred to as Spectroscopy. In representative inspected builds, Spectroscopy recursively traversed the document tree and searched text nodes and HTML attributes for chrome-extension:// strings and related extension traces. Chrome's developer documentation explains that, although content scripts and webpages run in isolated execution contexts, they share access to the page's DOM. On information and belief, LinkedIn deliberately exploited that shared-DOM condition to infer the presence of extensions from traces those extensions left behind after interacting with the page, thereby allowing LinkedIn to identify extension activity even where the extension's own execution environment remained isolated.

204. LinkedIn did not perform these probes in a transparent or obvious manner. In representative inspected builds, LinkedIn's code could execute the probing logic only when the browser was idle through requestIdleCallback, and could further throttle the probes through a configurable staggerDetectionMs delay so that the requests were spread over time rather than launched in one obvious burst. The code also silently caught failed requests and discarded them without surfacing console warnings or user-facing notices. On information and belief, these implementation choices were intended to reduce performance visibility, minimize ordinary signs of the scan, and lower the likelihood that users would detect what LinkedIn's code was doing.

205. LinkedIn further concealed the challenged activity through auxiliary components that were not visible to ordinary users. In representative inspected builds, LinkedIn loaded a hidden cross-

origin iframe sized invisible at zero by zero pixels, positioned in a negative space off-screen, and marked hidden from assistive technologies. That concealed iframe operated during live sessions, received session-linked values, and participated in cross-origin exchanges while the same APFC and extension-detection systems were running. On information and belief, the concealed placement of that iframe and the associated cross-origin messaging path were designed to obscure from users the existence of an active outside-recipient communication endpoint operating in parallel with the user's ordinary LinkedIn session.

206. LinkedIn's APFC and DNA systems also serialized, encrypted, stored, transmitted, and reused the results of the challenged collection. In representative inspected builds, LinkedIn encrypted the fingerprint payload with the apfcDfPK key, stored the resulting value on globalThis.apfcDf, transmitted it to LinkedIn telemetry endpoints, and reused it by injecting it into later API requests during the same session. On information and belief, this design further reduced user transparency by preventing ordinary users from readily understanding the substance of what was being transmitted or how the results of the covert probing were being reused across later session activity.

207. The challenged conduct was materially different from ordinary page rendering. The LinkedIn pages Plaintiff requested could render without brute-force extension probing, fallback DOM trace mining, idle-time execution, staggered scheduling, concealed cross-origin auxiliary components, client-side encryption of the collected fingerprint, and session-wide propagation of the result. On information and belief, these features were included to cause users' browsers and devices to reveal information about installed software, browser state, and related environment characteristics that Chrome's architecture does not ordinarily provide to websites as a general feature.

208. By these acts, LinkedIn intentionally overcame, circumvented, or routed around Chrome's architectural and code-based safeguards that separate ordinary webpages from extension contexts, extension resources, and extension-derived traces. LinkedIn thereby caused Plaintiff's and class members' browsers and computers to disclose, process, and transmit information from the users' extension and browser environment without permission and beyond the scope of any authorization a reasonable user would understand by merely visiting or using LinkedIn's services.

209. Direct and/or Indirect Liability. LinkedIn is directly and indirectly liable for third-party actions alleged above.

210. LinkedIn and/or the third parties alleged above violated Cal. Pen. Code § 502(c)(1) by knowingly accessing and without permission using, altering, or damaging both Plaintiff's and the class members' computers, computer systems, computer networks, and their data contained therein,

in order to engage in the surveillance and data extraction alleged above. The code altered the users' computers as alleged above—access to the user data at issue wouldn't have been possible without such alteration by the code-based contaminant—and the extracted data was used and re-used as alleged above, including uses that monetized the stolen data.

211. LinkedIn and/or the third parties violated Cal. Pen. Code § 502(c)(2) by knowingly accessing and without permission taking, copying, and making use of Plaintiff's and class members' private data from Plaintiff's and class members' computers, computer systems, or computer networks.

212. LinkedIn and the third parties violated Cal. Pen. Code § 502(c)(3) by knowingly and without permission using or causing to be used "computer services" within the meaning of CDAFA causing injury and damages to Plaintiff and the class members alleged herein.

213. LinkedIn and/or the third parties violated Cal. Pen. Code § 502(c)(4) by knowingly accessing and without permission adding, altering, or damaging data, computer software, or computer programs residing or external to a computer, computer system, or computer network, causing injury and damages to Plaintiff and the class members alleged herein.

214. LinkedIn and/or the third parties violated Cal. Pen. Code § 502(c)(7) by knowingly and without permission accessing or causing to be accessed computers, computer systems, or computer networks causing injury and damages to Plaintiff and the class members alleged herein.

215. LinkedIn and/or the third party violated Cal. Pen. Code § 502(c)(8) by introducing a computer contaminant into computers, computer systems, or computer networks causing injury and damages to Plaintiff and the class members alleged herein.

216. LinkedIn is indirectly liable for the actions of any third party alleged above for aiding and abetting and/or conspiring to violate Cal. Pen. Code § 502, resulting in damage or loss to Plaintiff and the class members as alleged herein.

217. LinkedIn knowingly and without permission provided the means to third parties, and provided them assistance, in the hacking of computers, computer services, computer systems, and/or computer networks to access and use class member data without consent or permission.

218. Plaintiff and the class members have suffered damage or loss. Their private data has been published to third parties. Plaintiff has spent time and funds attempting to determine the extent and scope of the violations of Cal. Pen. Code § 502, in assessing the extent and scope of any alteration of or damage to his data, computers, computer systems, and computer networks, and to protect himself and his devices. Plaintiff has expended approximately $100.00 on services to protect his devices and identity after learning of these data breach and extraction issues.

219. Additionally, Plaintiff and the class members have been injured by LinkedIn's violation of Cal. Pen. Code § 502. CDAFA provides that the term "[i]njury means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program." As discussed above, the affected computer systems, computer networks, computer programs, or data have been altered or damaged with LinkedIn's and/or its third party's computer contaminants. LinkedIn has altered, damaged, or caused to be altered or damaged, Plaintiff's data, computers, computer systems, and/or computer networks, by, among other things, introducing and/or causing to be introduced, computer contaminants, which have recorded, transmitted information, modified, damaged, or destroyed information of Plaintiff and the class members, as alleged above.

220. For all of the above, Plaintiff and the class members are entitled to compensatory damages.

221. LinkedIn acted with oppression, fraud, and malice and, as such, Plaintiff and the class members are entitled to punitive or exemplary damages under Cal. Civ. Code 3294 as permitted per Cal. Pen. Code § 502(e)(4).

222. Plaintiff and the class members are entitled to equitable relief for LinkedIn's violation of Cal. Pen. Code § 502(c).

223. In addition to the above, even if there is no finding of damages or loss, Plaintiff and the class members are entitled to declaratory relief under Cal. Civ. Code Proc. § 1060 for LinkedIn's actions in violation Cal. Pen. Code § 502(c) as this claim presents substantial justiciable issues.

224. Plaintiff seeks an order for their attorney fees for which LinkedIn is liable pursuant to Cal. Pen. Code § 502(e)(2) for "any" action brought pursuant to Cal. Pen. Code § 502, including without limitation the action for damages, equitable relief, and/or declaratory judgment.

THIRD CAUSE OF ACTION

VIOLATION OF CAL. PENAL CODE §§ 638.50–638.51 (PEN REGISTER / TRAP AND TRACE DEVICE) AND § 637.2 (CIVIL REMEDY)

225. Plaintiff re-alleges and incorporates by reference the allegations in this Complaint regarding Defendant's installation and use of client-side code and embedded third-party code that records and transmits non-content dialing, routing, addressing, and signaling information ("DRAS") from users' browsers and devices during website sessions. This Count is pleaded in the alternative pursuant to Federal Rule of Civil Procedure 8(d), including as an alternative to any claim (elsewhere in the Complaint) that certain captured data constitutes the "contents" of a communication.

226. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, he asserts this cause of action on behalf of himself and the California Class.

227. The California Invasion of Privacy Act, Cal. Pen. Code § 630, *et seq*., ("CIPA") grants Plaintiff and class members the power to bring a private right of action to remedy the privacy violations alleged herein for $5,000.00 per violation. *See* Cal. Pen. Code § 637.2.

228. Cal. Penal Code § 638.51 prohibits any person from installing or using a pen register or trap-and-trace device absent a court order, subject only to narrow statutory exceptions.

229. Cal. Penal Code § 638.50 defines a "pen register" as any "device or process" that records or decodes "dialing, routing, addressing, or signaling information" transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the "contents" of a communication, and defines a "trap and trace device" as any "device or process" that captures incoming impulses identifying the originating number or other DRAS reasonably likely to identify the source of a wire or electronic communication, excluding contents.

230. Defendant installed and used a "device or process" within the meaning of California Penal Code sections 638.50 and 638.51 by deploying and executing JavaScript-based telemetry, synchronization, and network-interceptor code on visitors' browsers. Upon loading LinkedIn pages, that code ran locally on the user's device and performed automated collection, encoding, persistence, and transmission of non-content dialing, routing, addressing, and signaling information.

231. This Count is pleaded only with respect to non-content information. To the extent Defendant's systems also collected information elsewhere alleged to be the contents or meaning of a communication, Plaintiff does not rely on such content allegations for this Count and instead relies here on Defendant's collection, decoding, persistence, and transmission of non-content DRAS and source-identifying signaling data.

232. Among other non-content DRAS, the deployed process recorded, decoded, captured, or caused the transmission of source-identifying and session-linking signals, including but not limited to: WebRTC-derived local-network IP signals; protocol, hostname, port, and origin components of active page-location data; full user-agent and related browser-identification strings; session-linked cookie or identifier values; and device and browser signaling data sufficient to identify, distinguish, and correlate a particular device and session across repeated electronic communications.

233. The APFC Processes. In representative inspected builds, the APFC process serialized the collected signaling data, encrypted it, stored the resulting value on globalThis.apfcDf, transmitted it to /platform-telemetry/li/apfcDf and /apfc/collect, and then reused that value or an equivalent derived identifier during the same session.

234. On information and belief, the APFC process further persisted non-content identifiers and injected, appended, or otherwise propagated session-linked signaling values into subsequent

communications, including as HTTP request headers or equivalent request metadata, so that the same source-identifying information accompanied subsequent searches, profile views, message actions, feed loads, and other API requests during the browsing session.

235. In representative inspected builds, internal feature flags included sync.apfc.headers and pemberly.tracking.apfc.network.interceptor. On information and belief, these features reflect that Defendant's process was designed to synchronize APFC-derived identifiers into request headers and related network flows so that subsequent communications could be recognized, correlated, and monitored as originating from the same browser and device.

236. The information collected and transmitted as described in this Count was dialing, routing, addressing, or signaling information used to establish, route, identify, correlate, and monitor electronic communications and sessions. It was not limited to the one-time addressing information necessary for an initial page load. Instead, it constituted an ongoing session-identification and signaling mechanism that enabled repeated recognition of the source device across multiple electronic communications during the same session.

237. The same process also functioned as a trap-and-trace device or process within the meaning of section 638.50 because, when later requests carrying the same APFC-linked signaling value arrived at LinkedIn's systems and related integrations, the process captured incoming source-identifying impulses and related DRAS reasonably likely to identify the originating browser, device, and session.

238. The above-described conduct occurred in connection with wire or electronic communications transmitted between users' browsers and devices, on the one hand, and LinkedIn's servers and related telemetry infrastructure, on the other, including repeated HTTP requests and responses exchanged to load pages, obtain platform content, and carry out user actions during live sessions.

239. Defendant did not obtain a court order under California Penal Code sections 638.52 or 638.53 authorizing the installation or use of any pen register or trap-and-trace device or process on Plaintiff's or class members' browsers, devices, instruments, or facilities.

240. Defendant did not obtain Plaintiff's or class members' informed consent for the installation and operation of this pen-register and trap-and-trace process. Defendant did not clearly disclose that it would generate a session-linked APFC identifier, persist it, inject or append it into later requests, and use that identifier to correlate subsequent communications throughout the session. General references to URLs, browser data, device features, cookies, security, fraud prevention, or automated systems did not amount to informed consent to the background DRAS collection and header propagation alleged herein.

241. The fingerprinting processes. LinkedIn's APFC system was a fingerprinting process, but it was not merely a passive fingerprint stored for a single moment. In representative inspected builds, LinkedIn converted browser and device signals into a session-linked identifier, encrypted that identifier, stored it in the browser context, transmitted it to LinkedIn telemetry endpoints, and then caused the same identifier or an equivalent derivative to accompany subsequent API requests during the same session.

242. On information and belief, this transformed the APFC fingerprint into a signaling mechanism that identified and linked the source of later communications. The fingerprint, or the signaling value derived from it, did not vanish after collection. It followed the session and allowed LinkedIn and related recipients to recognize the same browser and device across repeated requests.

243. In this way, Defendant's fingerprinting process functioned as more than analytics. It acted as a device or process that recorded, decoded, and propagated dialing, routing, addressing, and signaling information used to identify and correlate the source of later electronic communications within the meaning of California Penal Code sections 638.50 and 638.51.

244. Defendant's processes were not a narrow or proportionate measure used only to operate, maintain, or test a communications service, or only to protect rights or property or protect users from abuse or any other disclosed reason. Instead, Defendant used a high-entropy, session-persistent, identity-linked signaling system that operated alongside multiple other anti-fraud tools, correlated the resulting identifiers to logged-in accounts, and swept far more broadly than any transaction-specific or narrowly tailored anti-abuse measure would require. Plaintiff and the class members did not consent to the actions described herein.

245. The overbreadth of the challenged process is further shown by its coexistence with Defendant's extension-probing and DOM-scanning systems, which were capable of identifying thousands of extensions and producing browserExtensionIds telemetry. Although Plaintiff does not rely on those extension outputs as the predicate DRAS for this Count, their integration into the same architecture demonstrates that Defendant's process was part of a broader identity-linked surveillance and profiling system rather than a narrowly confined technical safeguard.

246. Plaintiff and class members were injured by these violations, including by the invasion of legally protected privacy interests, the loss of control over their non-content addressing and signaling data, and the creation and reuse of persistent session-linked identifiers used to recognize, correlate, and profile them across repeated electronic communications. Plaintiff spent approximately $100.00 on services to protect his devices and identity after learning of these privacy violations.

247. Pursuant to California Penal Code section 637.2, Plaintiff and the class seek statutory damages, actual damages if any, injunctive relief, declaratory relief, and such other relief as the Court deems proper.

FOURTH CAUSE OF ACTION

VIOLATION OF CALIFORNIA PENAL CODE § 631

248. Plaintiff repeats and realleges each and every preceding allegation as though fully set forth herein.

249. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, he asserts this cause of action on behalf of himself and the California Class.

250. Section 631(a) of the California Penal Code imposes direct or indirect liability for four patterns of conduct. Liability under § 631(a) attaches to any person:

> [1] Who by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; OR
>
> [2] Who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; OR
>
> [3] Who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; OR
>
> [4] Who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

251. The numbering of § 631(a)'s clauses is added for clarity. The first three clauses set forth scenarios in which a person can be held liable directly, while the fourth clause creates indirect liability for a person who aids, abets, employs or conspires with another to violate one or more of the first three clauses.

252. The claims against LinkedIn under this count are limited to § 631(a)'s fourth prong, aiding and abetting liability. Plaintiff and class members communicated with LinkedIn for the ordinary purpose of using LinkedIn's services. LinkedIn nonetheless caused those communications, including

duplicated content-bearing href, pathname, hash, and related page-context fields relaying what users were doing, viewing, and/or requesting during live sessions, to be furnished through a separate but simultaneous channel to undisclosed outside recipients that were not parties to those communications, thereby aiding, agreeing with, employing, and procuring those outside recipients to read, attempt to read, or learn the contents or meaning of the communications, and thereafter using information so obtained.

253. LinkedIn and its third-party partners alleged herein are "persons" within the definition of the statute.

254. As alleged above, LinkedIn or its third-party partners violated CIPA by using machines, instruments, contrivances, or in other manners alleged in detail herein to intentionally "tap" or make unauthorized connections physically, electrically, acoustically, inductively, or otherwise, with telegraph or telephone wires, lines, cables, or instruments, including the wires, lines, cables, or instruments of any internal telephonic communication systems, with respect to the allegations set forth above. As alleged in this complaint, LinkedIn violated clause four by aiding, agreeing with, employing, or conspiring with other persons to violate clause one, two, and three.

255. California Penal Code section 631 prohibits, among other things, reading, attempting to read, learning, or attempting to learn the contents or meaning of any message, report, or communication while the same is in transit, passing over a wire, line, or cable, or being sent from, or received at, any place within this State, without the consent of all parties; using, or attempting to use, information so obtained; and aiding, agreeing with, employing, or conspiring with any person to do or permit those acts.

256. At all relevant times, Plaintiff Jeff Ganan used LinkedIn in California, from a computer in Los Angeles County, through a Chrome browser to request, receive, render, and interact with pages, feeds, profiles, searches, messages, job-related pages, and other features on linkedin.com. The transmissions between Plaintiff's browser and device, on the one hand, and LinkedIn's site, servers, and related session infrastructure, on the other, were communications within the meaning of section 631.

257. During those live sessions, LinkedIn served and executed hidden client-side code in Plaintiff's browser contemporaneously with page loads, user inputs, page rendering, session processing, and related requests and responses. In representative inspected builds, that code included APFC and DNA fingerprinting logic, telemetry logic, and associated auxiliary integrations operating in parallel with the user's ordinary session.

258. LinkedIn's hidden code collected a feature internally identified as "location," which included protocol, hostname, port, origin, href, hash, and pathname. In doing so, LinkedIn captured more than abstract destination or addressing information. By capturing href, pathname, hash, and related page-context values from Plaintiff's live LinkedIn sessions, LinkedIn caused information to be duplicated that relayed what Plaintiff and class members were doing, viewing, and/or requesting on LinkedIn, including the specific page or feature being used, the context of the interaction, and the nature of the activity occurring during the session.

259. Plaintiff does not allege that every URL-related field is contents in every context. Plaintiff alleges that the descriptive page-context fields captured here, including href, pathname, hash, and related page-state values, conveyed the contents or meaning of Plaintiff's and class members' communications because those fields disclosed what those users were doing, viewing, and/or requesting during their live LinkedIn sessions.

260. LinkedIn's hidden code operated while Plaintiff's browser communications with LinkedIn were being sent, received, processed, and rendered in real time. The challenged conduct was not limited to a later review of stored information. Instead, LinkedIn's code contemporaneously duplicated and transmitted content-bearing page-context fields through a covert, separate, but simultaneous surveillance and telemetry channel during Plaintiff's live sessions.

261. On information and belief, LinkedIn packaged those duplicated content-bearing page-context fields together with other session-linked information, serialized and encrypted the resulting payload, stored the encrypted payload in the browser context, transmitted the payload to LinkedIn-controlled telemetry destinations including li/track and APFC-related collection endpoints, and propagated the resulting APFC value into subsequent API requests during the same session.

262. In representative inspected builds, LinkedIn also embedded concealed auxiliary integrations, including a hidden cross-origin iframe and related anti-fraud and anti-abuse scripts, that operated during the same live sessions, received session-linked values, and engaged in cross-origin exchanges while the session was ongoing.

263. On information and belief, LinkedIn thereby caused the contents or meaning of Plaintiff's and class members' communications, including the duplicated content-bearing href, pathname, hash, and related page-context fields alleged herein, to be transmitted to, disclosed to, and/or made available for contemporaneous interception or acquisition by LinkedIn's undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, and similar outside recipients through that covert, separate, but simultaneous channel, who uses that content data for their own purposes.

264. LinkedIn knowingly embedded a concealed access and transmission point in users' live sessions. This concealed point was used by a third party to intercept, access, or to receive the contents of user communications. That third party maintained its own undisclosed cookies and cross-origin messaging channel. Either LinkedIn routed session-linked content data to that third party or the third party intercepted said data. This third party then went on to use that content data, Plaintiff's content data and the content data of the class members, including not sensitive information about the behavior and personal information concerning Plaintiff and the class members, to enhance its own products and services, to share with the third party's other clients, to perform analytics to improve behavior prediction models, and for corporate marketing. When integrated into the products and services, this data and/or the information derived from the use of this data, the third party sells those products and services to other clients. In this sense, the third party monetizes the class member data at issue. All of this is done without disclosure or consent.

265. Those outside recipients were not parties to Plaintiff's and class members' ordinary communications with LinkedIn for use of LinkedIn's services. Plaintiff and class members did not knowingly communicate those duplicated contents to such outside recipients and did not authorize LinkedIn to create a separate copied stream of content-bearing session data for transmission, disclosure, or interception by them.

266. LinkedIn intentionally aided, agreed with, employed, procured, and/or conspired with those outside recipients to read, attempt to read, learn, or attempt to learn the contents or meaning of Plaintiff's and class members' communications without consent, including by embedding the hidden code, auxiliary integrations, and covert transmission path described herein, and by causing the duplicated contents to be routed through that path during live sessions.

267. Alternatively and additionally, after causing the contents or meaning of Plaintiff's and class members' communications to be obtained as alleged herein, LinkedIn intentionally used that information and, on information and belief, disclosed it to or made it available for use by LinkedIn's undisclosed third-party data partners, anti-fraud partners, anti-abuse partners, and similar outside recipients, knowing or having reason to know that the information had been obtained through the conduct alleged herein.

268. LinkedIn used the information so obtained to generate, encrypt, store, transmit, and session-reuse APFC and related telemetry tied to Plaintiff's and class members' browsers, accounts, sessions, and activities.

269. LinkedIn's extension-probing and DOM-scanning systems were part of the same covert browser-surveillance architecture. Plaintiff does not allege that every extension-related signal,

standing alone, independently constitutes the contents of a communication under section 631. Plaintiff alleges that this extension-probing and DOM-scanning architecture further demonstrates the intentional, technically sophisticated, overbroad, and non-innocent design of the overall scheme through which LinkedIn duplicated, transmitted, and made available content-bearing page-context communications to undisclosed outside recipients.

270. Plaintiff did not consent to LinkedIn's creation of a covert, separate, but simultaneous channel through which content-bearing page-context communications would be duplicated, transmitted, used, disclosed, or made available to undisclosed outside recipients. LinkedIn did not clearly disclose that hidden code on linkedin.com would extract and transmit href, pathname, hash, and related page-context fields from Plaintiff's live sessions, encrypt the resulting payload, propagate the resulting APFC value across later requests, and transmit or make the contents or meaning of those communications available to undisclosed third-party partners. General references to URLs, browser data, device features, security, anti-abuse, fraud prevention, add-ons, cookies, or automated systems did not amount to consent to the covert contents-interception scheme alleged herein.

271. Plaintiff used LinkedIn for ordinary professional-networking purposes. Plaintiff did not knowingly authorize LinkedIn to create a separate copied communication stream for undisclosed outside recipients, and did not knowingly authorize those outside recipients to intercept, receive, read, attempt to read, learn, use, or store the contents or meaning of his communications.

272. The challenged conduct exceeded any ordinary, disclosed, or consented-to website functionality. LinkedIn already employed multiple anti-fraud and anti-abuse measures, yet nonetheless chose to duplicate and transmit content-bearing page-context data and related live-session information through hidden code and auxiliary integrations to undisclosed outside recipients. The conduct alleged herein exceeded the scope of any purported authorization.

273. Plaintiff is informed and believes, and on that basis alleges, that the same acts were carried out through materially similar code, telemetry architecture, auxiliary integrations, and disclosures with respect to members of the proposed class while they used LinkedIn in California.

274. As a direct and proximate result of LinkedIn's violations of section 631, Plaintiff suffered injury, including invasion of privacy, unlawful acquisition, use, and disclosure of the contents or meaning of his communications, loss of control over content-bearing session information and related browser-resident data, unauthorized use of his browser and computer resources, and the need to take protective measures against continued eavesdropping and surveillance. After learning of the

challenged conduct, Plaintiff purchased spent approximately $100.00 on services to help protect his devices and protect his identity after learning of these privacy violations.

275. Plaintiff and class members are each persons injured by LinkedIn's violations of California Penal Code section 631 and are therefore entitled to relief under California Penal Code section 637.2, including the greater of statutory damages or actual damages according to proof, injunctive relief, and such other preliminary, equitable, declaratory, and further relief as the Court deems proper.

276. LinkedIn's conduct was willful, knowing, malicious, oppressive, and in conscious disregard of Plaintiff's and class members' statutory privacy rights.

FIFTH CAUSE OF ACTION

INVASION OF PRIVACY IN VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION

277. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

278. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, he asserts this cause of action on behalf of himself and the California Class.

279. Article I, section 1 of the California Constitution protects Plaintiff's and class members' privacy rights, including their informational privacy interests and their interests in controlling unnecessary collection and misuse of personal information.

280. Plaintiff and class members had legally protected privacy interests in the software, extension-related information, browser-resident traces, device-resident characteristics, session-linked identifiers, and other browser and device information collected or derived through the challenged conduct.

281. Plaintiff and class members also had a reasonable expectation of privacy, particularly when using LinkedIn from personal and household computers or devices in California residences, that LinkedIn would not covertly interrogate their browsers and computers for installed extensions, extension traces, and session-linked fingerprinting data absent clear disclosure and informed authorization. They further had a reasonable expectation of privacy in the security and integrity of their data, communications, and the contents of their data—not that any of that material would be shared or exposed or available to nondisclosed third parties, with the ability to reuse that data for their own purposes.

282. Defendant intentionally collected, inferred, transmitted, stored, and reused such information through covert browser probing, DOM scanning, fingerprinting, and related telemetry.

283. The invasion was serious. It was covert, repeated, technically sophisticated, overinclusive, identity-linked, and broader than reasonably necessary to render LinkedIn's services or to address narrow anti-abuse objectives. It reached information users did not meaningfully expose to LinkedIn as part of ordinary page use.

284. Any generalized disclosure that LinkedIn receives routine browser or add-on information, uses data for security or fraud prevention, or uses anti-abuse cookies did not clearly disclose the specific practices alleged herein and did not negate Plaintiff's or class members' reasonable expectations of privacy.

285. Even if Defendant possessed a legitimate interest in combating scraping, fraud, abuse, or automation, Defendant's means were not reasonably necessary or proportionate because Defendant already employed multiple anti-abuse technologies and nevertheless chose to engage in mass browser probing, DOM scanning, broad extension targeting, and session-linked fingerprint reuse.

286. In the name of an anti-fraud and abuse, LinkedIn intentionally engaged in a massive surveillance program affecting potentially tens of millions of people. This is an outrageous violation of privacy.

287. Defendant's conduct therefore violated Plaintiff's and class members' rights to privacy under article I, section 1 of the California Constitution.

288. As a direct and proximate result of Defendant's conduct, Plaintiff and class members suffered the injuries and damages alleged herein and are entitled to compensatory, equitable, declaratory, injunctive, and other relief allowed by law.

SIXTH CAUSE OF ACTION

INTRUSION UPON SECLUSION

289. Plaintiff realleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

290. Plaintiff asserts this cause of action on behalf of himself and the Nationwide Class. Alternatively, he asserts this cause of action on behalf of himself and the California Class.

291. Plaintiff and class members had a reasonable expectation of privacy in the personal browser and device environments they used from their California residences and personal or household computers, including installed-extension presence, extension traces, browser-resident information, and other device-linked information not knowingly furnished to LinkedIn in the manner alleged herein. Plaintiff certainly had no expectation that his data, communications, their content would not be made available to undisclosed third parties with the ability to reuse that information.

292. Defendant intentionally intruded into that private sphere by causing LinkedIn-served code to probe extension resources, scan the DOM for extension traces, and collect account- or session-linked browser and device fingerprints.

293. Defendant's intrusion was highly offensive to a reasonable person because it was covert, technically sophisticated, not requested by the user, broader than ordinary page functionality, directed at personal browser and device information, performed at scale, linked to real identities and professional profiles, and broader than reasonably necessary for narrow anti-abuse objectives.

294. The offensiveness of the intrusion is heightened by Defendant's choice to perform the challenged conduct without clear advance disclosure, while using generic anti-abuse language that did not tell users what was actually occurring.

295. The offensiveness of the intrusion is further heightened by the breadth of the target list, which, on information and belief, included categories of extensions that had little or no obvious relation to narrow anti-scraping needs.

296. Defendant's conduct was not de minimis. It involved active browser-resource probing, full DOM traversal for extension traces, broad fingerprint collection, encrypted telemetry, and session-linked reuse of the resulting profile.

297. As a direct and proximate result of Defendant's intrusion, Plaintiff and class members suffered harm, including invasion of privacy, loss of control over personal browser and device information, unauthorized use of computer resources, time spent investigating and responding, and other damages according to proof.

298. Defendant acted intentionally and with conscious disregard of Plaintiff's and class members' privacy rights.

299. Plaintiff and class members are therefore entitled to damages, punitive or exemplary damages as permitted by law, and injunctive and other equitable relief.

VII. PRAYER FOR RELIEF

300. Wherefore, Plaintiff, on behalf of himself and the proposed classes, prays for judgment against Defendant as follows:

301. For an order certifying this action as a class action under the Federal Rules of Civil Procedure, appointing Plaintiff as class representative, and appointing Plaintiff's counsel as class counsel.

302. For compensatory, general, special, and consequential damages according to proof.

303. For exemplary damages as permitted by law.

304. For declaratory relief that Defendant's challenged conduct violated California law.

305. For preliminary and permanent injunctive relief prohibiting Defendant from continuing the challenged browser probing, DOM scanning, fingerprinting, and related telemetry practices without clear and lawful disclosure and authorization, and requiring Defendant to cease using, retain no longer than lawful and necessary, and delete or disassociate extension-detection and related fingerprint data collected through the challenged practices to the extent traceable to Plaintiff and class members.

306. For reasonable attorney's fees and costs as permitted by statute, including Penal Code section 502, and by other applicable law.

307. For pre-judgment and post-judgment interest as allowed by law.

308. For such other and further relief as the Court deems just and proper.

VIII. JURY DEMAND

309. Plaintiff hereby demands a trial by jury on all issues so triable.

.

Respectfully submitted,

J.R. HOWELL,
LAW OFFICE OF J.R. HOWELL

Date: April 6, 2026

By: _____
J.R. Howell (State Bar No. 268086)
Attorney for Plaintiff and the Proposed Class