MOGIN LAW LLP
Daniel J. Mogin (SBN No. 95624)
Timothy Z. LaComb (SBN No. 314244)
4225 Executive Square, Suite 600
La Jolla, CA 92037
Telephone: (619) 687-6611
Facsimile: (619) 687-6610
dmogin@moginlawllp.com
tlacomb@moginlawllp.com

JOSEPH SAVERI LAW FIRM, LLP
Joseph R. Saveri (SBN 130064)
Cadio Zirpoli (SBN 179108)
Kevin E. Rayhill (SBN 267496)
Holden Benon (SBN 325847)
601 California Street, Suite 1505
San Francisco, CA 94108
Tel.: (415) 500-6800
jsaveri@saverilawfirm.com
czirpoli@saverilawfirm.com
hbenon@saverilawfirm.com
krayhill@saverilawfirm.com

DON BIVENS PLLC
Don Bivens (*pro hac vice* forthcoming)
15169 N. Scottsdale Road, Suite 205
Scottsdale, AZ 85254
Telephone: (602) 762-2661
don@donbivens.com

Counsel for Plaintiffs and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF ALAMEDA

DANIEL WINE, ALLISON BLANK, SANDRA SION, and KEVIN SMITH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

WUNDERKIND CORP., a Delaware corporation,

Defendant.

Case No.: 25CV145737

CLASS ACTION COMPLAINT FOR:

Violation of Cal. Penal Code § 631
Violation of Cal. Penal Code § 638.51
Violation of Cal. Penal Code § 502
Violation of the California Constitution Art. 1, § 1
Violation of Cal. Bus. & Prof. Code § 17200, *et seq*.
Common Law Invasion of Privacy – Intrusion Upon Seclusion

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Daniel Wine, Allison Blank, Sandra Sion, and Kevin Smith ("Plaintiffs") bring this Class Action Complaint and Demand for Jury Trial against Defendant Wunderkind, Inc. ("Defendant" or "Wunderkind") for surreptitiously collecting information regarding consumers' web browsing activities and behaviors while using subject websites. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. To ensure its citizens enjoy the constitutionally recognized right to privacy and to protect against the threat to this right posed by new surveillance technology (like online tracking software), the California Legislature enacted the California Invasion of Privacy Act ("CIPA"). CIPA makes it unlawful for a third party (like Defendant Wunderkind) to intercept communications between a website visitor and the website operator without the website visitor's consent. CIPA also makes it unlawful for third parties to record, decode, or capture addressing or signaling information through use of a "pen register" or "trap and trace" device without the website visitor's consent. As discussed in detail below, Wunderkind unambiguously, egregiously, and repeatedly violated these sections of CIPA, as well as other California statutes and common law torts, by intercepting Plaintiffs' and Class members' communications with website operators without consent, using devices to record and capture their addressing and signaling information without consent, using the intercepted data to create substantive consumer profiles for them, and ultimately monetizing the intercepted data.

2. Wunderkind is an online surveillance conglomerate with the explicit goal of knowing "all that is knowable about [website operators'] customers to drive contextual and personalized experiences."[1] Stated in laymen's terms, Wunderkind uses tracking and related technology to intercept as much data as possible about individuals so it can learn about them, predict their consumer behaviors, and target them with directed advertisements. It utilizes several tactics to effectuate that goal – many of them unlawful.

[1] https://www.wunderkind.co/platform/identity/.

3. Even though intercepting data without consent violates several California laws, Wunderkind uses its tracking software to intercept data from more than a billion individuals when they visit any of the thousands of websites on which Wunderkind's software is installed. Wunderkind not only intercepts communications between the individual and the website (e.g., search terms entered into an internal search bar) but also intercepts the individual's "digital body language," which includes things like how a cursor is moving on a webpage or the amount of time a user has been idle on a webpage. Wunderkind feeds this data into its proprietary artificial intelligence ("AI") and machine learning systems to understand the intent of the individual, predict next actions by the individual, and determine the precise moment to target him or her with a specific advertisement, such as when a person is getting ready to leave a website. Put differently, Wunderkind not only intercepts communications between website visitors and website operators but also watches the website visitors while they do it.

4. The scale and scope of Wunderkind's data collection practices are staggering. According to Wunderkind, 25% of combined total digital eCommerce revenue is driven by marketing texts and emails sent by Wunderkind to website visitors they have identified. Wunderkind also boasts that it has created consumer profiles for more than a billion people, recognized more than 9 billion devices, and tracked more than 2 trillion digital events per year.

5. But intercepting the data is only part of the equation. Wunderkind also matches the data to a specific individual to later target them with advertisements. To accomplish this, Wunderkind either intercepts personal information when a user inputs it into a website (e.g., entering a name, email address, or phone number on a web form) or intercepts identifiers that its Identity Network can use to identify otherwise anonymous web traffic. Wunderkind is so effective at identifying anonymous website users that it can also identify when a person is using a new device (and, therefore, connects that device to the individual) or when a person is engaging with a different platform.

6. Once Wunderkind identifies the person behind the communications, it creates a user profile or "PrivacyID" for that person. The PrivacyID is a comprehensive profile that enables Wunderkind to track and assign intercepted data to that user across websites, platforms, and

devices. The PrivacyID does not expire or reset and was designed to evade traditional privacy protections like clearing cookies, operating in incognito modes, and using VPNs. Wunderkind, therefore, secretly and without consent creates an ever-expanding, substantive, and durable consumer profile for individuals that is immune to traditional privacy protections and uses that comprehensive profile to predict future behaviors to perfectly time advertisements.

7. Through these practices, and those discussed below, Wunderkind violated several California laws that protect the privacy interests of its residents, including: Cal. Penal Code §§ 631, 638.51, 502; Article 1, § 1 of the California Constitution; Cal. Bus. & Prof. Code § 17200, *et seq.*; and committed a common law invasion of Plaintiffs' and Class Members' privacy.

PARTIES

8. Plaintiff Daniel Wine is a natural person and citizen of California. Mr. Wine was in California when he visited CNN.com. Wunderkind unlawfully tracks and intercepts data from individuals when they use this website. In addition, CNN.com does not obtain consent from or provide notice to website visitors that Wunderkind is tracking them and intercepting their data.

9. Plaintiff Allison Blank is a natural person and citizen of California. Ms. Blank was in California when she visited CNN.com and Imgur.com, two of the many websites through which Wunderkind mines information from site visitors without their consent. Wunderkind unlawfully tracks and intercepts data from individuals when they use these websites. In addition, neither CNN.com nor Imgur.com obtain consent from or provide notice to website visitors that Wunderkind is engaging in its data interception and tracking practices.

10. Plaintiff Sandra Sion is a natural person and citizen of California. Ms. Sion was in California when she visited Legacy.com, one of the many websites through which Wunderkind mines information from site visitors without their consent. Wunderkind unlawfully tracks and intercepts data from individuals when they use this website. In addition, Legacy.com does not obtain consent from or provide notice to website visitors that Wunderkind is engaging in its data interception and tracking practices.

11. Plaintiff Kevin Smith is a natural person and citizen of California. Mr. Smith was in California when he visited CNN.com and Everlane.com, two of the many websites through which

Wunderkind mines information from sites visitors without their consent. Wunderkind unlawfully tracks and intercepts data from individuals when they use these websites. In addition, neither CNN.com nor Everlane.com obtain consent from or provide notice to website visitors that Wunderkind is engaging in its data interception and tracking practices.

12. Defendant Wunderkind, Inc. is a corporation organized and existing under the laws of Delaware with its principal place of business located at 1 World Trade Center, Floor 74, New York, New York 10007.

JURISDICTION AND VENUE

13. This Court has jurisdiction pursuant to Article VI, Section 4 of the California Constitution and Code of Civil Procedure Section 410.10.

14. This Court has personal jurisdiction over Defendant because Defendant

15. conducts significant business throughout the State of California. Moreover, Wunderkind is a registered data broker in California, and it has purposefully directed its conduct toward California residents. Through the deployment of its tracking technology on widely accessed websites, Wunderkind caused the unauthorized interception and collection of data from California residents while they were physically located in the state, constituting significant, continuous, and pervasive contacts with the State of California.

16. Venue is proper pursuant to Code of Civil Procedure § 395.5 because the obligation or liability giving rise to this action arose in this county.

COMMON FACTUAL ALLEGATIONS

A. Background of CIPA

17. The California Legislature enacted CIPA to protect the privacy rights of California citizens. In doing so, the California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

18. Section 631(a) of CIPA prohibits any of the following, "by means of any machine, instrument, contrivance, or in any other manner":

Intentionally tap[ping], or mak[ing] 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

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[ing] or attempt[ing] to read or 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

Us[ing], or attempt[ing] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

or

Aid[ing], agree[ing] with, employ[ing], or conspire[ing] 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.

19. CIPA extends to new technologies like software tracking. Notably, "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted." *Vishal Shah v. Fandom, Inc*., 754 F. Supp. 3d 924, 930-931 (N.D. Cal. Oct. 21, 1994). Likewise, the "California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc*., No. 13-MD-02430, 2013 U.S. Dist. LEXIS 172784, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013). As such, "courts have repeatedly held" that CIPA is "not limited to the traditional versions of the tools at issue" and have applied CIPA to online tracking technologies "based on the plain language of the statute, the California Supreme Court's pronouncements regarding the broad legislative intent underlying CIPA," and "the California courts' approach to updating obsolete statutes in light of emerging technologies." *Vishal*, 754 F. Supp. 3d at 930-931.

20. Moreover, CIPA § 638.51(a) prohibits companies from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

21. A "pen register" is a "device or process that records or decodes dialing, rerouting, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 683.50(b). A "trap and trace" device is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.*

22. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless of whether they suffered actual damages. Cal. Penal Code § 637.2(a)(1).

23. In addition, Article I, Section 1, of the California Constitution lists privacy as a fundamental right of all Californians and provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1. A party has a private right of action against a party that violates this privacy right when it can show (i) it has a legally protected privacy interest in the information at issue (e.g., privacy interest in keeping browsing activity and online interactions private); (ii) it has a reasonable expectation of privacy in the information at issue; and (iii) an intrusion into the privacy interest at issue constitutes an egregious breach of social norms (e.g., watching someone interact with a website and intercepting communications and browsing data without consent).

24. Also, California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice . . .." Cal. Bus. & Prof. Code § 17200. The data collection practices challenged herein form the crux of Defendant's business model, meaning they are unequivocally a business act or practice. And, as shown herein, such conduct is both unlawful (violates CIPA, the UCL, the California Constitution and other statutes and common law torts) and unfair.

B. Background of Wunderkind

25. Wunderkind operates a marketing platform that promises to "increase[] revenue from [website operators'] digital traffic."[2] As Wunderkind explains, its "proprietary identity network recognizes anonymous visitors, combines real-time behavioral signals and autonomously triggers the highest-performing messages across email, text, social, and advertising channels."[3] To do this, Wunderkind must intercept data from and otherwise spy on website visitors.

26. According to Wunderkind, 25% of combined total digital eCommerce revenue is driven by marketing texts and emails sent by Wunderkind to website visitors they have identified. Wunderkind also boasts that it has created consumer profiles for more than a billion people, recognized more than 9 billion devices, and tracked more than 2 trillion digital events per year.

27. Wunderkind promises that its platform "increases revenue through reach and seamlessly integrates into [the website operator's] existing stack, meaning no replatforming needed."[4] According to Wunderkind, "[i]ts all about revenue, all on your own terms and in your own tech."[5]

28. To achieve the revenue increases it promises, Wunderkind engages in systematic and non-consensual online tracking of individuals through its software and related tools. Specifically, Wunderkind has (i) induced thousands of website operators to install its tracking software on their websites; (ii) used the tracking software to intercept data from website visitors in real time; (iii) used the intercepted data and/or its Identity Network to identify those visitors, including when the visitors took steps to prevent such identification and tracking; (iv) created substantive and durable consumer profiles for the individuals once they are identified by assigning them a "PrivacyID," which both elude traditional privacy safeguards consumers use to prevent online tracking and track individuals across devices and websites; and (v) used the consumer profiles in combination with its AI to track and watch website visitors as they interact with the websites, predict future behavior based on the intercepted data, and use that information to determine the exact moment during which

[2] https://www.wunderkind.co/.
[3] *Id.*
[4] *Id.*
[5] *Id.*

they should target them with advertisements (e.g., when a website visitor is getting ready to leave the website).

29. For many websites on which Wunderkind's software is installed, website visitors are neither informed that Wunderkind is intercepting their data nor required to consent to the data interception. This is true for every website at issue in this case and includes: CNN.com, imgur.com, Legacy.com, Macys.com, HelloFresh.com, and Everlane.com. As discussed above, each Plaintiff visited at least one of these websites and, as a result, had their data intercepted as discussed herein.

C. Wunderkind Uses its Identity Network to Identify and Assign a PrivacyID to Website Visitors

30. Generally, a person visiting a website remains anonymous to the website operator unless the visitor takes affirmative steps like inputting their name, email address, and/or phone number. Absent this type of information, website operators are generally unable to identify website visitors. And, even when providing the website operator with this information, the visitor does not expect this personal information to be intercepted by an unknown third party.

31. Wunderkind estimates that "over 90% of web traffic remains anonymous."[6] Website operators do not like this because "customers are browsing [their] website, but [they] have no idea who they are."[7] This is akin to a person walking into a brick-and-mortar store, browsing, and leaving without making a purchase or providing identifiable information. The store operator does not know who the visitor was and would be unable to directly advertise to him or her as a result.

32. Wunderkind designed its Identity Network and related tools to de-anonymize website traffic for website operators by identifying website visitors regardless of whether they took affirmative steps to identify themselves. In its own words, the "cutting-edge [Identity Network] solution enables marketers to bridge the gap between anonymous web traffic and actionable first-party data" and allows website operators to "recognize and understand consumer behavior at scale."[8] This is akin to a brick-and-mortar store using facial recognition software to identify

---

[6] https://www.wunderkind.co/blog/article/unlocking-the-power-of-wunderkinds-identity-graph-for-personalized-marketing/.

[7] *Id.*

[8] *Id.*

consumers without their consent or knowledge, recording which sections of the store they visited and which products they viewed, and targeting them with advertisements as a result.

33. The core of the Identity Network is the Identity Graph, which is "a comprehensive and proprietary database that stores and manages vast amounts of e-commerce, travel, and publisher client data collected by Wunderkind."[9] By analyzing intercepted data indicating IP address, browser version, and/or device type of the user and using tools like cross-website identification, advanced machine learning, cross-device tracking, cookies, and other non-cookie signals, the Identity Graph can determine who website visitors are regardless of whether the user took affirmative steps to identify themselves.

34. Once Wunderkind identifies an individual on a website, it assigns the individual a PrivacyID. The PrivacyID brings together multiple identifiers for the individual, such as email addresses, phone numbers, device IDs, and even third-party IDs, into a single, unified user profile that is meant to capture user online behavior and engagement.

35. The PrivacyID follows the individual across devices, platforms, and websites. Wunderkind designed the PrivacyID and its tracking software to be durable and evade tools that website visitors traditionally used to prevent this type of tracking. For example, website visitors can typically prevent or limit pixel tracking by taking any of the following actions: clearing cookies, navigating the internet in a privacy mode (e.g., Google's incognito mode), and/or using VPNs to prevent tracking. However, Wunderkind designed the PrivacyID and related tracking technology to evade these tools, as none limit (let alone prevent) Wunderkind from tracking and intercepting website visitor data. In addition, unlike traditional cookies that reset fairly frequently, Wunderkind designed the PrivacyID to neither expire nor reset. The effects of this decision are twofold: (i) it prevents consumers from using common privacy safeguards (such as clearing cookies) to prevent Wunderkind from tracking their behavior and (ii) enables Wunderkind to more effectively track consumers across multiple devices and websites.

[9] https://www.wunderskind.com/blog/article/unlocking-the-power-of-wunderkinds-identity-graph-for-personalized-marketing/index.htm.

D. Once Assigned a PrivacyID, Wunderkind Tracks Website Visitors Across Websites and Devices

36. After Wunderkind assigns an individual a PrivacyID, it tracks that individual across thousands of websites on which Wunderkind's software has been installed, covertly intercepting data about the individual all the while. To intercept the data, Wunderkind uses invisible tags, pixels, and related tracking software to instantaneously and automatically send website visitors' data and communications with website operators to Wunderkind.

37. Wunderkind intercepts at least the following data from website visitors: online browsing data (i.e., what webpages a consumer has visited and for how long); purchase and consumer data (i.e., the products the individual has purchased); abandoned cart data (i.e., data showing what items a person placed in their online shopping cart but did not purchase); input data (email addresses, phone numbers, and addresses); device information (IP addresses, device details, browser types, and referral sources); and location data of the user.

38. Wunderkind also intercepts several types of behavioral data, including (i) how a user is scrolling on a website; (ii) the level of activity of a user on a webpage; (iii) how and where a user's cursor is moving on a website; (iv) when a user indicates an intent to leave a website; and (v) other mouse and key actions that indicate an intent to act by website visitors.

39. When talking about its customer profiles in an article, Wunderkind lists the following as some of the data it intercepts.[10]

[10] https://www.wunderkind.co/blog/article/one-to-one-marketing/#:~:text=One-to-one%20as%20a%20marketing%20strategy%20isn%E2%80%99t.

> Marketers talk a lot about customer personas, but to make one-to-one marketing work, you have to build segments of "one." Drill down to the customer level.
>
> Data can tell you a lot about any given customer. Create a unique profile for all of your prospects and customers using:
>
> - Browsing Data: What pages do they visit? For how long?
> - Purchase Data: Have they already purchased from you? If so, what did they buy? Are there patterns?
> - Abandoned Cart Data: How likely are they to make a purchase or are they serial shoppers?
> - Customer Support/Sales Touchpoint Data: Have they spoken with someone on your team before?
> - NPS (Net Promoter Score) Data: How satisfied are they with your business?
>
> You need to know more than their title and demographics, but exactly where they are in the funnel and what they need to get them to click that "Buy" button again and again.

40. Wunderkind intercepts this user data because it wants to know exactly what website visitors are doing on their clients' websites so it can show the visitors advertisements at the exact moment the user is most likely to engage with the advertisement. The more effective Wunderkind is at predicting user engagement, the more revenue its clients generate through advertising. And, the more revenue that is attributable to Wunderkind's services and software, the more likely businesses are to purchase them.

41. Wunderkind leverages the intercepted data and WunderkindAI to identify consumers and to predict their future behaviors. As Wunderkind explains, "by combining identity, behavioral data, and agentic automation, Wunderkind doesn't just react to consumers—it anticipates their intent."[11]

E. Wunderkind Intercepted Plaintiffs' and Class Members' Data Without Consent

42. For the websites identified herein and those at issue in this case, Wunderkind intercepts data from website visitors without consent or informing the website visitors that the interceptions are occurring. Plaintiffs and Class members visited at least one such website and had their data intercepted without consent as a result.

[11] https://www.wunderkind.co/how-it-works/performance-marketing-solutions-for-ecommerce/#:~:text=Wunderkind's%20proprietary%20Identity%20Network%20recognizes,but%20streamlines%20execution%20across%20teams.

43. Moreover, Wunderkind designs its software to operate covertly and to overcome many of the privacy tools available to website visitors. Therefore, a consumer never knows whether any given website has Wunderkind's tracking software embedded and the entire data collection process takes place surreptitiously without the consumer's knowledge or consent.

F. Wunderkind Uses Consumer Data for Its Own Purposes

44. By the terms of the agreement between Wunderkind and clients, Wunderkind is specifically allowed to use the intercepted data for its own purposes. Wunderkind admits that it does so, stating that it uses the data "to help us improve our Websites and the products, Services, applications, content and features that we provide."[12]

45. Furthermore, Wunderkind admits that it "may use machine learning via data collected across Client Digital Properties to optimize ad and message timing and to use data to target ads and marketing messages to users inferred interests."[13] Wunderkind also admits that it trains the WunderkindAI on the data it intercepts from website visitors. That means Wunderkind may learn from the intercepted data to develop advertising and marketing strategies that it then sells to its clients.

FACTS SPECIFIC TO PLAINTIFFS

46. Each Plaintiff visited at least one website containing the Wunderkind tracker that did not prompt them to provide consent to Wunderkind's data tracking and interception.

47. Wunderkind collected Plaintiffs' behavioral data and their communications with the website operators, which included the products they viewed and purchased, the pages they viewed, form inputs, and how they behaved when on the websites. Defendant also collected other data from Plaintiffs, such as information about their browsers, persistent identifiers, IP addresses, and device fingerprint data to identify them.

48. Wunderkind's tracking software intercepted communications between Plaintiffs and the website operators while those communications were in transit. As data traveled between Plaintiffs' browsers and the website servers, Wunderkind's tracking software intercepted and read

[12] https://www.wunderkind.co/privacy/.
[13] *Id*.

these transmissions in real-time, capturing clicks and page visits as they happened, keystrokes and form entries as they were submitted, and navigation commands during transmission. Wunderkind read or attempted to read these communications by analyzing and interpreting the data streams mid-transmission, automatically identifying and classifying data types and values, extracting personal information, search queries, and behavioral data while the communications were still traveling to their intended destination.

49. Given the above, Wunderkind identified Plaintiffs, assigned them a PrivacyID, and created profiles containing their likes and interests, which Wunderkind continued to enrich as Plaintiffs used websites on which Wunderkind was installed.

50. Plaintiffs did not give Wunderkind consent to track or intercept their data. Plaintiffs also did not know or have any reason to know that Wunderkind was secretly and surreptitiously collecting their data and/or creating consumer profiles for them that were used to target marketing at them.

CLASS ACTION ALLEGATIONS

51. **Class Definition**: Plaintiffs bring this proposed class action pursuant to California Code of Civil Procedure § 382 on behalf of themselves and a Class of others similarly situated, defined as follows:

> All California residents who visited a website with Wunderkind's software embedded during the applicable statute of limitations period and had their data captured by Wunderkind without providing informed consent.
>
> Excluded from the Class are Defendant and its officers, directors or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir or assign of Defendant. Also excluded from the Class are any attorneys appearing in this matter, any federal, state or local governmental entities, any judicial officer presiding over this action and the members of his or her immediate family and judicial staff, and any juror assigned to this action.

52. The Class Period is the full extent of the applicable limitations period, including any tolling or other equitable considerations that extend the limitations period.

53. **Class Identity/Ascertainability:** The Class is readily identifiable and is one for which records should exist. Wunderkind has records of those the websites with its software embedded and of the parties whose data was captured.

54. **Numerosity**: The exact number of Class Members is unknown and not available to Plaintiffs at this time. However, given the scale and scope of Defendant's data collection practices, it is clear that there are hundreds of thousands or millions of California residents who are members of the Class.

55. **Typicality**: Plaintiffs' claims are typical of the claims of Class Members because Plaintiffs and Class Members have had their personal information and communications with website operators intercepted by Defendant without consent and using the same tracking technologies.

56. **Commonality**: There are many questions of law and fact common to the claims of Plaintiffs and the Class, including:

A. Whether Defendant read, attempted to read, or learned the content of the communications intercepted by its tracking technology;

B. Whether Defendant intercepted the communications while in violation of § 631 of CIPA;

C. Whether Defendant's data interception was willful;

D. Whether Defendant used the intercepted data;

E. Whether Defendant's data collection practices constitute a business practice as the term is used in the UCL;

F. Whether Defendant's data collection practices constitute unfair or unlawful business practices, as those terms are used in the UCL;

G. Whether Defendant's data collection practices constitute a breach of social norms, as those terms are used in Section 1 of the California Constitution.

57. **Predominance:** The above-listed questions of law and fact are common to the Class and will predominate over questions that may affect individual Class Members.

58. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class because Plaintiffs' interests are aligned with, and not antagonistic to, those of the other members of the Class and Plaintiffs have retained counsel competent and experienced in the prosecution of class actions and complex data privacy cases to represent them and the Class.

59. **Superiority and manageability**: A Class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. The individual prosecution of separate actions by individuals would lead to repetitive adjudication of common questions and fact and law and create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant. There will be no difficulty in the management of this action as a Class action.

FIRST CAUSE OF ACTION
Violation of Cal. Penal Code § 631
(On behalf of Plaintiffs and the Class)

60. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

61. Wunderkind, "by means of any machine, instrument, contrivance, or in any other manner," has "willfully and without the consent of all parties to the communications, or in any unauthorized manner, read[] or attempt[ed] to read or learn the contents or meaning of any message, report, or communication while the same is in transit or being sent from or received at any place within this state." Cal. Penal Code § 631(a). Wunderkind has also "use[d], or attempt[ed] to use, in any manner, or for any purpose, or to communicate in any, any information so obtained." *Id.*

62. Defendant's software is a "machine, instrument, contrivance . . ." used to track and intercept data from website visitors.

63. Defendant read, attempted to read, or otherwise learned the content of the communications between Plaintiffs/Class members and website operators, which included information about the web pages Plaintiffs and the Class viewed, items they placed inside their shopping carts, and behavioral data like how they scrolled on a website. As such, the data intercepted by Wunderkind is "content" under § 631 of CIPA.

64. Information such as email addresses, phone numbers, IP addresses, and form inputs that Plaintiffs and the Class input into the websites is also "content" under § 631 of CIPA.

65. Furthermore, Defendant read, attempted to read, and/or learned the contents of communications sent from or received within the State of California in real time. Plaintiffs and the Class intended their transmissions to be private communications between them and the business website, and not an unknown third party.

66. Defendant did not act as a mere extension of the website visited by Plaintiffs and the Class because it used the communications for its own purposes. Defendant used or (in the alternative) has the capability to use the data it intercepted to develop and/or improve its own products and services.

67. Defendant never obtained any consent whatsoever from Plaintiffs and the Class.

68. Plaintiffs and the Class seek an injunction and statutory damages in the amount of $5,000 per violation pursuant to Cal. Pen. Code § 637.2.

SECOND CAUSE OF ACTION
Violation of Cal. Penal Code § 638.51
(On behalf of Plaintiffs and the Class)

69. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

70. California law prohibits the installation of a pen register without first obtaining a court order. Cal. Penal Code § 638.51.

71. The statute defines a "pen register" as "a 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, but not the contents of a communication." Cal. Penal Code § 638.50(b).

72. Defendant's software is a "pen register" because it is a device or process that records addressing or signaling information—in this instance, Plaintiffs' and Class Members' identifying information device fingerprint data, IP addresses, and other persistent identifiers—from electronic communications transmitted by their devices. Furthermore, Defendant's software is a device or process that identifies consumers, gathers data, and correlates data through sophisticated device fingerprinting and its consumer identification functionality.

73. Defendant was not authorized by any court order to use a pen register to track Plaintiffs' and Class Members' location and personal information, nor did it obtain consent from Plaintiffs and the Class to operate such a device.

74. Plaintiffs and the Class seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

THIRD CAUSE OF ACTION
Violation of the California Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
(On behalf of Plaintiffs and the Class)

75. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

76. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act ("CDAFA") to "expand the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). In enacting the statute, the Legislature emphasized the need to protect individual privacy: "The Legislature further finds and declares 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." *Id*.

77. Plaintiffs' and Class Members' devices are "computers" or "computer systems" within the meaning of § 502(b) because they are devices capable of being used in conjunction with external files and perform functions such as logic, arithmetic, data storage and retrieval, and communication.

78. Defendant violated the following sections of CDAFA § 502(c):

79. "Knowingly accesses and without permission... uses any data, computer, computer system, or computer network in order to... wrongfully control or obtain money, property, or data." *Id*. § 502(c)(1).

80. "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." *Id*. § 502(c)(2).

81. "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." *Id*. § 502(c)(7).

82. Defendant knowingly "accessed" Plaintiffs' and the Class Members' computers and/or computer systems because it purposefully gained entry to and/or caused output from their computers to obtain personal information, which includes the data Wunderkind intercepted.

83. Plaintiffs and the Class suffered damage and/or loss resulting from Defendant's conduct described herein. Specifically: (1) Defendant's software occupied Plaintiffs' and the Class's storage space on their devices without authorization; (2) Defendant's software caused data to be output from Plaintiffs' and the Class's devices; (3) Defendant's acts used computer resources of the device; and (4) Defendant was unjustly enriched and profited from the data taken from Plaintiffs and the Class.

84. Plaintiffs and the Class now seek compensatory damages, injunctive relief, disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to § 502(e)(1)–(2).

FOURTH CAUSE OF ACTION
Invasion of Privacy
Violation of Art. 1, § 1 of the California Constitution
(On behalf of Plaintiffs and the Class)

85. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

86. "Privacy" is listed in Article I, Section 1, of the California Constitution as a fundamental right of all Californians. That section of the Constitution provides as follows: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

87. The right to privacy in California's Constitution creates a right of action against private entities such as Defendant. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

88. Plaintiffs and Class Members have a legally protected privacy interest in their IP addresses, location data, browsing data, product selections, form inputs, and other routing

information that Wunderkind captures without notice or consent when they access and view websites implementing Wunderkind's Tracking Software. These privacy interests are recognized by the California Constitution, CDAFA, and CIPA.

89. Plaintiffs and Class Members had a reasonable expectation of privacy concerning this data when navigating the internet. Wunderkind is a third-party data broker with whom Plaintiffs and Class Members have no direct relationship, which Wunderkind and its client-websites use to collect Plaintiffs' and Class Members' IP addresses, location data, device information, and other routing information across multiple unrelated websites. Wunderkind also uses this information to build comprehensive profiles of their online activities.

90. The identifiable and private information Wunderkind intercepted, stored, and used without Plaintiffs' and Class Members' consent was used to track them consistently and persistently across multiple websites and to serve targeted advertisements. The manner in which Wunderkind intercepted this information deliberately circumvented established privacy-protection mechanisms and violated social norms.

91. Defendant's conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person because: (i) the information collected by Wunderkind is personally identifying information protected by the California Constitution and numerous statutes; (ii) Wunderkind deliberately designed its Tracking Software to circumvent privacy protections such as Safari's tracking prevention and Chrome's Incognito mode; (iii) Wunderkind's "identity resolution" technology creates comprehensive profiles of users by linking their activities across multiple unrelated websites and across multiple devices; (iv) Defendant did not have authorization or consent to collect users' IP addresses and other routing information; and (v) this invasion deprived Plaintiffs and Class Members of the ability to control the dissemination and use of their personal information, an ability that is a fundamental privacy right.

92. Reasonable individuals do not expect that there is an entity intercepting and monitoring their personally identifiable online activity across multiple websites, let alone using this information for profit through its identity resolution and behavioral targeting services.

93. Defendant's conduct violated the privacy of hundreds of thousands (if not millions) of Class Members, including Plaintiffs. Defendant did not have consent to intercept this information, let alone use and monetize it.

94. As a direct and proximate result of Defendant's actions, Plaintiffs and Class Members have had their privacy invaded and have sustained injury, including injury to their peace of mind and the loss of control over their personal information.

95. Plaintiffs and Class Members seek appropriate relief for those injuries, including but not limited to restitution, disgorgement of profits earned by Defendant because of, by way of or in connection with the intrusions upon Plaintiffs' and Class Members' privacy, nominal damages, and all other equitable relief that will compensate Plaintiffs and Class Members properly for the harm to their privacy interests.

96. Plaintiffs also seek such other relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION
Violation of the Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiffs and the Class)

97. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

98. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

99. Defendant engaged in unlawful business practices in connection with their unauthorized collection of Plaintiffs' and Class Members' private information, in violation of the UCL.

100. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

101. Defendant violated the "unlawful" prong of the UCL by violating, inter alia, Plaintiffs' and Class Members' constitutional rights to privacy, state privacy statutes, and state consumer protection statutes.

102. Defendant's acts, omissions, and conduct also violate the "unfair" prong of the UCL because those acts, omissions, and conduct, as alleged therein, offended public policy (including state privacy statutes and state consumer protection statutes) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Class Members.

103. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein.

104. As result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, including but not limited to valuable consideration, e.g., access to their private and personal data. Plaintiffs' and Class Members' personal data, including web browsing and device data and personally identifying and addressing information has monetary value. Defendant deprived Plaintiffs and Class Members of that valuable data without providing just compensation. Plaintiffs and Class Members would not have used certain websites had they known Defendant was disclosing their personally identifying and addressing information to third parties through those sites.

105. UCL § 17203 provides that the Court may restore to any person in interest any money or property which may have been acquired by means of unfair, deceptive, and fraudulent business acts and practices and may order restitution to Plaintiffs. Plaintiffs and Class Members are entitled under UCL §§ 17203 and 17208 to restitution and restoration of all ill-gotten money and property belonging to Plaintiffs and Class Members in Defendant's possession.

106. As a result of Defendant's violations of the UCL, Plaintiffs and Class Members are further entitled to injunctive relief enjoining Defendant's unlawful and unfair business activities and practices, including an injunction terminating all further distributions of Plaintiffs' and Class Members' personal data. This is particularly true since the dissemination of Plaintiffs' and Class Members' information is ongoing.

107. Plaintiffs additionally seek any and all other equitable relief that the Court deems just and proper.

SIXTH CAUSE OF ACTION
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiffs and the Class)

108. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

109. To state a claim for intrusion upon seclusion, Plaintiffs must establish that: (1) the defendant intruded on a place, conversation, or matter in which Plaintiffs had a reasonable expectation of privacy; and (2) the intrusion would be highly offensive to a reasonable person.

110. Defendant's collection, interception, and use of Plaintiffs' and Class Members' personally identifiable information, including IP addresses, location information, and device identifiers constitutes an intentional intrusion. Wunderkind's use of this information to create detailed profiles of individuals through its "identity resolution network," which tracks and profiles Plaintiffs and Class Members across multiple unrelated websites, likewise constitutes an intentional intrusion.

111. Plaintiffs and Class Members reasonably expected that their IP addresses, location data, and other personal information would not be intercepted, collected, and used by Wunderkind—a third-party data broker with whom they have no direct relationship.

112. This expectation is particularly reasonable given that Wunderkind operates entirely behind the scenes, with no visible interface for users, no direct services provided to users, and no opportunity for users to review or consent to Wunderkind's privacy practices.

113. The information Wunderkind collects is especially sensitive because it includes IP addresses (which reveal users' geographic locations) and is used to create comprehensive profiles tracking users' activities across multiple unrelated websites.

114. Plaintiffs and Class Members did not consent to, authorize, or understand Wunderkind's interception or use of their private data.

115. Defendant's conduct is highly offensive to a reasonable person because: (a) it violates established social norms and expectations regarding online privacy; (b) it circumvents standard privacy protection measures, continuing to function even when users take affirmative steps to protect their privacy through traditional tracking prevention features; (c) it occurs without users' knowledge or consent and provides no opportunity for users to opt out; (d) it creates comprehensive

profiles of users' online activities across multiple unrelated websites and across devices through Wunderkind's identity resolution technology; and (e) it monetizes users' personal information for Defendant's commercial gain without their knowledge or compensation.

116. Defendant's intrusion is particularly egregious because it deliberately undermines users' attempts to protect their privacy. As demonstrated in Wunderkind's own documentation, its Tracking Software continues to function even when users employ privacy-focused browsers or browsing modes, revealing Wunderkind's intent to surveille users regardless of their expressed privacy preferences.

117. Defendant's conduct caused Plaintiffs and Class Members harm, including a violation of their privacy interests, loss of control over their personal information, and emotional distress from the knowledge that their online activities have been secretly monitored and profiled.

118. Plaintiffs and Class Members seek damages to compensate for the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Defendant as a result of its intrusion upon seclusion.

119. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

120. Plaintiffs and Class Members also seek any other relief the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Daniel Wine, Allison Blank, Sandra Sion, and Kevin Smith individually and on behalf of the Class, pray for the following relief:

(a) An order certifying the Class as defined above, appointing Daniel Wine, Allison Blank, Sandra Sion, and Kevin Smith as the representatives of the Class, and appointing their counsel as Class Counsel;

(b) An order declaring that Defendant's actions, as set out above, violate Cal. Pen. Code § 631(a), Cal. Pen. Code § 638.51, Cal. Pen. Code § 502, Art. 1, § 1 of the California Constitution,

and Cal. Business & Professional Code § 17200, and constitute a common law invasion of privacy;

(c) An injunction requiring Defendant to cease all unlawful activities, including the use of its software on websites without obtaining consent from website visitors;

(d) An award of statutory damages, compensatory damages, disgorgement of profits, punitive damages, costs, and attorneys' fees;

(e) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully submitted,

MOGIN LAW LLP

Dated: September 26, 2025

By: */s/ Daniel J. Mogin*

Daniel J. Mogin (SBN No. 95624)
Timothy Z. LaComb (SBN No. 314244)
4225 Executive Square, Suite 600
La Jolla, CA 92037
Telephone: (619) 687-6611
Facsimile: (619) 687-6610
dmogin@moginlawllp.com
tlacomb@moginlawllp.com

JOSEPH SAVERI LAW FIRM, LLP
Joseph R. Saveri (SBN 130064)
Cadio Zirpoli (SBN 179108)
Kevin E. Rayhill (SBN 267496)
Holden Benon (SBN 325847)
601 California Street, Suite 1505
San Francisco, CA 94108
Tel (415) 500-6800
jsaveri@saverilawfirm.com
czirpoli@saverilawfirm.com
hbenon@saverilawfirm.com
krayhill@saverilawfirm.com

DON BIVENS PLLC
Don Bivens (*pro hac vice* forthcoming)
15169 N. Scottsdale Road, Suite 205

Scottsdale, AZ 85254
Telephone: (602) 762-2661
don@donbivens.com

Counsel for Plaintiffs and the Proposed Class