M. Anderson Berry, (SBN 262879)
Gregory Haroutunian (SBN 330263)
EMERY REDDY, PC
333 University Avenue, Suite 200
Sacramento, CA 95825
Telephone: (916) 823-6955
Fax: (206) 441-9711
anderson@emeryreddy.com
gregory@emeryreddy.com

Israel David *
Adam M. Harris*
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, New York 10004
Telephone: (212) 350-8850
israel.david@davidllc.com
adam.harris@davidllc.com

Mark A. Cianci *
ISRAEL DAVID LLC
399 Boylston Street, Floor 6, Suite 23
Boston, Massachusetts 02116
Telephone: (617) 295-7771
mark.cianci@davidllc.com

**Pro Hac Vice Forthcoming*

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALEXIS FENNESSY, BREU'ANA COLE, CATHERINE BROOKS, KELTIN GARNER, KEVIN FREDLEY, MELODIE MOSLEY, MICHAEL DOHERTY, and ROGER JOLLIS, on behalf of themselves and all others similarly situated,

Plaintiff,

v.

GOOGLE, LLC,

Defendant.

Case No. 5:26-cv-06534

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Alexis Fennessy, Breu'ana Cole, Catherine Brooks, Keltin Garner, Kevin Fredley, Melodie Mosley, Michael Doherty, and Roger Jollis, on behalf of themselves and all others similarly situated ("Plaintiffs"), by and through their undersigned attorneys, bring this class action complaint against Defendant Google LLC ("Google" or "Defendant"), and allege as follows based upon personal knowledge as to themselves and their own actions, and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This action challenges Google's systematic collection, storage, and commercial use of the facial-recognition data of people who did not consent to having their faces scanned. Google Nest security cameras and doorbells offer a "Familiar Face Detection" feature that uses artificial intelligence to scan the face of every person who appears in the camera's field of view, to capture an image of that person's face, to create a mathematical template of the person's facial geometry (a "faceprint"), and to compare that faceprint against a library of stored profiles (a "familiar face library"). The feature is activated by the camera's owner. It is not activated by, and cannot be consented to by, the bystander whose face is being scanned.

2. Google knows this is unlawful. It has disabled Familiar Face Detection in Illinois, the only state with a hyper-specific biometric privacy statute allowing private citizens to sue for unconsented collection of facial-recognition data. In every other state, including states where regulators have taken enforcement actions against Google for this very conduct, Google has made the calculated decision to continue scanning bystanders' faces without consent and without disclosure.

3. Google designed the system to be invisible to its subjects. A Nest camera that has Familiar Face Detection enabled gives the people it scans no notice, no indicator, no opportunity to consent or decline, and no means of ever learning that their facial geometry has been captured, processed, and catalogued. The only parties who know which devices are scanning, and whose faces they have processed, are Google and, in part, the device owners Google equips.

4. Plaintiffs are residents of the Commonwealth of Virginia. They are not customers of Google Nest or Google Home products. In the ordinary course of their daily lives, Plaintiffs regularly walk through neighborhoods, visit homes, and conduct errands in areas where Google Nest doorbells and cameras are visibly installed at numerous homes and businesses. Familiar Face Detection is among Google's most heavily marketed camera features, and a substantial share of Nest camera households subscribe to Google Home Premium and enable the feature. It is highly likely that one or more of the Nest devices whose fields of view Plaintiffs have entered had Familiar Face Detection enabled, which is designed to scan every face that appears within a camera's field of view, and Google's system captured images of their faces, created faceprints of their facial geometry, and processed and retained that biometric data in systems designed, operated, and controlled by Google, all without Plaintiffs' knowledge, consent, or compensation.

5. Plaintiffs cannot identify which devices scanned them or on which occasions with certainty because Google built the system to make that information virtually impossible for Plaintiffs to obtain. Google, by contrast, can determine whether and where images of Plaintiffs' faces have been captured and stored: the very faceprint-matching technology at issue allows Google to identify every familiar face library in which Plaintiffs' facial geometry appears. Those records are in Google's possession.

6. Plaintiffs bring this action on behalf of a nationwide class and a Virginia subclass of persons whose facial-recognition data was collected, stored, and used by Google's Familiar Face Detection feature without their consent, seeking damages, injunctive relief, and all other relief this Court deems just and proper.

PARTIES

7. Plaintiffs Alexis Fennessy, Breu'ana Cole, Catherine Brooks, Keltin Garner, Kevin Fredley, Melodie Mosley, Michael Doherty, and Roger Jollis are natural persons and residents of Virginia. Plaintiffs regularly walk through residential neighborhoods, visit the homes of friends and family, and patronize local businesses throughout Virginia. There are numerous residences and

businesses along Plaintiffs' regular routes at which Google Nest doorbells or cameras are visibly installed.

8. It is highly likely that many of those Nest devices had Familiar Face Detection enabled during the limitations period. As to such devices, on each occasion on which Plaintiffs entered the field of view of such a device, Google's system captured an image of each Plaintiff's face, derived a faceprint from his or her facial geometry, and compared that faceprint against the familiar face library associated with the device owner's account. Because Plaintiffs repeatedly traverse the same routes, the same devices would have captured and processed their faces on multiple occasions, and Google's system — which is designed to be able to recognize returning faces — has the capability to associate their facial geometry across those encounters.

9. Plaintiffs did not consent in any form to Google's collection, creation, or storage of their facial-recognition data. Plaintiffs were never informed that their faces would be scanned, were never given any opportunity to opt in or opt out, and have no means of learning which devices scanned them or what Google has done with their biometric data. Google, by contrast, possesses records and technology sufficient to determine whether and where Plaintiffs' faceprints have been captured and stored.

10. Plaintiffs continue to live, walk, and visit residences in the same neighborhoods. Unless Google is enjoined, Plaintiffs face a substantial and imminent risk that Google will continue to capture and process their facial geometry — on a recurring basis — each time they pass a Nest device with Familiar Face Detection enabled.

11. Plaintiffs have never purchased, registered, or used any Google Nest product or service. They have never created a Google Home account or a Nest account. They have never agreed to any terms of service, arbitration provision, or class-action waiver governing Google Nest devices or services. They have no contractual or commercial relationship with Google concerning Nest devices, Google Home, or any home-security product or service.

12. Defendant Google LLC is a Delaware limited liability company with its principal

place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google designs, manufactures, markets, sells, and operates Nest-branded security cameras and doorbells, including the Familiar Face Detection feature. Google processes and manages facial-recognition data collected by Nest cameras through systems Google designs, operates, and controls. Google is the entity that designed, and profits from, the Familiar Face Detection feature at issue in this action.

JURISDICTION AND VENUE

13. This Court has subject-matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) the proposed classes contain more than 100 members; (b) minimal diversity exists between the parties, as Plaintiffs are citizens of Virginia and Defendant is a citizen of Delaware and California; and (c) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

14. This Court has personal jurisdiction over Google because Google is headquartered in this District, has its principal place of business in this District, and has purposefully directed its products, services, and the conduct at issue toward residents of this District and of every state in the United States.

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Google resides in this District and a substantial part of the events giving rise to the claims occurred here, including the design, development, operation, and management of the Familiar Face Detection feature and the data infrastructure that processes the facial-recognition data at issue. Pursuant to Civil Local Rule 3-2(c) and (e), this action is properly assigned to the San Jose Division because a substantial part of the events giving rise to the claims occurred in Santa Clara County, where Google maintains its principal place of business.

CHOICE OF LAW

16. California substantive law governs the claims of the Nationwide Class. Applying California law to the claims of all Nationwide Class members is appropriate and constitutional because the conduct at issue emanates from California. Familiar Face Detection was designed and

engineered at Google's headquarters in Mountain View, California. California law applies to the Nationwide Class because California has a paramount interest in regulating conduct by corporations headquartered and making decisions within its borders. The corporate decisions challenged here — to scan every face in a camera's field of view without the data subject's consent; to provide no notice, indicator, or opt-out opportunity to the people being scanned; to set the feature's data-retention and storage architecture; to disable the feature in Illinois while operating it everywhere else; and to market and monetize the feature through Google Home Premium subscriptions — were all made by Google personnel in California. In addition, the facial-recognition algorithms are maintained and updated in California, and the systems that process, organize, and "clean-up" the resulting biometric data are operated and controlled from California. Facial images captured by Google Nest products in all states, and biometric data derived from those facial images, are processed, organized, and cleaned up by Google's systems, which were designed and continue to be managed in California.

17. Virginia law governs the claims of the Virginia Subclass, whose members are Virginia residents whose facial-recognition data was captured by devices located in the Commonwealth of Virginia.

FACTUAL ALLEGATIONS

A. Google's Familiar Face Detection Feature

18. Google Nest-branded security cameras and doorbells are among the most widely deployed home-surveillance devices in the United States. They are sold through Google's online store and major retailers including Best Buy, Walmart, and Amazon, and are installed at millions of American homes and businesses.

19. As described above, Google offers a feature called "Familiar Face Detection" for its Nest cameras and doorbells. According to Google's own published support documentation, Familiar Face Detection "teach[es] your Google Nest camera to recognize faces of people that you know" and "notif[ies] you if it detects people it doesn't recognize." Familiar Face Detection exists precisely to identify and re-identify individuals — identification is the feature's sole purpose.

20. The reason Google heavily markets Familiar Face Detection is obvious: it requires a paid subscription to Google Home Premium (formerly Nest Aware), currently priced at $10 per month. When the device owner activates the feature, the Nest camera scans every face that appears in its field of view. The system captures an image of each face and, consistent with how facial-recognition technology generally operates, analyzes the geometric relationships between the person's facial features — such as the distance between the eyes, the shape of the cheekbones, the contour of the jawline, and other measurements unique to the individual — and creates a mathematical faceprint from those measurements. Google does not publicly disclose the precise technical operation of its facial-recognition algorithms. The faceprint is then compared against a library of stored facial profiles — the faces the device owner has labeled with associated names — maintained in connection with the account holder's Google Home account.

21. This process — capturing a facial image, creating a faceprint, and comparing it against stored profiles — occurs for every person in the U.S. (other than in Illinois) whose face appears in the camera's field of view, without exception. That is how the system was designed. Google's own documentation confirms: "Whenever your camera detects a face, the activity is marked in your camera's recorded video." When the system detects an "unfamiliar face," the app asks the device owner "whether it's someone you know." This confirms that the initial face capture, facial-geometry analysis, and faceprint creation occur before any user labeling — and occur regardless of whether the person is known to the device owner.

22. Google's system also uses "additional non-biometric signals (body size, clothing color, etc.)" to enhance facial recognition, demonstrating that the biometric processing extends beyond the face itself to build a broader profile of each detected person.

23. Nest cameras in the same home share the same familiar face library, meaning that facial-recognition data collected by one camera is accessible to, and used by, every other camera linked to the same account. This expands the scope of biometric surveillance across multiple entry points within a single home.

24. Google's storage of facial-recognition data varies by camera model. According to Google's own documentation, earlier Nest camera and doorbell models, set up in the Nest app, store familiar face data in Google's cloud. Newer models, set up in the Google Home app, store familiar face data in the device's internal memory, but Google's cloud remains involved in the data lifecycle: Google's documentation states that "the cloud is used for clean-up" of familiar face data on these models. In both configurations, the facial-recognition data is created, processed, and stored by Google's software and algorithms; the familiar face library is shared across all cameras in the same home; and the data remains within Google's possession, custody, or control.

25. Upon information and belief, Google does not publicly disclose the retention period for facial-recognition data of persons not labeled by the device owner. Google's Familiar Face Detection documentation does not specify an automatic deletion period for "unfamiliar" face data, unlike some competitors that impose 30-day automatic deletion for unnamed faces. Rather, Google retains unlabeled faceprints for an indefinite or undisclosed period sufficient to enable the system to detect and match repeat visitors across multiple visits.

26. Google's system indiscriminately scans the face of every person who appears in the camera's field of view, including the faces of minors. Google has no mechanism to identify, segregate, or protect the facial-recognition data of children, and does not obtain parental consent before scanning the faces of minors or creating faceprints from their facial geometry.

27. Familiar Face Detection is not a niche or obscure setting. To the contrary, Google promotes the feature prominently in its product pages, advertisements, and retail packaging. A substantial share of Nest camera households subscribes to Google Home Premium, and a substantial share of those subscribers enable Familiar Face Detection — a rate Google tracks internally and does not disclose. The consequence is that an ordinary person moving through an American residential neighborhood today may pass through the fields of view of multiple Nest devices, a meaningful portion of which are scanning, and creating faceprints of, every face that appears.

///

B. Google's Knowledge That This Conduct Violates Privacy Rights

28. Google has long known that the unconsented collection of facial-recognition data from bystanders violates biometric privacy rights. Google has taken steps to comply with biometric privacy laws where the risk of private enforcement is highest and has deliberately chosen not to comply everywhere else.

29. In particular, Google has disabled Familiar Face Detection for cameras based in Illinois, citing "state regulatory restrictions." Google's own support documentation states that "[f]amiliar face detection is not available for cameras based in Illinois…." Illinois is the only state with a biometric privacy statute — the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 et seq. — that provides a private right of action allowing individuals to sue for violations. Google does not disable the feature in any other state. However, Google does publicly recognize the possibility that Familiar Face Detection violates privacy laws in other jurisdictions, by instructing camera owners: "Before you save any of your camera's face data, check your local privacy laws."

30. Google also restricts certain features of Google Photos (another Google product) that rely on face-grouping technology in both Illinois and Texas, demonstrating that Google is technically capable of implementing geographic restrictions for biometric features when it chooses to do so. Yet Google has chosen to restrict Nest's Familiar Face Detection only in Illinois — the one state where private individuals can most easily sue — and nowhere else.

31. Google's selective compliance with privacy law is underscored by history. In May 2025, Google agreed to pay $1.375 billion to the Texas Attorney General to settle claims that Google's products, including Nest cameras, captured Texans' biometric data without consent. Nevertheless, Google continues to operate Familiar Face Detection. The feature remains available in Texas and in every other state except Illinois. Google has not modified the feature to obtain consent from bystanders, has not implemented any mechanism for bystanders to opt out, and has not disclosed to bystanders that their facial-recognition data is being collected.

///

32. Google's decision to disable Familiar Face Detection only where it faces private enforcement risk — while continuing to scan bystanders in states where individuals cannot readily sue under a hyper-specific statute — demonstrates a knowing, deliberate business decision to collect bystanders' facial-recognition data wherever Google calculates that the risk is manageable. This knowing conduct is directly relevant to the punitive-damages standard under Va. Code § 8.01-40 and to the offensiveness of the intrusion under California law.

C. The Sensitivity and Immutability of Biometric Data

33. Facial-recognition data is among the most sensitive categories of personal information because it is immutable. Unlike a password, credit card number, or address, a person's facial geometry cannot be changed. Once captured, a biometric faceprint can be used to track, identify, and surveil an individual for the rest of his or her life. If compromised through a data breach, the individual has no ability to "change the locks.

34. Facial-recognition technology operates by analyzing the geometric relationships between a person's facial features and converting those measurements into a mathematical template. This template — the faceprint — is a unique biometric identifier tied to the individual's physical appearance. It is the facial equivalent of a fingerprint.

D. Google's Commercial Benefit

35. Familiar Face Detection is a core commercial feature of the Google Nest product line and a primary driver of Google Home Premium subscriptions at $10 per month per household. Google markets the feature as a key benefit in product pages, advertisements, and retail packaging.

36. The feature cannot function without scanning and processing the faces of all persons in the camera's field of view, including bystanders. To determine whether a face is "familiar," the system must first capture an image of every face, create a faceprint, and compare that faceprint against the stored library. Bystanders' facial data is not a byproduct of the feature — it is its essential input. Without scanning bystanders, the system cannot identify anyone.

37. Google derives substantial commercial benefit from the biometric data of Plaintiffs

and class members through: (a) recurring subscription revenue from Google Home Premium; (b) enhanced marketability and competitiveness of its Nest cameras and doorbells; and (c) the accumulation of facial-recognition data and algorithmic training that could be used to improve Google's broader artificial-intelligence capabilities. This commercial use of Plaintiffs' and class members' facial data without consent or compensation constitutes use "for the purposes of trade" within the meaning of Va. Code § 8.01-40, "for purposes of . . . selling, or soliciting purchases" within the meaning of Ca. Civ. Code § 3344, and an unfair and unlawful business practice under California law.

E. Harm to Plaintiffs and Class Members

38. Plaintiffs and class members have suffered concrete, particularized injuries as a result of Google's conduct. The nonconsensual creation and retention of a biometric faceprint from an individual's facial geometry is itself a concrete invasion of a legally protected privacy interest with a close historical analogue to traditionally recognized harms, including intrusion upon seclusion. The creation, retention, and exploitation by Google's system of an immutable biometric identifier without consent — an ongoing course of conduct — is not a mere procedural violation — it is a substantive invasion of the individual's private affairs that causes real, continuous harm. Specifically, Plaintiffs and class members have suffered:

a. The creation and retention of biometric faceprints from their facial geometry without consent, constituting an invasion of their substantive privacy interests in their own biometric identities;

b. The appropriation and commercial use of their facial images and derived faceprints — a form of personal property protected by law — without consent and without compensation;

c. The loss of control over immutable biometric identifiers now stored, processed, or cleaned up in systems that Google controls and thus potentially accessible to Google employees, contractors, third parties, and law enforcement;

d. The ongoing risk of harm from the collection and retention of permanent,

unchangeable biometric data, which, if compromised through a data breach or unauthorized access, cannot be revoked or reissued;

e. The substantial and imminent risk of repeated, ongoing capture and processing of their facial geometry each time they pass a Nest device with Familiar Face Detection enabled; and

f. Emotional distress from the knowledge that their facial-recognition data has been, and continues to be, collected, stored, and commercially exploited without their consent.

F. Google's Conduct Is Not Protected Speech or Immunized Conduct

39. Google's collection and commercial use of bystanders' facial-recognition data is commercial conduct undertaken for profit — not speech or expression protected by the First Amendment. The facial scanning at issue occurs at private residences and in residential neighborhoods and is performed by Google's proprietary hardware and software to generate revenue from a paid subscription service. The First Amendment does not immunize a corporation's nonconsensual extraction of biometric data from private individuals for commercial purposes.

40. Nor is Google's conduct immunized by Section 230 of the Communications Decency Act, 47 U.S.C. § 230. Section 230 provides immunity for platforms with respect to content created by third-party users. The facial-recognition data at issue — the captured images, the derived faceprints, and the stored facial profiles — is created by Google's own algorithms running on Google's own hardware, not by a third-party user. The device owner activates the feature, but Google's system autonomously captures the bystander's face and processes it. This is Google's own content and conduct, not third-party content entitled to Section 230 protection.

G. Google's Exclusive Possession of Key Evidence

41. Google possesses records and data essential to establishing the full scope of its Familiar Face Detection operations, including: (a) records identifying which Nest devices had Familiar Face Detection enabled, and when; (b) the images in device owners' familiar face libraries, including any images of Plaintiffs' faces; (c) internal documents identifying whether, and to what extent, Google accesses facial-recognition data and faceprints created from bystanders; (d) retention

periods, deletion logs, and data-lifecycle records for unfamiliar face data; (e) internal documents evaluating the legal risks of deploying Familiar Face Detection without bystander consent; (f) internal documents relating to the decision to disable the feature in Illinois but not in other states; (g) device sales, revenue, and subscriber data attributable to Google Home Premium and the Familiar Face Detection feature, including the rates at which camera owners subscribe and enable the feature; and (h) records and technical capability sufficient to confirm — through the very faceprint-matching technology at issue — that Plaintiffs' faces appear in the familiar face libraries associated with Nest devices, including the devices along Plaintiffs' regular routes. Plaintiffs cannot access this information without discovery. To the extent Plaintiffs' allegations are made upon information and belief, they are so made because the relevant facts are within Google's exclusive possession and control — a condition of Google's own design.

CLASS ACTION ALLEGATIONS

42. Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and, in the alternative, 23(c)(4), on behalf of the following classes:

Nationwide Class (Third through Eighth Causes of Action):

> All natural persons in the United States whose facial-recognition data was collected, created, stored, or used by Google's Familiar Face Detection feature on Nest cameras or doorbells without their written consent during the applicable limitations period.

Virginia Subclass (First and Second Causes of Action):

> All natural persons residing in the Commonwealth of Virginia whose facial-recognition data was collected, created, stored, or used by Google's Familiar Face Detection feature on Nest cameras or doorbells located in the Commonwealth of Virginia without their written consent during the applicable limitations period.

43. Excluded from the classes are: (a) any judge or magistrate presiding over this action and members of their immediate families; (b) Google, its officers, directors, employees, subsidiaries, and affiliates; and (c) counsel for the parties.

44. **Numerosity.** The classes are so numerous that joinder of all members is impracticable. Upon information and belief, Nest cameras with Familiar Face Detection enabled are installed at residences and businesses throughout the United States, and the feature scans the face of every person who appears in each camera's field of view. The Nationwide Class likely includes millions of persons, and the Virginia Subclass likely includes tens of thousands or more.

45. **Ascertainability.** Class membership is objectively ascertainable from Google's own records. Google's systems record which devices have Familiar Face Detection enabled and contain familiar face libraries generated by the feature, and Google's faceprint-matching technology is capable of determining whose facial geometry those libraries contain.

46. **Commonality and Predominance.** Common questions of law and fact predominate over any individual issues, including: (a) whether Google collected class members' facial-recognition data without consent; (b) whether the facial images captured by Google's cameras and the faceprints derived from them constitute "pictures" or "portraits" under Va. Code § 8.01-40 and "photographs" under Ca. Civ. Code § 3344; (c) whether Google's use of that data constitutes use "for the purposes of trade" under Va. Code § 8.01-40 and "for purposes of ... selling, or soliciting purchases" under Ca. Civ. Code § 3344; (d) whether Google acted "without authority" in examining class members' identifying information under the Virginia Computer Crimes Act; (e) whether Google's conduct constitutes an intrusion upon seclusion and a violation of the right to privacy guaranteed by Article I, Section 1 of the California Constitution; (f) whether Google's conduct constitutes an unlawful or unfair business practice under California Business and Professions Code § 17200; (g) whether Google was unjustly enriched; and (h) the appropriate measure of damages, restitution, and injunctive relief.

47. **Typicality.** Plaintiffs' claims are typical of the claims of the classes. Plaintiffs and all class members were subjected to the same conduct: Google's system captured images of their faces, created biometric faceprints, and processed and retained that data without their knowledge, consent, or compensation.

48. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the classes. Plaintiffs have retained counsel experienced in complex class-action and privacy litigation. Plaintiffs have no interests antagonistic to the classes.

49. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The damages suffered by individual class members are relatively small compared to the expense and burden of individual litigation against Google, making individual lawsuits impracticable. Because Google's system gives its subjects no notice that they have been scanned, virtually no class member could definitively discover — let alone individually litigate — his or her claim.

50. **Rule 23(b)(2).** Google has acted on grounds that apply generally to the classes — operating Familiar Face Detection identically as to every person who enters a camera's field of view — so that final injunctive and declaratory relief is appropriate respecting the classes as a whole. Every class member faces the same ongoing and future scanning to which any person in the field of view of an enabled device is subjected.

FIRST CAUSE OF ACTION
Violation of Virginia Code § 8.01-40
(Unauthorized Use of Name or Picture for Purposes of Trade)
(On Behalf of the Virginia Subclass)

51. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

52. Virginia Code § 8.01-40 provides that "[a]ny person whose name, portrait, or picture is used without having first obtained the written consent of such person . . . for advertising purposes or for the purposes of trade" may maintain a suit for injunctive relief and damages. If the defendant "knowingly used such person's name, portrait or picture in such manner as is forbidden," the jury may award punitive damages.

53. Google Nest cameras captured images of Plaintiffs' and Virginia Subclass members' faces — "pictures" within the plain meaning of the statute — and used those images to create biometric faceprints: mathematical representations of their facial geometry that constitute derived "portraits" uniquely identifying each individual.

54. Google used Plaintiffs' and Virginia Subclass members' facial images and faceprints "for the purposes of trade." The statute's prohibition on use "for advertising purposes" and use "for the purposes of trade" are separate, distinct concepts; Plaintiffs need not allege that Google used their likenesses in an advertisement. Google's use falls squarely within the trade-purpose prong: Familiar Face Detection is a paid commercial feature offered as part of the Google Home Premium subscription at $10 per month; Google markets the feature as a primary benefit of Nest cameras and doorbells; Google derives subscription revenue, product-enhancement value, and competitive advantage from the feature; and the facial images and faceprints of Plaintiffs and Virginia Subclass members are the essential inputs without which the feature cannot operate. Google's commercial exploitation of bystanders' facial-recognition data to power, and profit from, a paid subscription product constitutes use for the purposes of trade. Google's use of Plaintiffs' and Virginia Subclass members' facial data is not incidental to any lawful purpose, is not newsworthy, and does not concern any matter of public interest; it is commercial use, undertaken for profit. Familiar Face Detection cannot operate without scanning every face that appears, and Google markets and charges for the very capability that bystanders' facial data makes possible.

55. Google did not obtain Plaintiffs' or Virginia Subclass members' written consent before capturing images of their faces, creating faceprints from their facial geometry, or storing and using that data.

56. Google's conduct was knowing and intentional. Google designed Familiar Face Detection to scan every face in the camera's field of view, including non-consenting bystanders. Google disabled Familiar Face Detection in Illinois to avoid BIPA liability, demonstrating that it understood the legal risks, yet chose to continue scanning bystanders in Virginia and every other state where it determined that the private enforcement risk was manageable. This knowing conduct supports an award of punitive damages under § 8.01-40.

57. As a direct and proximate result of Google's violations, Plaintiffs and Virginia Subclass members have suffered damages, including the invasion of their privacy, the appropriation

of their biometric identities for commercial purposes, the loss of the value of their biometric data, and emotional distress. Plaintiffs and Virginia Subclass members are further entitled to punitive damages.

SECOND CAUSE OF ACTION
Violation of the Virginia Computer Crimes Act
Va. Code §§ 18.2-152.5, 18.2-152.12
(On Behalf of the Virginia Subclass)

58. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

59. Virginia Code § 18.2-152.5(A) makes it unlawful for any person to use "a computer or computer network" to "intentionally examine[] without authority any employment, salary, credit or any other financial or identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, relating to any other person." It is the unauthorized use of a computer or computer network to access the information that constitutes a violation of the Code — regardless of whether the information is subsequently used.

60. The "identifying information" protected by § 18.2-152.5 expressly includes, among the categories enumerated in § 18.2-186.3(C), "biometric data" and "fingerprints." The faceprints Google creates from class members' facial geometry are biometric data — and the facial equivalent of a fingerprint — and therefore constitute "identifying information" within the express terms of the statute. Because Google designed Familiar Face Detection for the sole purpose of identifying and re-identifying individuals, the faceprints Google creates serve to identify.

61. Google used a computer network — its Nest camera hardware, applications, data infrastructure, and facial-recognition algorithms — to intentionally access and examine Plaintiffs' and Virginia Subclass members' identifying information by capturing images of their faces and analyzing their facial geometry to create biometric faceprints to be compared with the faces in a familiar face library. Each Nest camera and doorbell is a "computer," and Google's integrated system of Nest devices, mobile applications, and cloud infrastructure is a "computer network," within the meaning of Va. Code § 18.2-152.2. This is true regardless of whether a particular camera model stores familiar face data in Google's cloud or in the device's internal memory: in both configurations,

Google's software performs the facial-geometry examination, Google's network synchronizes the shared familiar face library across the home's cameras, and Google's cloud performs "clean-up" of the familiar face data.

62. Google acted without the authority of Plaintiffs and class members. The authority required by the statute is the authority of the person whose identifying information is being examined — here, the bystander — not the authority of a third party such as the device owner. A device owner's decision to activate Familiar Face Detection authorizes Google to operate the camera on the owner's behalf; it does not authorize Google to collect and examine the biometric identifiers of every other person who comes into the camera's view. Plaintiffs and Virginia Subclass members did not authorize Google to scan their faces, create faceprints, or store or use their biometric data. Google did not obtain consent of any kind from them. And Google analyzes class members' biometric data at a time when it knows, or should know, that it is without authority to do so: Google's decision to disable the feature in Illinois, and its settlement of government claims that Google's products captured biometric data without consent, demonstrate that Google has long known it lacks the consent of the people its cameras scan.

63. The statutory exceptions do not apply. Google's collection of bystanders' biometric data is not reasonably needed to protect the security of any computer, computer service, or computer business, nor to facilitate diagnostics or repair, nor to determine whether a user is licensed or authorized to use software or a service. It exists to power a paid consumer convenience feature for Google's profit.

64. Virginia Code § 18.2-152.12 provides a civil action for any person "whose property or person is injured by reason of a violation" of the Virginia Computer Crimes Act. Google's unauthorized examination and appropriation of Plaintiffs' and Virginia Subclass members' facial-recognition data injured both their property and their persons: under Virginia law, a person holds a legally protected property interest in his or her name and likeness, which Google appropriated without consent or compensation; and Google's covert biometric surveillance invaded class

members' privacy and caused them distress — an injury to the person.

65. Plaintiffs and Virginia Subclass members seek compensatory damages, costs, and reasonable attorneys' fees pursuant to Va. Code § 18.2-152.12.

THIRD CAUSE OF ACTION
Intrusion Upon Seclusion — California Common Law
(On Behalf of the Nationwide Class)

66. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

67. Plaintiffs and Nationwide Class members possess a legally protected privacy interest in their facial geometry and biometric identifiers, and a reasonable expectation that private companies will not covertly capture, measure, and catalogue their faces as they approach private residences and move through residential neighborhoods. That expectation is objectively reasonable: Google provides no notice or indicator that scanning is occurring; no social norm puts a passerby on notice that a doorbell is generating a mathematical map of his or her face; and Google's own conduct — disabling the feature in Illinois and warning camera owners to "check your local privacy laws" — concedes the sensitivity of the data.

68. Google intentionally intruded upon that seclusion. Through Familiar Face Detection, Google's systems capture images of class members' faces, derive biometric faceprints, compare those faceprints against stored libraries, and retain the resulting data — all without the knowledge or consent of the people scanned. The intrusion is accomplished by conduct emanating from California, where Google designed and manages the feature and made every challenged decision.

69. The intrusion is highly offensive to a reasonable person. It is covert by design; it is indiscriminate, sweeping in every face, including those of children; it converts the approach to a private home — a context of trust and invitation — into an occasion for biometric harvesting; it is undertaken for profit; and it has continued unabated after Google paid $1.375 billion to resolve government claims arising from the same conduct. The degree and setting of the intrusion, as well as Google's motives, render it egregious.

70. As a direct and proximate result, Plaintiffs and Nationwide Class members suffered

harm, including the loss of control over their immutable biometric identifiers, the invasion of their private affairs, and emotional distress, and they are entitled to damages, including nominal and punitive damages, and injunctive relief.

FOURTH CAUSE OF ACTION
Invasion of Privacy — California Constitution, Article I, Section 1
(On Behalf of the Nationwide Class)

71. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

72. Article I, Section 1 of the California Constitution guarantees an inalienable right to privacy that protects against invasions by private actors, including the unauthorized collection and use of sensitive personal information.

73. Plaintiffs and Nationwide Class members possess a legally protected informational-privacy interest in their biometric identifiers, including their facial geometry. They held a reasonable expectation of privacy in that information under the circumstances: they were not notified that Nest devices would scan their faces, they did not consent, and they had no means of discovering the collection.

74. Google's conduct constitutes a serious invasion of that protected interest. Google's systems capture, measure, catalogue, and retain the immutable biometric identifiers of every person who enters an enabled camera's field of view — conduct sufficiently serious in its nature, scope, and actual impact to constitute an egregious breach of the social norms underlying the privacy right. The invasion is aggravated by its covert design, its inclusion of children, its commercial motive, and Google's demonstrated knowledge of its unlawfulness.

75. Google has no legitimate countervailing interest that justifies the invasion. Whatever interest device owners have in home security can be served — as Google itself demonstrates in Illinois — without the nonconsensual biometric processing of bystanders. As a direct and proximate result, Plaintiffs and Nationwide Class members suffered harm and are entitled to damages and injunctive relief.

///

FIFTH CAUSE OF ACTION
Violation of California Business and Professions Code § 17200 et seq.
(Unlawful and Unfair Business Practices)
(On Behalf of the Nationwide Class)

76. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

77. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 et seq., prohibits any unlawful or unfair business act or practice.

78. Google's conduct is unlawful because it violates the right to privacy guaranteed by Article I, Section 1 of the California Constitution and constitutes the tort of intrusion upon seclusion, as alleged above, and, as to Virginia Subclass members, violates Va. Code §§ 8.01-40 and 18.2-152.5.

79. Google's conduct is also unfair. It causes substantial injury — the nonconsensual taking of immutable biometric identifiers from millions of people — that consumers and bystanders cannot reasonably avoid, because Google provides no notice, indicator, or opt-out, and that is not outweighed by any countervailing benefit to consumers or competition. The conduct is immoral and unethical, and it offends the public policy of California as expressed in Article I, Section 1 of the California Constitution and in California's statutory protections for personal and biometric information.

80. Plaintiffs and Nationwide Class members lost money or property as a result of Google's practices: their biometric identifiers and the likenesses from which they are derived are property of value, which Google took, retained, and commercially exploited without compensation, diminishing class members' ownership and control of their own biometric property while unjustly enriching Google.

81. Plaintiffs and Nationwide Class members are entitled to restitution of the value of the biometric data Google took and to injunctive relief restraining the unlawful and unfair practices described herein.

///

///

SIXTH CAUSE OF ACTION
Commercial Misappropriation — California Common Law
(On Behalf of the Nationwide Class)

82. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

83. Google Nest cameras captured images of Plaintiffs' and Nationwide Class members' faces and used those images to create biometric faceprints — mathematical representations of their facial geometry — to operate the Familiar Face Detection feature. The faceprint is unique to the individual whose facial image was used to create the faceprint, and it serves to identify the individual.

84. Google appropriated Plaintiffs' and Nationwide Class members' facial images and derived faceprints to Google's advantage. Familiar Face Detection is a paid commercial feature offered as part of Google's Google Home Premium subscription at $10 per month; Google markets the feature as a primary benefit of Nest cameras and doorbells; Google derives subscription revenue, product-enhancement value, and competitive advantage from the feature; and the facial images and derived faceprints of Plaintiffs and Nationwide class members are not incidental but are the essential input without which the feature cannot operate. Google commercially exploits bystanders' facial-recognition data to power, and profit from, a paid subscription product; the facial images and faceprints are the operative inputs that Google Nest cameras and doorbells enabled with Familiar Face Detection process and store. Familiar Face Detection cannot operate without scanning every face that appears, and Google markets and charges for the very capability that bystanders' facial data makes possible.

85. Google did not obtain Plaintiffs' or Nationwide Class members' written consent before capturing images of their faces, creating faceprints from their facial geometry, or storing and using that data. Plaintiffs and Nationwide Class members did not impliedly consent merely by walking in, visiting, and/or conducting errands in neighborhoods with no notice that cameras and doorbells were capturing their facial images and generating mathematical maps of their faces.

///

///

///

86. As a direct and proximate result of Google's violations, Plaintiffs and Nationwide Class members have suffered damages, including the invasion of their privacy, the appropriation of their facial images and biometric identities for commercial purposes, the loss of the value of their biometric data, and emotional distress.

SEVENTH CAUSE OF ACTION
Violation of California Right of Publicity
Ca. Civ. Code § 3344
(On Behalf of the Nationwide Class)

87. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

88. California Civil Code § 3344 provides that "[a]ny person who knowingly uses another's . . . photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of . . . selling, or soliciting purchases of, products, merchandise, goods, or services, without that person's prior consent . . . shall be liable to the injured party or parties in an amount equal to the greater of seven hundred fifty dollars ($750) or the actual damages suffered by them as a result of the unauthorized use, and any profits from the unauthorized use that are attributable to the use and are not taken into account in computing the actual damages," as well as for attorney's fees and costs. The injured party may seek an injunction or temporary restraining order.

89. Google Nest cameras captured images of Plaintiffs' and Nationwide Class members' faces — "photograph[s]" within the plain meaning of the statute — and used those images to create biometric faceprints — mathematical representations of their facial geometry — to operate the Familiar Face Detection feature. These photographs are readily identifiable as photographs of Plaintiffs' and Nationwide Class members by anyone viewing the photographs with the naked eye.

90. Google used Plaintiffs' and Nationwide Class members' facial images "for purposes of . . . selling, or soliciting purchases of, products, merchandise, goods or services" — namely, Google Nest cameras and doorbells and Google Home Premium subscriptions. Familiar Face Detection is a paid commercial feature offered as part of the Google Home Premium subscription at $10 per month; Google markets the feature as a primary benefit of Nest cameras and doorbells; Google derives subscription revenue, product-enhancement value, and competitive advantage from

the feature; and the facial images and derived faceprints of Plaintiffs and Nationwide Class members are not incidental but are the essential inputs without which the feature cannot operate. Google's commercial exploitation of bystanders' facial-recognition data to power, and profit from, a paid subscription product constitutes use for the purposes of selling or soliciting purchases. Familiar Face Detection operates only by scanning every face that appears, and Google markets and charges for the very capability that bystanders' facial data makes possible.

91. Google did not obtain Plaintiffs' or Nationwide Class members' written consent before capturing images of their faces, creating faceprints from their facial geometry, or storing and using that data. Plaintiffs and Nationwide Class members did not impliedly consent merely by walking in, visiting, and/or conducting errands in neighborhoods with no notice that cameras and doorbells were capturing their facial images and generating mathematical maps of their faces.

92. Google's conduct was knowing and intentional. Google designed Familiar Face Detection deliberately to capture and process the image of every individual who appears in the camera's field of view. The intentional design and operation of a paid commercial feature whose entire function is to capture and process individuals' faces constitutes knowing commercial use of Plaintiffs' and Nationwide Class members' photographs. The purpose of Familiar Face Detection is precisely to single out and identify specific individuals and Google markets the feature around its ability to do so. Google promotes the feature prominently in its product pages, advertisements, and retail packaging.

93. The statutory exceptions do not apply. Google's use of Plaintiffs' facial images and faceprints is not in connection with any news, public affairs, or sports broadcast or account, or any political campaign; the material containing the use neither is commercially sponsored nor contains paid advertising; and this action is not brought against the owners or employees of a medium used for advertising.

94. As a direct and proximate result of Google's violations, Plaintiffs and Nationwide Class members have suffered damages, including the invasion of their privacy, the appropriation of

their facial images and biometric identities for commercial purposes, and emotional distress. Plaintiffs and Nationwide Class members are further entitled to profits from the unauthorized use that are attributable to the use and are not taken into account in computing the actual damages, as well as attorney's fees and costs.

EIGHTH CAUSE OF ACTION
Unjust Enrichment / Quasi-Contract
(On Behalf of the Nationwide Class, Under California Law or, in the Alternative, the Materially Similar Laws of the Class Members' Home States)

95. Plaintiffs re-allege and incorporate by reference all preceding paragraphs.

96. Google received a benefit from Plaintiffs and Nationwide Class members in the form of the enhanced marketability of, and revenue from, Google Nest products and Google Home Premium subscriptions — both of which are dependent on Plaintiffs' and Nationwide Class members' highly valuable facial-recognition data, which Google collected, processed, and retained without authorization and without compensation.

97. Google used Plaintiffs' and Nationwide Class members' biometric data to operate and improve Familiar Face Detection, a paid commercial feature that generates subscription revenue and increases the market value and competitiveness of Google Nest products. The faceprints of Plaintiffs and Nationwide Class members are essential inputs to the commercial operation of this feature — the feature cannot function without scanning and processing the faces of all persons in the camera's field of view, including bystanders.

98. Google knew of the benefit conferred by Nationwide Class members' biometric data and should reasonably have expected to compensate them for its use. Google's retention of this benefit without payment is unjust. The core equitable principle — that Google should not be permitted to profit from biometric data taken from millions of Americans without their knowledge, consent, or compensation — does not vary in any material respect among the states.

99. Plaintiffs and Nationwide Class members seek restitution and disgorgement of all profits, benefits, and other compensation unjustly obtained by Google through its unauthorized collection and use of their facial-recognition data.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed classes, respectfully request that this Court enter judgment against Defendant and grant the following relief:

A. An order certifying the Nationwide Class and the Virginia Subclass and appointing Plaintiffs as class representatives and their counsel as class counsel;

B. A declaration that Google's conduct as alleged herein is unlawful;

C. Injunctive relief requiring Google to: (i) cease collecting facial-recognition data from class members without their prior informed, written consent; (ii) delete all facial-recognition data of class members collected without consent; (iii) implement visible indicators on Nest devices when Familiar Face Detection is active, to provide notice to bystanders; (iv) implement automatic deletion of all facial-recognition data for persons not affirmatively labeled by the device owner within thirty (30) days of collection; and (v) submit to periodic independent auditing of its biometric data collection, retention, and deletion practices;

D. Compensatory damages for all injuries suffered by Plaintiffs and class members;

E. Punitive damages based on Google's knowing and intentional conduct;

F. Restitution and disgorgement of all profits and benefits unjustly obtained by Google through its unauthorized collection and use of class members' facial-recognition data;

G. Pre-judgment and post-judgment interest;

H. Reasonable attorneys' fees, costs, and expenses as provided by law, including under Va. Code § 18.2-152.12 and Cal. Civ. Proc. Code §§ 1021.5 and 1033.5; and

I. Such other and further relief as this Court deems just and proper.

JURY TRIAL DEMANDED

100. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

///

///

DATED: June 29, 2026

Respectfully submitted,

By: _____

M. Anderson Berry, (SBN 262879)
Gregory Haroutunian (SBN 330263)
EMERY REDDY, PC
333 University Avenue, Suite 200
Sacramento, CA 95825
Telephone: (916) 823-6955
Fax: (206) 441-9711
anderson@emeryreddy.com
gregory@emeryreddy.com

Israel David (*pro hac vice* forthcoming)
Adam M. Harris (*pro hac vice* forthcoming)
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, New York 10004
Telephone: (212) 350-8850
israel.david@davidllc.com
adam.harris@davidllc.com

Mark A. Cianci (*pro hac vice* forthcoming)
ISRAEL DAVID LLC
399 Boylston Street, Floor 6, Suite 23
Boston, Massachusetts 02116
Telephone: (617) 295-7771
mark.cianci@davidllc.com

Attorneys for Plaintiffs and the Proposed Class