Lori G. Feldman (WSBA 29096)
lfeldman@hechtpartners.com
David L. Hecht (N.Y. Bar 4695961)
(*pro hac vice* forthcoming)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Telephone: (212) 851-6821

Lina Kaisey (SBN 314322)
(*pro hac vice* forthcoming)
lina@kaiseylaw.com
KAISEY LAW P.C.
100 Wilshire Boulevard, Suite 700
Santa Monica, California 90403
Telephone: (858) 774-0819

Blake Hunter Yagman (N.Y. Bar 5644166)
(*pro hac vice* forthcoming)
blake.yagman@yagmanpllc.com
YAGMAN PLLC
118-35 Queens Boulevard, Suite 444
New York, New York 11375
Telephone: (929) 709-1493

Counsel for Plaintiff Charles Sigwalt and the Proposed Classes and Subclasses.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

CHARLES SIGWALT, *on behalf of himself and all others similarly situated*,

Plaintiff,

v.

AMAZON.COM, INC. and RING LLC,

Defendants.

Case No. 26-cv-1887

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff, CHARLES SIGWALT ("Plaintiff"), brings this class action complaint (the "Action") on behalf of himself and others similarly situated for violations of state and common laws against Defendants, AMAZON.COM INC. ("Amazon") and RING LLC ("Ring" collectively, the "Defendant"), upon personal knowledge as to himself and his own actions, information and belief, and the investigation of his counsel, seeking actual damages, statutory damages, restitution, disgorgement of profits into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys' fees, a declaratory judgment, injunctive relief, and any other relief this Court deems just and proper, as follows:

NATURE OF THE ACTION

1. Plaintiff and Class members had their privacy rights violated when they, along with millions of other Americans, passed by a Ring security camera and unknowingly had their facial recognition information collected by Defendant as part of Defendant's new 'Familiar Faces' Ring security camera feature (the "Class").

2. Beginning as late as December of 2025 (and April of 2026 in the United Kingdom), Ring, which is owned by Amazon, launched the Familiar Faces feature for its security cameras in the United States.[1][2] Specifically, Familiar Faces uses facial recognition technology to scan the face of all guests and passersby before categorizing who they are using artificial intelligence ("AI").[3] AI then collects a "face print" of the respective person and translates it into a unique patchwork of numbers that allows Ring to

[1] Webb Wright, "*Ring's 'Familiar Faces' is here: Why privacy experts worry its mass surveillance in disguise*," ZDNET (DEC. 10, 2025), at https://www.zdnet.com/article/amazon-ring-familiar-faces-feature-privacy-concerns/ ("Wright").

[2] Cat Ellis, "*Who goes there? Your Ring doorbell can now recognize up to 50 familiar faces and let you know if a caller is a friend or stranger,*" TECHRADAR (APRIL 16, 2026), at https://www.techradar.com/home/home-security/ring-familiar-faces-uk-launch.

[3] Wright.

re-identify who that person is each time Familiar Faces deploys facial recognition on them.[4]

3. Facial recognition data is highly sensitive and is the type of identifying information which cannot be altered or changed.[5] Indeed, like Ring and the Familiar Faces feature, "[f]acial recognition systems don't keep actual images […] [t]hey convert a face into a mathematical template that maps the positions and proportions of the face's features. When [the] camera scans a person later, the system checks their live face against these templates to confirm an identity."[6]

4. When Plaintiffs and Class members entered the homes and businesses of places which had Ring cameras that deployed Familiar Faces, they did not consent to have their privacy rights violated at the entrance way. However, that is exactly what happened. Much to the consternation of privacy experts and members of Congress, Ring continues to deploy mass surveillance technology at each of these entrance ways without adequate consent.

5. As the Electronic Frontier Foundation ("EFF") stated, "[t]oday's feature to recognize your friend at your front door can easily be repurposed tomorrow for mass surveillance."[7] United States Senator Edward Markey of Massachusetts sent a letter condemning the Familiar Faces feature, stating in-part: "[a]lthough Amazon stated that Ring doorbell owners must opt in to activate the new [Familiar Faces] feature, that safeguard does not extend to individuals who are unknowingly captured on video by a Ring doorbell camera. These individuals never receive notice, let alone the opportunity

---

[4] *Id.*

[5] Jonathan S. Weissman, "*Facial recognition data is a key to our identity – if stolen, you can't just change the locks*," THE CONVERSATION (APR. 28, 2026), at https://theconversation.com/facial-recognition-data-is-a-key-to-your-identity-if-stolen-you-cant-just-change-the-locks-278289 ("Weissman").

[6] *Id.*

[7] *Id.*

to opt in or opt out of having their face scanned and logged in a database using [facial recognition technology.]. To put it plainly, Amazon's system forces non-consenting bystanders into a biometric database without their knowledge or consent. This is an unacceptable privacy violation."[8] According to EFF, "Amazon may retain a person's biometric data for up to six months even if they're not saved by a Ring user in the Familiar Faces [feature] library."[9]

6. Ring clearly has the ability to follow biometric privacy laws with respect to the Familiar Faces feature – but it deliberately chooses not to. Specifically, Ring told *The Washington Post* that Familiar Faces will not be available in Texas, Illinois, or Portland, Oregon because each jurisdiction has strict laws banning this type of biometric facial recognition surveillance.[10] However, the rest of the country, including Plaintiff and Class members do not get the same respect.

7. As EFF states, "[i]t is troubling that companies are making a product that by design is taking biometric information from people who are doing the innocent act of walking onto a porch."[11]

8. Defendant's conduct here represents a profound privacy failure for millions of people who are now being tracked by Amazon – which has a contentious relationship with and tempestuous history regarding consumer privacy rights. Ring is, by far, the largest deployable front door camera in the United States, which means that Ring's creation of Familiar Faces will impact more consumers than any of its competitors could.

---

[8] Sen. Markey Letter to Amazon CEO Andrew Jassy re Privacy Concerns over Ring's Familiar Faces feature (October 31, 2025), at https://www.markey.senate.gov/imo/media/doc/letter_to_ring_on_frt.pdf.

[9] Wright.

[10] Shira Ovide, "*Amazon's Ring plans to scan everyone's face at the door*," THE WASHINGTON POST (OCT. 3, 2025), at https://www.washingtonpost.com/technology/2025/10/03/amazon-ring-doorbell-facial-recognition-pricacy/.

[11] *Id.*

However, rather than act as an industry leader and respect digital privacy rights, Ring has consciously chosen the exact opposite.

9. As such, Defendant has invaded or allowed for the invasion of Plaintiff's and Class members' privacy rights.

10. Against that backdrop, Plaintiff seeks to rectify these harms under state and common law, pursuing actual damages, statutory damages, restitution, disgorgement of profit into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys' fees, a declaratory judgment, injunctive relief and any other relief this Court deems just and proper.

JURISDICTION AND VENUE

11. *Subject Matter Jurisdiction.* Plaintiff brings this under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), which allows state and common law class actions to be prosecuted in federal courts if those actions: (1) represent over 100 putative class members, (2) have minimal diversity between the litigants, and (3) seek over $5,000,000.00 in damages exclusive of costs and interest. Here, there are millions of Americans who have walked by Ring cameras which have activated the Familiar Faces feature. Additionally, there is minimal diversity between the litigants – including in this instance, where Plaintiff Sigwalt is a Virginia resident whereas Defendant Amazon is headquartered in this District, in Washington. Finally, the damages in this action far exceed $5,000,000.00 when calculating the statutory damages that may be owed to each Class member in addition to the actual damages caused by the aggregate loss of value of biometric information.

12. *Personal Jurisdiction.* This Court has personal jurisdiction over the litigants because Defendant Amazon is headquartered here, Defendant Amazon's acts or practices were directed toward this State (and thus, Defendant Amazon intentionally availed itself of this jurisdiction by choosing to do business here) and, since Defendant Amazon's products are used throughout the United States, Defendant Amazon knew or should have

known that facial recognition technologies were being used to intercept the actions of Class members in this State.

13. *Venue.* Venue is proper because (1) the Defendant Amazon is headquartered and conducts business in this District, (2) Defendant Amazon acts or omissions were directed toward this District, (3) a substantial part of the events, acts and omissions giving rise to Class members' claims occurred here, and (4) because Class members were harmed here.

14. Additionally, Defendant Ring's Terms of Service select this District as a preferred venue which also contains a choice of law and jurisdiction provision for Washington.

PARTIES

PLAINTIFF

Plaintiff Charles Sigwalt

15. Plaintiff Charles Sigwalt is a resident of the Commonwealth of Virginia.

16. During the relevant period, Plaintiff Sigwalt visited friends and family members' homes and, unbeknownst to him, had his facial recognition data collected by Ring through the Familiar Faces feature. To this day, Plaintiff Sigwalt believes that Ring continues to retain his biometric information in the form of his facial recognition template.

17. Not only was Plaintiff Sigwalt not adequately informed about the collection of his facial recognition data, but he was also not adequately given compensation for his sensitive and valuable information.

18. Plaintiff Sigwalt has suffered the following injuries from (1) the interception of his private and valuable data, including his biometric facial recognition data, (2) the retention and use of this private and valuable data to Ring, and (3) the failure to justly compensate Plaintiff for his valuable information. Plaintiff Sigwalt feels the emotional stress of not knowing when or where his facial recognition information might be collected under the mass surveillance system set by Ring. Plaintiff Sigwalt was harmed as follows:

a. Through the loss of value of his sensitive information that might be associated and collected with Plaintiff's visits to properties which use the Familiar Faces feature;

b. Intrusion upon Plaintiff and Class members' privacy at the homes of family members and friends and the right in those places to have a reasonable expectation of privacy;

c. Lack of compensation for the use and retention of Plaintiff and Class members' data, as well as increased sales due to the Familiar Faces feature of Ring cameras; and

d. Profiting from the retention and use of Plaintiff and Class members' biometric facial recognition data in a way that would be inequitable sans disgorgement of profit.

19. As a result of these privacy injuries, Plaintiff seeks all relief available to him and as this court deems just and proper.

DEFENDANTS

Defendant Amazon.com, Inc.

20. Defendant Amazon.com, Inc. is a Delaware corporation with its principal place of business located in Washington.

Defendant Ring LLC

21. Defendant Ring LLC is a Delaware limited liability company with its principal place of business located in California.

22. Defendant is a sophisticated business owned by Amazon.com, Inc., which sells home security and smart home devices.

23. In the past, Ring has faced substantial scrutiny for both facial recognition data collection as well as various privacy violations – which have all been the subject of other litigation, including fines by the Federal Trade Commission which have totaled several million dollars.

FACTUAL ALLEGATIONS

Defendant's Business and Privacy Representations

24. Ring cameras are as ubiquitous as Defendant's parent company – Amazon.

25. Found on almost any doorway or entrance into a small business or home in America, Defendant's Ring cameras revolutionized the ability of these small businesses and homes to protect themselves against the possibility of crime at their doorstep.

26. An example of a Ring camera can be seen in the image below:

27. For as long as Ring cameras have existed (nearly a decade), there have been grave concerns about consumer privacy associated with the placement of cameras all across the entrance ways in America.

28. These concerns recently became loud demands for change as Defendant implemented its "Familiar Faces" into each of its devices. According to Defendant, "Familiar Faces uses advanced intelligence to help you get personalized alerts when your camera recognizes people you know. For example, instead of seeing "Person at Front Door" you'll see "Chris at Front Door." Your camera learns how to recognize friends, family, and frequent visitors over time."[12]

29. As Defendant states, "when your camera detects a face, it captures the person and adds them to your Familiar Faces library."[13] Indeed, for this feature to even function, it must recognize faces at the onset; including each and every face that enters into the view of the camera which has Familiar Faces enabled. This is confirmed by the fact that Familiar Faces also keeps a library of "unfamiliar faces" which are faces which have not been labeled by the Ring user, but which have been identified using facial recognition by Defendant.

30. Familiar Faces also has the capacity to detect repeating faces which can be merged into one named person.[14] This means that Ring's cameras which use Familiar Faces can use facial recognition technology and assigned, specific identifiers to detect when it sees the same person more than once.

31. The facial recognition data collected by Defendant are not stored locally, they are shared and then subsequently stored on Amazon's cloud product.[15]

---

[12] https://ring.com/support/articles/z3yhg/familiar-faces?srsltid=AfmBOoq6eEna6YYsYlP9YbgOc5XVMQc3JK86kKlv5hIyfKaZGuxLYHcf, (last accessed June 1, 2026).

[13] *Id.*

[14] *Id.*

[15] *Id.*

32. While Defendant claims that images (and subsequent facial recognition data) of 'unrecognized faces' are only kept for 30 days and 'recognized faces' for 180 days, this appears to be untrue as Ring users can unsubscribe for an unquantified amount of time – only to have facial recognition resumed using saved profiles.[16]

33. There are serious civil rights concerns about the use of facial recognition, as facial recognition products regularly mis-identifies people of color and women. Defendant even acknowledges this, stating: "recognition results might vary, and misidentification can occur. We continuously improve the technology to enhance performance."[17]

The Sensitivity of Biometric Information

34. Biometric technologies, at the most basic level, collect biometric data and use that data to identify or recognize a person based upon some biometric identifier. Specifically, as relevant here, facial recognition technology is a category of biometric technology that analyzes facial features to identify a person.

35. Facial recognition technology operates by detecting an individual's face in person or from an image. A facial recognition technology system then generates a unique faceprint (similar to a fingerprint) by performing an analysis of facial geometry and other features of the face, such as the distance between the nose and the mouth, the shape of the cheekbones, depth of eye sockets, and contour of the lips, ears and chin, among other unique measurements and features.

36. Faceprints generated by facial recognition technology systems may be used by the system to verify a person's identity by conducting a one-to-one comparison. For example, U.S Customs and Border Protection uses facial recognition technology to biometrically confirm the identity of travelers that come to the United States by comparing a photo taken of the traveler at arrival against the passport photo presented by the traveler.

[16] *Id.*

[17] *Id.*

Facial recognition technology systems may also compare an individual's face print against a larger database of face prints in order to determine whether the individual matches any person included in the database.

37. New privacy and biometrics laws addressing the growing risks and proliferation of identifying people by their unique biological characteristics. More advanced biometric identification methods continue to be rapidly developed, such as brain signal identification, heart pattern recognition, and finger vein pattern tracking.

38. Two main classes of biometrics data can be collected from individuals: (i) behavioral characteristics and (ii) physiological characteristics.[18] Behavioral characteristics track the conduct and actions of an individual, which may include an individual's keystroke, signature, and voice recognition.[19] Physiological characteristics examine the size, shape, or composition of the individual's face and body, including hand geometry and facial recognition.[20] "Biometric identification has expanded from describing basic physical attributes to now include fingerprint scans, iris scans, retinal scans, voice recognition," and DNA.[21]

39. Biometric identifiers come in a variety of forms that are unique (and largely unchangeable) to each person. This sensitivity prompts a critical need to protect and secure biometric identifiers that may: specifically link an individual to a data record; create digital

---

[18] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589–592 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; *see* generally, "*What is Biometrics?*," IDEMIA, www.morpho.com/en/biometrics (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable) (last visited May 15, 2026).

[19] *Id.*

[20] *Id.*

[21] Center for Global Development, *Biometrics FAQs*, CGD, 2019, https://www.cgdev.org/page/biometrics-faqs (last visited May 15, 2026).

identities that can be used for fraudulent purposes;[22] and, be compromised by their immutability and limitations to modification.

40. Businesses like Disney can use biometric data to identify consumers and link it to information such as their methods of payment, and types of credit cards and debit cards they own. The result is a vast repository of information—purchasing history, consumer habits, medical services paid for, etc.—all tied to an individual's biometric identifiers.

41. In 2023, the U.S. biometrics market and industry were valued at nearly $9.98 billion.

42. Personally identifiable information ("PII") has intrinsic value; however, biometric data often carries significantly greater value than other forms of PII–such as an address or passport number–because it is generally immutable and cannot be changed once compromised. According to the Richmond Journal of Law and Technology (Volume XV, Issue 4):

> PII is an exceptional resource that companies can use for internal purposes or to sell to other companies…. Due, in part to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII. The value of the data increases when combined to provide information, such as consumer preferences that are not discernable from the data points individually.
>
> As a result, companies are maintaining, sharing and selling dossiers of millions of consumer preferences… The potential for increased profits and cost savings serve as a substantial impetus for companies to ensure and cost savings serve as substantial impetus for companies to ensure that their actions

[22] https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity (last accessed May 26, 2026).

do not compromise access to this valuable resource.

43. Companies operating in data driven environments use PII for a variety of purposes, such as targeting specific consumers or, as in this case, reducing costs associated with labor and security. Data breaches further illustrate the value of PII, when information is assigned a resale price on the dark web. In previous data breach litigation, the loss of value of PII has been calculable and compensable to an exact dollar amount per individual—logic equally applicable to the most valuable biometric type.

44. Recognizing the need to protect consumers and citizens, the FTC Policy Statement on Biometric Information and Section 5 of the Federal Trade Commission Act provides:

> Even outside of fraud, uses of biometric information or biometric information technology can pose significant risks to consumers…. Moreover, without clear disclosures and meaningful choices for consumers about the use of biometric technologies, consumers have little way to avoid these risks or unintended consequences of these technologies.

45. It goes on to state that the "use of biometric information technology may be an unfair practice within the meaning of the FTC Act":

> As discussed […] the collection of biometric information can create a serious risk of harm to consumers. Such harms are not reasonably avoidable by consumers if the collection and use of such information is not clearly and conspicuously disclosed or if access to goods and services is conditioned on providing the information. For instance, if businesses automatically and surreptitiously collect consumers' biometric information as they enter or move through a store, the consumers have no ability to avoid the collect or use of that [valuable] information.

46. In response to the growing use of invasive biometric technologies, state legislatures and city councils across the country have either enacted or are contemplating biometric privacy statutes. Many of these statutes impose high statutory penalties to safeguard critical privacy rights and deter unlawful data practices.

Defendant's Conduct Violates the FTC Act

47. Ring's conduct violates numerous laws as well as basic notions of consumer privacy.

48. *Defendant's Conduct Violates the FTC Act.* Ring's collection, retention, and use of biometric information without adequate consent demonstrates that Ring violates Section 5 of the Federal Trade Commission Act – which protects against deceptive and unfair trade practices.

49. According to the Federal Trade Commission, the collection, retention, and use of biometric information does not, on its face, violate Section 5 of the Federal Trade Commission Act. However, it is considered a deceptive and unfair trade practice when the party collecting the information (here, Ring) "[e]ngag[es] in surreptitious and unexpected collection or use of biometric information."

50. In this instance, Ring fails to adequately disclose the collection of facial recognition data, which violates Section 5 of the Federal Trade Commission Act. California's consumer protection laws follow Federal Trade Commission guidance regarding deceptive and unfair trade practices: this means that Ring's conduct violates consumer protection laws because of the failure to follow the Federal Trade Commission's guidance with respect to the disclosure biometric information collection.

51. *Defendant's Conduct Offends Basic Privacy Rights.* Ring's collection of facial recognition violates basic notions of consumer privacy in the United States. Indeed, studies prove as much:[23]

[23] https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/, (last accessed June 1, 2026).

a. A majority of people (55%) want the government to impose restrictions on police use of facial recognition technology.

b. Nearly half of the public (46%) want the right to opt out of the use of facial recognition technology, with an even higher figure for minority ethnic groups (56%) for whom the technology is even less accurate.

c. Most people oppose the use of facial recognition technologies for commercial benefit, often because they do not trust that facial recognition technology will be used ethically; this includes that 77% of people are uncomfortable with facial recognition being used in public places.

d. People fear the normalization of surveillance but are prepared to accept facial recognition when there is a clear public benefit – though 67% oppose its use in public places like schools and 61% oppose its use on public transport.

52. There is no clear benefit to the use of facial recognition by Ring; and consumer privacy advocates, like Senator Markey, have been concerned that the day would come where Ring would integrate facial recognition technology to implement mass surveillance without consent on Plaintiff and Class members. Unfortunately, that day has come.

The Value of Consumer Biometric Data and Harm to Consumers

53. Plaintiff and Class members were harmed when Defendant invaded their privacy rights by collecting their facial recognition data without consent. Reasonable consumers, including Plaintiff, would not have entered into the presence of Ring cameras had they known that their privacy rights would be invaded as a result.

54. PII and PHI is extremely valuable.

55. There is a huge market for the type of data collected by Ring, including facial recognition data. Plaintiff and Class members have suffered pecuniary losses when Defendant collected and retained their sensitive biometric data because of the value of the data itself.

56. The value of consumers' biometric data is axiomatic. Indeed, it is estimated that the facial recognition data of each consumer is valued at between $20 to $134 per operational savings and fraud prevention programs.[24] [25]

57. As the Defendant's industry continues to grow in the United States, so too are the desires of the advertising industry to profit from the data that accompanies biometric information collection.

58. Plaintiff Sigwalt and Class members suffered concrete harm when Ring collected, used, and retained and converted their facial recognition data for profit. Plaintiff Sigwalt's facial recognition data was used for profit because the Familiar Faces feature is sold is now advertised as a key feature when sold to potential consumers and purchasers of Ring cameras.

59. Ring caused damage and diminution in the value of biometric data — a form of personal property protected by both inherent and statutory privacy rights.

60. This is type of biometric information is aa gold mine for hackers, and a data breach of biometric information would be devastating for Plaintiff and Class members.

61. The severity of this violation is heightened by the immutable nature of biometric identifiers; once an individual's facial data is captured and linked to identity, it cannot be changed or revoked. To make matters worse, Ring does not have an established policy about collecting facial recognition data from minors who pass by their cameras with Familiar Faces activated. Thus, when Ring collects facial recognition from minor class members – whom cannot adequately consent to having their privacy rights violated – that facial recognition data does not and cannot change.

[24] Navrup Tom, "*What are biometrics? The pros and cons of biometric security*." AUTHO BLOG (ONLINE) (MAY 24, 2021), at https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/.

[25] "*The Numbers Don't Lie: 80+ Biometric Statistics*," IPROOV (ONLINE) (JAN. 7, 2026), at https://www.iproov.com/blog/biometric-statistics-70.

CLASS ACTION ALLEGATIONS

62. Plaintiff Sigwalt brings this action pursuant to Federal Rule of Civil Procedure 23, *et seq.* individually and on behalf of the following Classes (collectively, the "Class"):

> ***Nationwide Class***. All natural persons in the United States who had their facial recognition data collected, retained, and otherwise used by the Familiar Faces feature created and implemented by Defendant during the applicable statutory period.
>
> ***Virginia Sub-Class***. All natural persons in the Commonwealth of Virginia who had their facial recognition data collected, retained, and otherwise used by the Familiar Faces feature created and implemented by Defendant during the applicable statutory period.

63. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

64. *Numerosity*. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands or even millions of individuals, and the members can be identified through Defendant's records.

65. *Predominant Common Questions*. The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant violated Plaintiff's and Class members' privacy rights;

b. Whether Defendant was unjustly enriched;

c. Whether Defendant's acts and practices violated state consumer protection laws;

d. Whether Defendant's acts and practices violated privacy state statutes and common laws;

e. Whether Plaintiff and the Class are entitled to equitable relief, including but not limited to injunctive relief, restitution, and disgorgement; and,

f. Whether Plaintiff and the Class are entitled to actual, statutory, punitive and/or other forms of damages, and other monetary relief.

66. *Typicality*. Plaintiff's claims are typical of the claims of the other members of the claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories.

67. *Adequate Representation*. Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to any Plaintiff. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to the interests of the other members of the Class.

68. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy, and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

69. Plaintiff may revise the foregoing class allegations and definitions based on

facts learned and legal developments following additional investigation, discovery, or otherwise.

FIRST CAUSE OF ACTION

VIOLATIONS OF STATE CONSUMER PROTECTION LAWS

VIRGINIA CONSUMER PROTECTION ACT OF 1977

Va. Code § 59.1, *et seq.*

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASS)

AND ALL SUBSTANTIALLY SIMILAR STATE STATUTES

70. Plaintiff re-alleges and incorporates by reference all preceding paragraphs with the same force and effect as if fully stated herein.

71. Defendant is considered a 'business' under Virginia's Consumer Protection Act of 1977 ("VCPA").

72. Defendant's business acts and practices are unfair and deceptive under the VCPA. Virginia (as well as other states through their respective unfair and deceptive trade practices statutes) has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal biometric data. Defendant violated VCPA by, among other things, intercepting and using Plaintiff's and Class members' sensitive data, including biometric information, without consent and for profit.

73. Defendant further engaged in unfair business practices because it made material omissions concerning the information including failing to gain adequate express consent, which knowingly deceived and misled Plaintiff and Class members

74. Defendant's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Defendant secretly collecting, intercepting, and misusing Plaintiff's and Class members' sensitive and highly valuable personal biometric data is significant, and there is no corresponding benefit resulting from such conduct.

75. Finally, because Plaintiff and Class members were completely unaware of Defendant's conduct, they could not have possibly avoided the harm.

76. In this instance, Plaintiff and the Class members cannot give informed consent for the collection and use of their data.

77. Additionally, Defendant's conduct violates the VCPA because it also violates another statute, the Va**.** Code § 59.1, et seq. of the Virginia Consumer Data Protection Act ("VCDPA").

78. Defendant is considered a 'business' under the VCDPA and is therefore defined as a 'controller' under the statute.

79. The information collected by Defendant is considered biometric information according to the VCDPA's definition of biometric information, which, therefore, is defined as 'sensitive data' under the statute.

80. Under the VCDPA, consumers have the right to:

a. Confirm whether or not a controller is processing consumer personal data and to access such personal data;

b. To request to delete personal data provided by or obtained about the consumer; and

c. To opt out of data collection;

81. Defendant meaningfully provides none of these options because Plaintiff and Class members have no clue that their biometric information is even being collected in the first instance.

82. Additionally, a controller, under the VCDPA, must limit the collection of personal data to that which is "adequate, relevant, and reasonably necessary" and none of which apply here. Controllers must also not process sensitive data concerning a consumer without consent – including with respect to children; and Defendant utterly fails to do this as alleged here.

83. Finally, controllers must take reasonable measures to anonymize sensitive data – including to make sure that data cannot be associated with a natural person. But, by design, Defendant's Familiar Faces does the exact opposite.

84. By unlawfully intercepting and using this data, Defendant has taken money or

property from Plaintiff and Class members.

85. Plaintiff and the Class Members seek all available damages under applicable state consumer protection laws, including statutory damages under VCPA.

SECOND CAUSE OF ACTION

VIOLATIONS OF APPROPRIATION LAWS

VIRGINIA APPROPRIATION LAW

Va. Code § 8.01-40, *et seq.*

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASS)

AND ALL SUBSTANTIALLY SIMILAR STATE STATUTES

86. Plaintiff re-alleges and incorporates by reference all preceding paragraphs with the same force and effect as if fully stated herein.

87. Virginia Code 8.01-40, *et seq.* provides: "any person whose name, portrait, or picture without having first obtained written consent of such person … ***for the purposes of trade*** … may maintain suit in equity against the person, firm, or corporation so using such person's name, portrait, or picture to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use. And, if the defendant shall have knowingly used such person's name, portrait, or picture in such a manner as is forbidden or declared unlawful by this chapter, the jury, in its discretion, may award punitive damages."

88. Defendant knowingly violated this provision of the Virginia code by using personal data, photographs, and likenesses in the form of pictures and biometric information of Plaintiff and Class members without their written consent for the purposes of trade.

THIRD CAUSE OF ACTION

VIRGINIA'S COMPUTER CRIMES ACT

Va. Code § 18.2-152.1, *et seq.*

(ON BEHALF OF BOTH THE STATE SUBCLASS)

89. Plaintiff re-alleges and incorporates by reference all preceding paragraphs with the same force and effect as if fully stated herein.

90. The Virginia Computer Crimes Act ("VCCA"), Va. Code § 18.2-152.1 makes unlawful the actions taken by Ring in this Action.

91. Specifically, VCCA section 152.5 provides that "[a] person is guilty of the crime of computer invasion of privacy when he uses a computer network and intentionally examines without authority any […] **identifying information** relating to any other person. 'Examination' under this subsection requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed."

92. Under the statute, identifying information includes, name, date of birth, and biometric data – which includes the images processed by Defendant for biometric information conversation to be used as part of the Familiar Faces feature.

93. Plaintiff will seek all available forms of damages under this statute and as this Court deems just and proper.

FOURTH CAUSE OF ACTION

INTRUSION UPON SECLUSION

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASS)

AND ALL SUBSTANTIALLY SIMILAR COMMON LAWS

94. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

95. Under Virginia common law as well as in numerous states with substantially similar common law recognition, an individual, including Plaintiff, has the right to control and protect their private information.

96. Ring's collection, retention and otherwise use of Plaintiff's and Class Members' identifiable information and biometric information constitutes an intentional invasion of privacy.

97. Plaintiff and Class Members reasonably expected their identifiable information, including their biometric information, would not be collected, retained, or otherwise used by Ring without express written consent – let alone a farcical opt out system. Biometric information, as collected here, is particularly private because these data points are directly identifiable, permanent identifiers.

98. This expectation is particularly heightened given that there were no adequate disclosures of Ring's involvement in collection, retention, and otherwise use of biometric information – even through Ring is sophisticated to know how sensitive it is and maintains more stringent protections for ways it collects biometric data in Illinois, Texas, and Portland, Oregon.

99. Plaintiff and Class Members did not consent to, authorize, or understand Ring's mass collection, retention, and use of their private data.

100. Ring's conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they go into public places including those homes of family and friends, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

101. Ring's conduct is also particularly offensive considering the unclear, opaque nature in which it takes place. Plaintiff and Class Members were completely unaware that Ring collected, retained, and used their biometric information.

102. Ring's conduct caused Plaintiff and Class Members harm and injury, including a violation of their privacy interests.

103. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Ring's as a result of its intrusion upon seclusion.

104. Ring's conduct was intentional, knowing, and carried out with a conscious

disregard for Plaintiff's and Class Members' rights. Thus, Plaintiff and Class Members are entitled to punitive and exemplary damages.

105. Plaintiff and Virginia Class Members also seek any other relief the Court may deem just and proper.

FIFTH CAUSE OF ACTION

GROSS NEGLIGENCE/NEGLIGENCE PER SE

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASS)

AND ALL SUBSTANTIALLY SIMILAR COMMON LAWS

106. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

107. Plaintiff and Class members unknowingly gave Defendant sensitive, nonpublic personal information. This information included biometric information, as discussed above.

108. While Defendant's conduct was intentional as alleged, it was at a minimum (and in the alternative) negligent.

109. By having the ability to collecting, storing, using, and profiting from this data, Defendant owed a duty of care to Plaintiff and Class members not to collect it without consent and to exercise reasonable care in keeping this information confidential.

110. Defendant had common law duties to prevent foreseeable harm to Plaintiff and Class members. These duties existed because Plaintiff and Class members were foreseeable and probably victims of any disclosure to Defendant of this biometric information sans consent.

111. Defendant's duties to protect the confidentiality of Plaintiff's and Class members' nonpublic information, including biometric data, also arose from the special relationship that existed between Plaintiff and Defendant – here, between a technology company which clearly had the capacity not to collect sensitive biometric information and chose to do so anyway. Defendant alone could have ensured that it did not collect or otherwise use the nonpublic personal information, including biometric information,

without consumers' consent – but did so anyway.

112. Defendant knew or should have known that by integrating the Familiar Faces facial recognition technologies on Defendant's Ring cameras that it was systemically collecting this information.

113. But for Defendant's conduct, Plaintiff's and Class members' biometric information would not have been collected and disclosed to itself without consent and, as a direct and proximate cause of this conduct, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial.

114. Plaintiff and Class members seek to recover the value of the unauthorized access to their biometric information resulting from Defendant's wrongful conduct. The measure of damages in this instance is analogous to the unauthorized use of intellectual property. Like a technology covered by a patent or protected by a trade secret, use or access to a person's biometric information is entirely non-rivalrous – the unauthorized use by another does not diminish the rights-holders' ability to practice the patented invention or use the protected trade secret technology. Nevertheless, a plaintiff may generally recover the reasonable use value of their most valuable intellectual property: their biometric information. Especially here, where that the potential use or release of this data can result in terrible consequences for Plaintiff and Class members.

115. This measure is appropriate because (a) Plaintiff and Class members have a protectable property interest in their PII and PHI; (b) the minimum damages value for the unauthorized use of personal property is its rental value; and (c) rental value is established with respect to market value (*i.e.,* evidence regarding the value of similar transactions). Put differently, the value of the data is equivalent to whatever third parties would otherwise pay for that respective data.

116. As such, Plaintiff seeks damages in an amount to be proven at trial.

117. Plaintiff also seeks such other relief as the Court may deem just and proper.

118. Where allowable, in addition to or alternatively to this count, Plaintiff pleads a Negligence Per Se count because Defendant's conduct violates the FTC Act.

SIXTH CAUSE OF ACTION

UNJUST ENRICHMENT

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND SUBCLASS)

AND ALL SUBSTANTIALLY SIMILAR COMMON LAWS

119. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

120. Defendant received benefits from Plaintiff and Class members and unjustly retained those benefits at their expense – namely biometric information.

121. Defendant received benefits from Plaintiff and Class members in the form of the Plaintiff's highly valuable sensitive data, including facial recognition data, that Defendant wrongfully intercepted and used from Plaintiff and Class members without authorization and proper compensation.

122. Defendant disclosed, intercepted, stored, and used this data for their own gain, providing Defendant with economic, intangible, and other benefits, including highly valuable data for the improvement of their platforms and services, including through the Familiar Faces feature.

123. Had Plaintiff known of Defendant's misconduct, they would not have provided any of their valuable data to Defendant.

124. Defendant unjustly retained these benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

125. The benefits that Defendant derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles in every state for Defendant to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

126. Defendant should be compelled to disgorge profits into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that

Defendant received, and such other relief as the Court may deem just and proper.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Finding that Defendant's conduct was unlawful, as alleged herein;

C. Awarding declaratory relief against Defendant;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including injunctive relief;

E. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

127. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial as to all issues triable by a jury.

Respectfully Submitted,

DATED: June 1, 2026

By: /s/ *Lori G. Feldman*

Lori G. Feldman (WSBA No. 29096)
lfeldman@hechtpartners.com
David L. Hecht
(*pro hac vice* forthcoming)
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, New York 10017
Telephone: (917) 983-9321

Lina Kaisey (CA SBN 314322)
(*pro hac vice* forthcoming)
lina@kaiseylaw.com
KAISEY LAW P.C.
100 Wilshire Boulevard, Suite 700
Santa Monica, California 90403
Telephone: (858) 774-0819

Blake Hunter Yagman (N.Y. Bar 5644166)
(*pro hac vice* forthcoming)
blake.yagman@yagmanpllc.com
YAGMAN PLLC
118-35 Queens Boulevard, Suite 444
New York, New York 11375
Telephone: (929) 709-1493

Counsel for Plaintiff Charles Sigwalt and the Proposed Classes and Subclasses