UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JOSEPH BLEIBERG, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. ANKER INNOVATIONS LIMITED, ANKER TECHNOLOGY CORPORATION, and FANTASIA TRADING LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Joseph Bleiberg ("Plaintiff"), individually and on behalf of all others similarly situated, alleges as follows against Defendants Anker Innovations Limited ("Anker Innovations"), Anker Technology Corporation ("Anker Technology"), and Fantasia Trading LLC ("Fantasia"):

NATURE OF THE ACTION

1. This action seeks damages for Plaintiff and other consumers who were victims of Defendants' fraudulent representations concerning the security and privacy features of their "Eufy" brand home security cameras, including the Video Doorbell, SoloCam, and eufycam product lines.

2. Defendants claimed, in marketing materials and elsewhere, that Eufy cameras store videos and images locally (*i.e.*, within the storage of the cameras themselves) and conduct facial recognition locally, rather than transmitting them to cloud storage, such that only the user has access to videos and images recorded by Eufy cameras. Defendants further claimed that Eufy cameras use "military-grade" end-to-end encryption. These claims formed part of a long-term

marketing campaign touting security and privacy, which Defendants conducted specifically to target privacy-conscious consumers and distinguish Eufy cameras from competing products.

3. However, as Defendants were aware, and as Plaintiff learned in November 2022, this was not true. That month, a technology security researcher sounded the alarm regarding Defendants' misrepresented and wrongful practices, revealing that Eufy cameras upload images and facial recognition data to Defendants' cloud storage, which is hosted by a third party (Amazon Web Services ("AWS"), a subsidiary of Amazon.com, Inc.), even where the user did not sign up for cloud storage or services. It was further revealed that separate Eufy cameras linked to other accounts can identify a user's face, meaning that Eufy cameras transmit facial recognition data to cloud storage and share that information between accounts.

4. The researcher also showed that persons can view live footage from Eufy cameras over web browsers, without logging in or otherwise providing any authentication, by using the correct web address, showing that Eufy cameras do not use end-to-end encryption.

5. In response, Defendants conceded that, even for users who did not create a cloud account or agree to the transmittal of images from their Eufy camera to Defendants' cloud storage, Defendants nevertheless collected such images and transmitted and disseminated them to the third-party company that hosts Defendants' cloud storage for consumers.

6. Defendants admitted that it was an "oversight" and an "error" to have represented that it did not engage in this practice, and promised to change their marketing and other consumer-facing materials to make this clear. As of December 20, 2022, however, Defendants continue to falsely advertise Eufy cameras as operating with "No Clouds" and make other misleading claims concerning Eufy cameras.

7. Plaintiff and other consumers relied on Defendants' misrepresentations when purchasing Eufy cameras. However, contrary to Defendants' representations, Eufy cameras transmit user data, including biometric information, to Defendants' third-party-hosted cloud storage, and leave user data unprotected by strong encryption.

8. As a result of Defendants' false representations and undisclosed practices, Plaintiff and other Class members were harmed.

9. This is a class action on behalf of (i) all individuals in the United States who purchased a Eufy camera for personal or household use, and not for resale, during the applicable statute of limitations period (the "Nationwide Class") and (ii) all individuals in New York State who purchased a Eufy camera for personal or household use, and not for resale, during the applicable statute of limitations period (the "New York Class").

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this class action under 28 U.S.C. § 1331 because this complaint asserts a claim arising under the laws of the United States. This Court has supplemental jurisdiction over the state law claims asserted in this complaint under 28 U.S.C. § 1367. In addition, this Court has subject matter jurisdiction under 28 U.S.C. § 1332(d), which, under the provisions of the Class Action Fairness Act ("CAFA"), provides federal courts original jurisdiction over any class action in which any member of a class is a citizen of a state different from any defendant, where there are at least 100 members of the proposed class and in which the matter in controversy exceeds in the aggregate the sum of $5 million, exclusive of interest and costs.

11. Minimal diversity exists between the parties because at least one member of the class is diverse from Defendants. There are at least one hundred members of the proposed class

and the amount in controversy exceeds $5 million to a reasonable probability. Therefore, CAFA jurisdiction properly lies within this Court.

12. This Court has personal jurisdiction over Defendants because Defendants regularly conduct business in Illinois, are present in and licensed to conduct business in Illinois, and engage in conduct that has the substantial, foreseeable, and intended effect of causing injury to persons in Illinois and throughout the United States, including by marketing and selling Eufy cameras to consumers in this Judicial District. Furthermore, pursuant to the End User License Agreement for Eufy products (including the Eufy camera purchased and used by Plaintiff) and the Eufy Security App (the "EULA"), Defendants irrevocably submitted to the jurisdiction of any federal or state court located in Cook County, Illinois, which is within this Judicial District.

13. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) because the EULA provides that any claim, dispute, action, cause of action, issue, or request for relief relating to the EULA will be governed by the laws of Illinois, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction, and that any action or proceeding relating to the EULA must be brought in a federal or state court located in Cook County, Illinois.

PARTIES

14. Plaintiff is a resident of Queens, New York. In or about November 2020, Plaintiff purchased a Eufy Wireless Video Doorbell in Queens, New York. Since then, Plaintiff has used his Eufy camera at his home in Queens, New York. Plaintiff also downloaded and installed Defendants' Eufy Security app for use with his Eufy camera. Plaintiff chose to purchase a Eufy camera, rather than competing products, because he read and relied on Defendants' representations concerning the security and privacy features of Eufy cameras, including their

claims that Eufy cameras operated with "no cloud," that only the user had access to images captured by the camera, and that Eufy cameras used strong encryption. Images of Plaintiff and members of Plaintiff's family and visitors to Plaintiff's home were captured by the Eufy camera and thereafter transmitted and disseminated to Defendants' cloud storage hosted by a third party and subjected to facial recognition technology, which generated a face template or faceprint of individuals captured in such images. When Plaintiff learned that his Eufy camera shared images with Defendants' cloud, he tried to find a way to disable the cloud-sharing function. Had Plaintiff known the truth about Defendants' collection and dissemination of images captured by his Eufy camera, or about Defendants' deficient privacy and security practices, he would not have purchased, or would have paid less for, his Eufy camera.

15. Defendant Anker Innovations is a Hong Kong company with its principal place of business at Room 1318-19, Hollywood Plaza, 610 Nathan Road, Mongkok, Kowloon, Hong Kong SAR, People's Republic of China. Anker Innovations designs and manufactures Eufy cameras for export and sale throughout the world, including throughout the United States, including in New York and Illinois. Anker Innovations offers the Eufy Security App for use with Eufy cameras, including by users in New York and Illinois.

16. Defendant Anker Technology is a Delaware corporation principal place of business in Bellevue, Washington. Anker Technology designs and manufactures Eufy cameras for export and sale throughout the world, including throughout the United States, including in New York and Illinois. Anker Technology offers the Eufy Security App for use with Eufy cameras, including by users in New York and Illinois.

17. Defendant Fantasia is a Delaware limited liability company headquartered in Ontario, California. Fantasia sells Eufy cameras throughout the United States, including in New

York and Illinois, and offers the Eufy Security App for use with Eufy cameras, including by users in New York and Illinois.

SUBSTANTIVE ALLEGATIONS

Defendants' Eufy Camera Products

18. Defendants design, manufacture, market, and sell a variety of consumer technology products under several brand names. Defendants' Eufy brand includes, among other products, several cameras marketed for home security use, allowing users to view live and recorded video of areas around their homes and to automatically receive notifications on their cell phone, tablet, or computer regarding activity detected by the cameras, including thumbnail images when a person is detected in the cameras' field of view or when a person presses the doorbell. Defendants' Eufy-branded security cameras, including the eufyCam product line (such as the eufyCam 2, eufyCam 2 Pro, eufyCam 2C, eufyCam 2C Pro, and the S-3300 eufyCam (also known as the eufyCam 3)), the SoloCam product line (such as the SoloCam S40), and the Solo IndoorCam product line (such as the Solo IndoorCam C24). Some Eufy cameras, such as the Video Doorbell Dual and other "doorbell cameras," also allow users to hear and speak to persons standing near the doorbell.

19. Eufy cameras have a "BionicMind" feature marketed by Defendants as "local artificial intelligence used for facial recognition." This feature enables Eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers (*i.e.*, details about the face's geometry as determined by facial points and contours) and comparing the resulting "face template" (or "faceprint") against the face templates stored in a database.

20. In addition, Eufy camera users must install and use a software application, or "app" (the "Eufy Security App") in order to enable and use the cameras. To set up the Eufy

Security App, a user must provide their email address and other personally identifiable information. The app allows users to access their cameras, view live and historical video feeds, and perform other functions. Eufy cameras communicate with the app to provide user notifications, including notifications of activity detected by the user's cameras.

Defendants' Claims Regarding Privacy and Security of Customer Information

21. At all relevant times, Defendants designed and conducted a long-term marketing campaign touting the supposed privacy and security features of Eufy cameras. Defendants did so in order to target and appeal to privacy-conscious consumers and to distinguish Eufy cameras from competing products. Defendants claimed that only the user can access data associated with their Eufy cameras, that data is stored locally and not sent to Defendants, and that data is always encrypted.

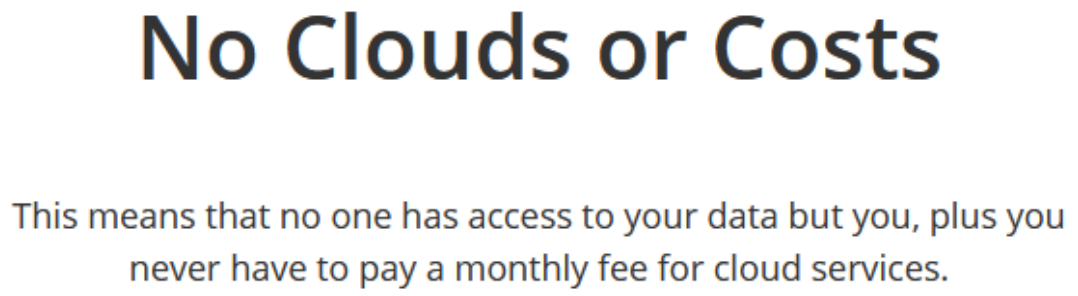
22. As part of this marketing campaign, Defendants' Eufy website for US consumers included a "Privacy Commitment" page containing extensive representations about security and privacy. In connection with marketing Eufy cameras, Defendants made statements such as:

> "To start, we're taking every step imaginable to ensure your data remains private, with you."
>
> "[Y]our recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you."
>
> "With secure local storage, your private data never leaves the safety of your home, and is accessible by you alone."
>
> "All recorded footage is encrypted on-device and sent straight to your phone—and only you have the key to decrypt and watch the footage. Data during transmission is encrypted."
>
> "For Your Eyes Only"
>
> "Everything In-House"
>
> "There is no online link available to any video."

23. Thus, Defendants represented that images and videos captured by Eufy cameras were stored and processed solely on the camera and/or the user's local network, and were not transmitted to Defendants' cloud storage, let alone to cloud storage hosted by a third party. Defendants further represented that facial recognition was performed locally and that biometric information was not shared with anyone, and that strong encryption was used for all data captured by Eufy cameras.

24. As noted above, Defendants offer the Eufy Security App for use with eufy Cameras. Defendants offer this app to consumers via the Google Play store, where Defendants represent that "[n]o data [is] shared with third parties" and that the app *may* collect only one type of personal info (*i.e.*, an email address). Defendants make equivalent representations in connection with offering the Eufy Security App to consumers via Apple's App Store.

25. Furthermore, the "Anker Privacy Policy" available to consumers does not disclose that Defendants will collect, transmit, and disseminate images and biometric information (*i.e.*, face templates) to third parties, including when the user has not created a cloud account or consented to such use of their images and information. Instead, it claims that Eufy cameras operate with "[n]o [c]louds" and that "no has access to your data but you," as follows:



26. In addition, the label for each Eufy camera states:

> Your Privacy is something that we value as much as you do. To start, we're taking every step imaginable to ensure that your data remains private, with you. Whether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you. That's just the start of our commitment to protect you, your family, and your privacy.

27. The label further states that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and that Eufy cameras have "Military-Grade AES-256 data encryption."

Purchasers of Eufy Cameras Rely on Defendants' Misrepresentations

28. Many users, including Plaintiff, selected Eufy cameras in reasonable reliance on Defendants' representations concerning privacy and security, and would have not purchased such products, or would have paid less for them, had Defendants truthfully represented their privacy and security practices. Defendants were aware that consumers relied on their statements concerning the privacy and security features of Eufy cameras, and Defendants designed and conducted a long-term marketing campaign specifically touting these features in order to attractive privacy-conscious consumers.

29. The data wrongfully collected, transmitted, and disseminated by Defendants includes "biometrics," or "biometric information." "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific biometric identifiers, and comparing the resulting "face template" (or "faceprint") against the face templates stored in a database. If a match is found, an individual may be identified.

30. Facial recognition technology in consumer products presents substantial consumer privacy concerns. For instance, an individual's face template may be used as a

password enabling the individual to access an app or program, or a device such as a cellular phone. Critically, though a password may be changed by the consumer if it is subject to a data breach, a face template *cannot* be changed. Thus, maintaining biometric information securely is especially important for consumers. For that reason, the Federal Trade Commission ("FTC") has emphasized that companies should obtain affirmative consent from consumers before collecting biometric identifiers and information from digital photographs and videos.

A Security Researcher Discovers Defendants' Improper Practices

31. On November 23, 2022, a technology security researcher publicly released information showing that Eufy cameras transmitted images and biometric information to Defendants' AWS-hosted cloud storage and applied facial recognition technology to such images to create face templates, even where the user had not signed up for Defendants' cloud storage.

32. The researcher demonstrated that Eufy cameras uploaded name-tagged images to Defendants' cloud storage without using encryption. Notifications that users received from their Eufy cameras thus were accessed and stored by Defendants. Furthermore, video footage was encrypted by a weak key rather than the ""Military-Grade AES-256 data encryption" advertised by Defendants.

33. The researcher demonstrated that Defendants collected and stored images from consumer's Eufy cameras, as well as biometric facial recognition data that identified the researcher as the owner of a Eufy camera, and that this information could be accessed by other persons without authentication. This revealed as well that Eufy cameras paired users' faceprints with other personally identifiable information, allowing Defendants to determine the identities of users.

34. Other researchers and media outlets replicated these findings. One person was able to watch live footage from two Eufy cameras using the open-source VLC media player, showing that Defendants can bypass any encryption and access Eufy cameras through the cloud.

35. Defendants also admitted that they were already aware that their Eufy cameras transmitted images and biometric information to their AWS-hosted cloud storage. In an email to the above-referenced technology security researcher, a Eufy "Customer Service Engineer specialized in safety and privacy" wrote that "the app *needs* to communicate with the cloud server in real-time" (emphasis added) (referring to the transmittal of images to Defendants' cloud storage and the application of facial recognition technology to such images on the cloud) and wrote that "we have also noticed it before," stating that Defendants were already developing a new-generation product that would function differently.

36. On November 29, 2022, after technology security researchers drew public attention to Defendants' misrepresented practices, Defendants issued a public statement conceding that they had misled consumers. Specifically, Defendants conceded that thumbnails (or preview images) of videos are transmitted to and hosted on a cloud server maintained by a third party, namely AWS.

37. Defendants stated:

> Although our eufy Security app allows users to choose between text-based or thumbnail-based push notifications, it was not made clear that choosing thumbnail-based notifications would require preview images to be briefly hosted in the cloud.
>
> That lack of communication was an oversight on our part and we sincerely apologize for the error.

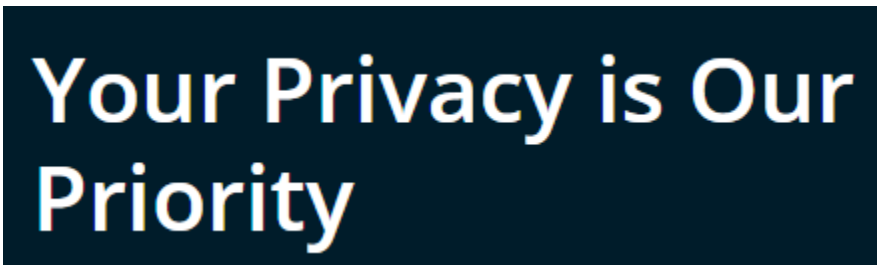
38. However, the researcher had demonstrated

39. Furthermore, Defendants stated that they were "revising the push notifications language in the eufy Security app to clearly detail that push notification with thumbnails require

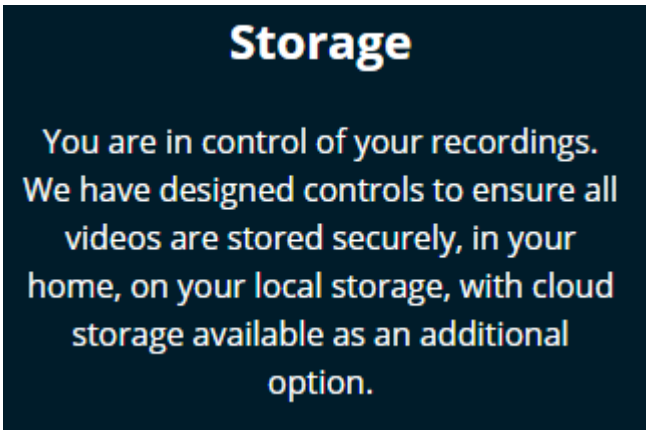
preview images that will be temporarily stored in the cloud," and that they "will be more clear about the use of cloud for push notifications in our consumer-facing marketing materials."

40. Defendants have failed to fulfill these promises, however. As of December 20, 2022, Defendants' Eufy website for US consumers (us.eufy.com) continued to state "No Clouds or Costs" for the Eufy Video Doorbell Dual camera, falsely representing that the product did not collect and transmit images to Defendants' cloud storage. According to Defendants, "[t]his means that no one has access to your data but you."

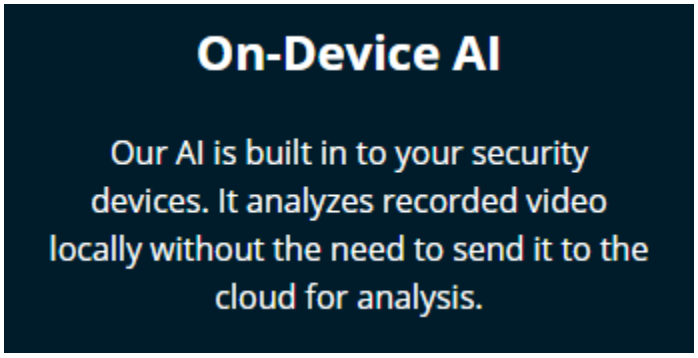
41. Furthermore, Defendants' "Privacy Commitment" page on the Eufy website for US consumers continues to misleadingly represent Defendants' privacy practices, reassuring consumers that consumer privacy is Defendants' priority:



42. Defendants also continue to represent that "all videos are stored securely, in your home, on your local storage, with cloud storage available as an additional option," misleadingly omitting to disclose that images and biometric information are transmitted to Defendants' cloud storage without users' knowledge or consent, even for users that did not create an account for Defendants' cloud storage, as follows:



43. Furthermore, Defendants emphasize that artificial intelligence features of Eufy cameras are built into the devices, misleadingly omitting that it applies facial recognition technology to images and biometric information transmitted, without users' knowledge or consent, to cloud storage hosted by AWS, claiming:



44. Thus, Defendants continue to mislead consumers and users of Eufy cameras, and injunctive relief is appropriate.

TOLLING ALLEGATIONS

45. Plaintiff and other Class members reasonably relied on Defendants' representations, including their representations that Eufy cameras store all information locally, do not share such information with Defendants, and was encrypted. Not until after November 23, 2022, when security researchers published information showing that Defendants' representations

were false, could Plaintiff or other Class members learn such information. Thus, the statute of limitations for all claims should be tolled until November 23, 2022.

CLASS ACTION ALLEGATIONS

46. Pursuant to Rules 23(a), 23(b)(2), or 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this class action on behalf of himself and all Members of the Nationwide Class (the "Nationwide Class"), which shall initially be defined as:

> All individuals in the United States who purchased a Eufy camera for personal or household use, and not for resale, during the applicable statute of limitations period.

47. Additionally, or in the alternative, pursuant to Rules 23(a), 23(b)(2), or 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this class action on behalf of himself and all members of the New York Class (the "New York Class"), which shall initially be defined as:

> All individuals in New York State who purchased a Eufy camera for personal or household use, and not for resale, during the applicable statute of limitations period.

48. Excluded from the Classes are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns, as well as any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

49. The Classes described in this Complaint may be jointly referred to as the "Class" and members of the proposed Classes may be jointly referred to as "Class Members."

50. Plaintiff reserves the right to amend or modify the Class definitions with greater specificity, further division into subclasses, or with limitation to particular issues as discovery and the orders of this Court warrant.

51. The Court can define the Classes and create additional subclasses as may be necessary or desirable to adjudicate common issues and claims of the Class Members if, based on discovery of additional facts, the need arises.

52. Pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure, Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby making final injunctive relief or corresponding declaratory relief and damages appropriate with respect to the Classes as a whole. Defendants continue to falsely market Eufy cameras as operating with "no clouds," continue to misrepresent that they apply facial recognition technology to images captured by Eufy cameras, and continue to apply facial recognition technology to images captured by Eufy cameras without users' knowledge or consent.

53. Numerosity and Ascertainability: The exact number of members of the Classes is unknown as such information is unavailable to Plaintiff at this time. However, Plaintiff believes that individual joinder in this case is impracticable. The Classes likely consist of hundreds of thousands of individuals. These individuals can be readily ascertainable through Defendants or their agents' records and are obtainable to Plaintiff only through the discovery process.

54. Predominance of Common Questions of Fact and Law: Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, but not limited to, the following

a. Whether Defendants unlawfully collected, transmitted, and disseminated images and biometric information from Plaintiff's and Class members' Eufy cameras;

b. Whether Defendants disclosed to Plaintiff and Class members before they purchased Eufy cameras that images and biometric information from such cameras would be collected and transmitted by Defendants;

c. Whether Defendants omitted material facts with regard to the collection and transmittal of images and biometric information from Eufy cameras;

d. Whether Plaintiff and Class members consented to the collection and transmittal of images and biometric information from Eufy cameras;

e. Whether Defendants' conduct constitutes violations of the laws and statutes asserted herein;

f. Whether Defendants' conduct was knowing and/or negligent;

g. Whether, as a result of Defendants' conduct, Plaintiff and Class members are entitled to damages, including compensatory, statutory, or punitive, and the amount of such damages;

h. Whether, as a result of Defendants' conduct, Plaintiff and Class members are entitled to equitable relief, such as declaratory or injunctive relief;

i. Whether, as a result of Defendants' conduct, Plaintiff and Class members are entitled to an award of reasonable attorneys' fees, prejudgment interest, or costs of suit.

55. Typicality: Plaintiff's claims, and Defendants' defenses, are typical of the claims and defenses of and to the Classes. Every member of the Classes was similarly affected by Defendants' course of conduct and experienced the same harm, damages and loss based on Defendants' unlawful conduct. As such, Plaintiff and Class members must establish the same facts in order to prove the claims asserted herein.

56. Adequacy of Representation: Plaintiff does not have any conflicts with any other members of the Classes, and will fairly and adequately represent and protect the interests of the members of the Classes and any other subclass. Plaintiff has retained counsel competent and experienced in consumer protection and class action litigation, trials, and appeals.

57. Superiority of a Class Action: A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of the individual litigation would make it impracticable or impossible for Class members to prosecute their claims individually. Absent a class action, Defendants likely will retain the benefits of their wrongdoing. Because of the small size of individual Class Members' claims, few, if any, Class members could afford to seek legal redress for these wrongs. Absent a representative action, the Class Members will continue to suffer losses and Defendants will be allowed to continue these violations of law and to retain the proceeds of their ill-gotten gains. The trial and litigation of Plaintiff's and Class members' claims are manageable. Individual litigation of the legal and factual issues raised by Defendants' conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform court judgment. Thus, the benefits of proceeding as a class action outweigh the difficulties.

COUNT I

(Common Law Fraud)

58. Plaintiff repeats and incorporates each and every allegation contained above as if fully set forth herein.

59. Defendants engaged in common law fraud when they misrepresented (both through affirmative statements and material omissions of information they had a duty to disclose)

their intention and ability to collect images and biometric information and transmit and disseminate them to a third-party cloud storage host.

60. Defendants knew that Eufy cameras collected images and biometric information and transmitted and disseminated them to third party-hosted cloud storage, that biometric information was accessible to other users, and that live video feeds could be accessed by other persons, but represented that Eufy cameras operated with "no clouds" and that "no one" could access user data except for the user. Defendants also knew that Eufy cameras did not use the level of encryption that Defendants represented they used.

61. Despite this knowledge, Defendants continued to misrepresent and fraudulently conceal the use of cloud storage and facial recognition technology by Eufy cameras, though they had a duty to disclose such information.

62. Defendants intentionally misrepresented that they did not transmit images and biometric information to their cloud storage, or apply facial recognition technology to such images and information, in order to induce Plaintiff and other Class members to purchase Eufy cameras and/or to pay more than Plaintiff and other Class members would have paid had they been aware of the concealed and misrepresented information.

63. Plaintiff and other Class members justifiably relied on Defendants' representations. Had Plaintiff and other members of the Classes known the truth about Defendants' collection, transmittal, and dissemination of images and biometric information captured by Eufy cameras, they would purchased such Eufy cameras, or at a minimum would have paid substantially less for those products.

64. Defendants' affirmative misrepresentations and omissions of material fact injured Plaintiff and other Class Members by causing them to lose money they paid for Eufy cameras.

Plaintiff and the Classes suffered injury at the time they purchased such products and each time that Defendants collected, transmitted, and disseminated images and biometric information in contravention of public representations.

65. As a result of the foregoing, Plaintiff and the Classes are entitled to relief against Defendants, including without limitation, actual damages (or in the alternative, nominal damages) and punitive damages.

COUNT II

(Privacy Violation Based on Intrusion)

66. Plaintiff repeats and incorporates each and every allegation contained above as if fully set forth herein.

67. Defendants, by collecting, transmitting, and disseminating images and biometric information from the Eufy cameras of Plaintiff and Class members without their knowledge, intentionally intruded into a realm in which Plaintiff and Class members have a reasonable expectation of privacy.

68. Defendants obtained unwanted access to Plaintiff's and Class members' data, including but not limited to images and biometric information.

69. Defendants' intrusion into Plaintiff's and Class members' privacy would be highly offensive to a reasonable person, namely because it occurred without their consent or knowledge.

70. Defendants have obtained moneys which rightfully belong to Plaintiff and the Classes to the detriment of Plaintiff and the Classes.

71. It would be inequitable and unjust for Defendants to retain these wrongfully obtained profits and benefits at Plaintiff's and Class members' expense.

72. Defendants' retention of these wrongfully-obtained profits would violate the fundamental principles of justice, equity, and good conscience.

73. Plaintiff and Class members are entitled to restitution of the profits unjustly obtained, plus interest.

COUNT III

(Violation of New York Deceptive Acts and Practices Law (New York General Business Law §§ 349 and 350))

74. Plaintiff repeats and incorporates each and every allegation contained above as if fully set forth herein.

75. By the acts and conduct alleged herein, Defendants committed deceptive acts and practices in the State of New York by making the above alleged misrepresentations directed to consumers in New York.

76. Plaintiff and other members of the New York Class are "consumers" in accordance with New York General Business Law ("GBL") § 349.

77. Defendants' statements concerning the security and privacy of Eufy cameras, alleged above, were advertisements in accordance with GBL § 350.

78. Defendants' statements concerning the security and privacy of Eufy cameras, alleged above, were misleading in violation of GBL §§ 349 and 350.

79. At all relevant times, Defendants conducted trade and commerce in New York and elsewhere within the meaning of GBL § 349, and profited from the sale of Eufy cameras within New York.

80. As a direct and proximate result of Defendants' conduct, Plaintiff and other members of the Classes have suffered damages.

81. Accordingly, Plaintiff and the Classes seek to enjoin the unlawful acts and practices described herein, to recover actual damages or statutory damages of fifty dollars, whichever is greater, as well punitive damages and reasonable attorneys' fees and costs.

COUNT IV

(Violation of the Federal Wiretap Act, 8 U.S.C. §§ 2510, *et seq.*))

82. Plaintiff repeats and incorporates each and every allegation contained above as if fully set forth herein.

83. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

84. The Wiretap Act protects both the sending and receipt of communications

85. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

86. As set forth above, Defendants represent, through advertising, labeling, marketing, and packaging, that Eufy cameras stored all data locally and encrypted such data. However, when electronic notifications are sent between Eufy cameras and a user's device (such as a notification that activity has been spotted on the camera), such communications are contemporaneously intercepted and sent to Defendants' third party-hosted cloud storage.

87. The communications intercepted by Defendants included "contents" of electronic communications made between Eufy cameras and Plaintiff and other Class members, such as the image associated with the notification and any facial recognition information.

88. The transmission of data between the Class members' smart phones, computers, and/or tablets and their Eufy cameras were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic,

photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12). Eufy cameras, Class members' smart phones, computers, and/or tablets, Defendants' third party-hosted cloud storage servers, and the code used by Defendants to direct communications to their servers are "devices" within the meaning of 18 U.S.C. § 2510(5).

89. Defendants were not authorized parties to these communications because Plaintiff and Class members were unaware of Defendants' redirecting of the camera notifications to its own server. Class members did not consent to Defendants' interception of their camera notifications.

90. After intercepting the communications, Defendants then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

91. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiff and the Class members, injunctive and declaratory relief, punitive damages, and reasonable attorneys' fee and other litigation costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants as follows:

A. Determining that the instant action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, certifying the Classes, Plaintiff as the representative of the Classes, and appointing Plaintiff's counsel as class counsel;

B. Awarding Plaintiff and other members of the Classes appropriate relief, including without limitation, actual damages (or in the alternative, nominal damages), restitution, disgorgement, and punitive damages;

C. Awarding equitable, injunctive and declaratory relief, as may be appropriate, including an order requiring Defendants to desist from false and misleading representations concerning the privacy and security of Eufy cameras;

D. Awarding Plaintiff and the other members of the Classes prejudgment and post-judgment interest, attorneys' fees, expenses and other costs; and

E. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

Dated: December 22, 2022

Respectfully submitted,

POMERANTZ LLP

/s/ Jeremy A. Lieberman
Jeremy A. Lieberman
Jonathan D. Park (*pro hac vice* forthcoming)
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (917) 463-1044
jalieberman@pomlaw.com
jpark@pomlaw.com

Joshua B. Silverman
10 South LaSalle Street
Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
Facsimile: (312) 229-8811
jsilverman@pomlaw.com

Counsel for Plaintiff and the Proposed Classes