IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

SAGAR R. DESAI, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ANKER TECHNOLOGY CORPORATION, a Delaware Corporation, FANTASIA TRADING LLC, a Delaware Limited Liability Company, and POWER MOBILE LIFE LLC, a Washington limited liability company,

Defendants.
_____/

Civ. No._____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Sagar Desai brings this class action against Defendants Anker Technology Corp., Fantasia Trading LLC, and Power Mobile Life LLC doing business as "eufy" or "Anker Innovations" (collectively Defendants or "Anker") on behalf of all consumers that have purchased security cameras, video doorbells, and floodlight cameras from Defendants.

I. INTRODUCTION

1. Consumers purchase Defendants' suite of eufy video cameras and video doorbell devices to provide security for, and confidence in the sanctity of, their homes.

2. Among other uses, consumers bought these products to safeguard their properties—setting them up both outside and indoors to give themselves comfort that their residences were secure—and to watch their children—setting them up above cribs and playpens.

3. Anker marketed its products as safe, private, and secure. These consumers took Anker at its word that the images captured by these cameras would be private, would not be stored on a cloud, and would not be visible to anyone else.

4. Anker lied.

5. Despite numerous representations that the eufy products provided "local only" and no "cloud storage" of consumers' information, it has come to light that Defendants were uploading consumers' thumbnail pictures and facial recognition data to the cloud.

6. Even worse, Anker stores unique identifiers matched to the face of any human being who walks in front of a eufy camera (whether that person is a eufy camera purchaser or simply happens to pass, unwittingly, in front of a eufy device); and then stores those identifiers in the cloud, essentially logging the locations of unsuspecting individuals anytime they happen to pass in front of one of the eufy cameras.

7. And, despite Anker's marketing representations that consumers information was "private" or "encrypted," it has been revealed that literally anyone in the world could access and view unencrypted images and footage from the insides of eufy camera owners' homes

8. Anker's corporate voyeurism and undisclosed use of biometric data is not only a deceptive trade practice but also a gross invasion of privacy of each person who has ever happened to walk in front of a eufy product.

9. The following eufy products are subject to this litigation and will be collectively referred to as the "eufy Security Cameras": eufyCam; eufyCam I; eufyCam 2; eufyCam 2C; eufyCam 2 Pro; eufyCam 2C Pro; Solo IndoorCam; Solo OutdoorCam; SoloCams E20, E40, L20, L40 & S40; Video Doorbell (wired); Video Doorbell (Battery); Video Dual Doorbell (Wired); Floodlight Cam 2K; Floodlight Cam 2 E 2k; Floodlight Cam 2 Pro; and 4G Starlight Camera.

10. Plaintiff, on behalf of himself and all others similarly situated, brings this action against Defendants for damages stemming from the above and below described misconduct. With knowledge of his own acts and acts taking place in his presence, and upon information and belief as to all other matters, Plaintiff alleges the following:

II. PARTIES

Plaintiff:

11. Mr. Desai is a Florida citizen residing in Miami-Dade County and is otherwise *sui juris*.

12. As detailed below, Mr. Desai purchased various eufy Security Cameras directly from Defendants and from online retailers.

13. When Mr. Desai purchased his eufy Security Cameras, he was unaware that Anker had misrepresented the privacy and security features of the cameras. Had Mr. Desai known that Anker had misrepresented, or failed to disclose, the privacy and security operations, he would not have purchased the eufy Security Cameras or would not have paid as much for it as he did.

Defendants:

14. Anker Technology Corporation is a Delaware corporation headquartered in Bellevue, Washington. Anker Technology, along with its co-Defendants, manufactures and markets the eufy Security Cameras at issue in this litigation.

15. Power Mobile Life, LLC is a Washington limited liability company with headquarters in Bellevue, Washington. Power Mobile Life, along with its co-Defendants, manufactures and markets the eufy Security Cameras at issue in this litigation.

16. Fantasia Trading, LLC is Delaware limited liability company headquartered in Ontario, California. Fantasia Trading, along with its co-Defendants, manufactures and markets the eufy Security Cameras at issue in this litigation.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this class action pursuant to the Class Action Fairness Act ("CAFA") and 28 U.S.C. § 1332(d), because members of the proposed Classes are citizens of states different from Anker Technology's home states of Delaware and Washington, Power Mobile Life's home state of Washington, and Anker Fantasia Trading, LLC's home states of Delaware and California. Upon information and belief, the total amount in controversy in this action exceeds $5,000,000 exclusive of interest and costs.

18. This Court has personal jurisdiction over Defendants pursuant to Florida Statutes § 48.193(1)(a)(1), (2), and (6) because Defendants, directly or through an agent, conduct substantial business in this judicial district; some of the actions giving rise to the claims took place in this judicial district; and some of the claims arise out of Defendants, directly or through an agent, operating, conducting, engaging in, or carrying on a business or business venture in Florida, committing a tortious act in this state, and causing injury to property in Florida arising out of Defendants' acts and omissions outside of Florida; and at or about the time of such injuries Defendants were engaged in solicitation or service activities within Florida, or products, materials, or things processed, serviced, or manufactured by Defendants were used or consumed within Florida in the ordinary course of commerce, trade, or use, and Defendants, directly or through an agent, derived substantial revenue from their activities within this State.

19. Florida has significant contacts with Defendants because Defendants have purposefully availed themselves of the Florida market and Florida consumers by marketing and distributing the eufy Security Cameras within this District and the State of Florida.

20. Defendants' purposeful availment and extensive contacts with Florida renders the exercise of jurisdiction by this Court over them and their respective affiliated or related entities permissible under traditional notions of fair play and substantial justice.

21. Venue is proper in this forum pursuant to 28 U.S.C. § 1391 because the named Plaintiff resides in this judicial district and purchased the eufy Security Cameras while residing in this district. In addition, Defendants transact business in Florida, and a substantial portion of the practices, events, and omissions complained of herein occurred in this judicial district.

22. All conditions precedent to this action have occurred, been performed, or have been waived.

IV. FACTUAL ALLEGATIONS

23. Anker produces smart home appliances and security devices that are sold on Amazon.com and in brick-and-mortar retailers, such as Walmart and Best Buy. The eufy Security Cameras are one such line of products that Anker markets and sells to consumers.

24. The eufy Security Cameras are marketed as "private" and as "local storage only" as a direct alternative to Anker's competitors that require the use of cloud storage.

25. The eufy Security Cameras allegedly contain storage functions that are designed to provide a eufy customer with an option to store his or her security camera footage locally as opposed to the cloud or an Anker server.[1]

[1] The eufy Security Cameras can access a eufy "HomeBase" hard drive, and some have microSD card slots, that allow customers to locally store images from their eufy Security Cameras.

26. Customers who bought any of the eufy Security Cameras were assured by Defendants on their "privacy commitment website" that "[w]ith secure local storage, your private data never leaves the safety of your home and is accessible by you alone" and that "your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you."[2] Anker assured the customers that it was "taking every step imaginable to ensure your data remains private with you." [3]

27. As of December 8, 2022, Anker promised on its website that "[a]t eufy Security, privacy and protection are our top priorities. Both are integral to our daily operations, and to implementing measures that ensure your data is always safe. From your newborn crying for mom, to your victory dance after a game, your personal moments are yours. We are committed to products and services that keep your data private and secure. That's just the start of our commitment to protect you, your family, and your privacy."[4]

28. Anker's purported and advertised commitment to privacy is remarkable: it promises that its customers' data will be stored locally, that the data "never leaves the safety of your home," that footage from the eufy Security Cameras only gets transmitted with "end-to-end" military-grade encryption, and that it will only send that footage "straight to your phone." A screenshot of Anker's "privacy commitment", as published on its website on November 27, 2022, is provided below:[5]

Customers also have the option of not storing images at all by not utilizing the HomeBase or microSD functions.

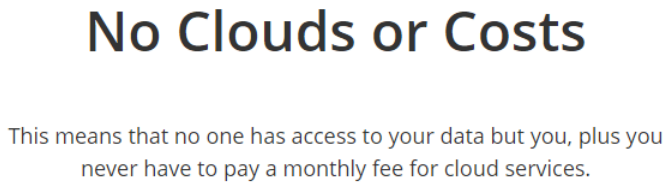
[2] *Privacy Commitment,* eufy Security, Dec. 8, 2022, https://web.archive.org/web/20221208112512/https://us.eufy.com/pages/privacy-commitment

[3] *Id.*

[4] *Id.*

[5] *Privacy Commitment,* eufy Security, Nov. 27, 2022, https://web.archive.org/web/20221127201321/https://us.eufy.com/pages/privacy-commitment

29. Notably, Anker takes care to note that its products use "Local Storage For Your Eyes Only" and emphasizes that "[t]here is no online link available to any video."[6] Anker further promised that "[a]ll recorded footage is encrypted on-device and sent straight to your phone-only you have the key to decrypt and watch the footage. Data during transmission is encrypted."[7] As recently as December 2022, Anker's eufy.com website made the following representation:[8]



[6] *Privacy Commitment,* eufy Security, Dec. 8, 2022, https://web.archive.org/web/20221208112512/https://us.eufy.com/pages/privacy-commitment
[7] *Id.*
[8] *Video Doorbell Dual,* eufy, Dec. 3, 2022, https://web.archive.org/web/20221203140001/https://us.eufy.com/pages/video-doorbell-dual

A. Anker's Privacy and Security Promises Are Revealed to be False.

30. On and around November 23, 2022, information security consultant Paul Moore and a hacker who goes by Wasabi both publicly revealed that Anker's representations regarding how it stores and secures consumers information were patently false.

31. It was first revealed that video and audio captured by Ankers' eufy Security Cameras could be streamed *and watched* by any third party using freely available VideoLAN Client (VLC) media player software.

32. The VLC software allows anyone, anywhere in the world, to access the eufy Security Cameras from someone's home, without the camera owner's permission and view live footage without encryption or the need for authentication.

33. Moore also exposed that Defendants' "supposedly 'private,' 'stored locally', 'transmitted only to you' doorbell is streaming to the cloud - without cloud storage enabled."

34. Not only does Anker not keep consumers' information private, it was further revealed that Anker was uploading facial recognition data and biometrics to its Amazon Web Services ("AWS") cloud *without* encryption.[9]

35. In fact, Anker has been storing its customers' data alongside a specific username and other identifiable information on its AWS cloud servers even when its "eufy" app reflects the data has been deleted.

[9] AWS is the cloud computing business of Amazon.com, providing customers with "cloud based" data management and data storage services, among other products. AWS customers need not store their data on local machines, as they are able to store and access data from anywhere in the world. *See* https://aws.amazon.com/what-is-aws/

36. Anker has been uploading both the images captured from its doorbell and camera products as sent through their push notification process, as well as facial recognition imaging to its cloud, even when customers have declined to utilize the eufy Security Cameras' cloud storage options.

37. Anker stores the facial recognition imaging that it captures through its products alongside several bits of metadata, two of which include the customer's username (owner_ID), another user ID, and the saved and stored ID for the face captured by the camera at that moment (AI_Face_ID).[10]

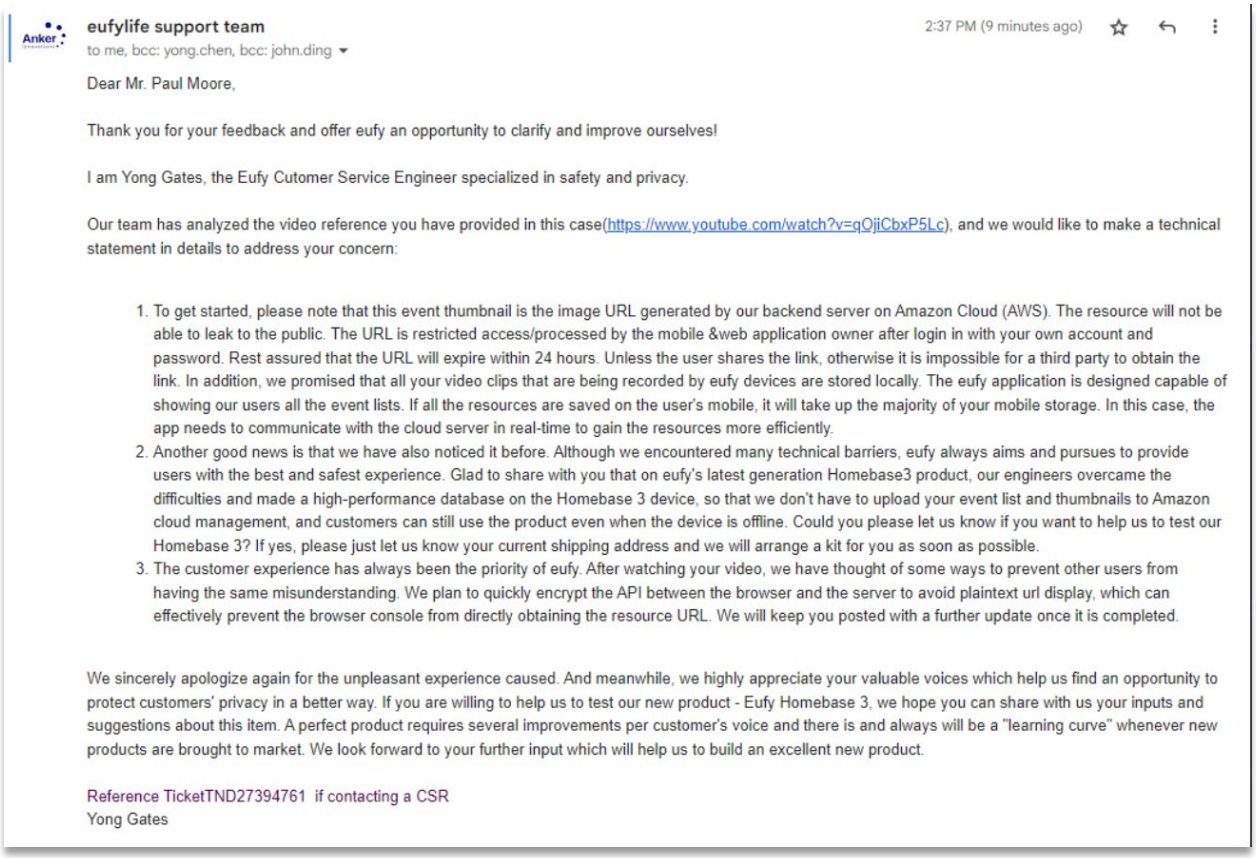
38. Further, even when using a different camera, different username, and even a different HomeBase to "store" the footage locally, Anker is still tagging and linking a user's facial ID to their picture across its camera platform. Meaning, once recorded on one eufy Security Camera, those same individuals are recognized via their biometrics on other eufy Security Cameras.[11]

39. Despite the representations on its website and in its marketing that its cameras use "no clouds or costs," the revelations regarding Anker's conduct have established that the eufy Security Cameras are not only uploading images to Anker's cloud but are also using facial recognition on those images to tie them to users (and nonusers). Further, the eufy Security Cameras have also been taking snapshots from their feeds before a face is recognized and uploading that to the cloud as well.

[10] *Eufy Leaking your "private" images/faces & names… to the cloud.*, Paul Moore, Nov. 23, 2022, https://youtu.be/qOjiCbxP5Lc
[11] *Id.*

B. Anker's Public Response

40. On November 24, 2022, Anker responded to these revelations by writing to Mr. Moore directly, who in turn published the response on his twitter account. In its response, Anker confirmed that images were being uploaded for notification purposes but asserted that the pictures were deleted afterwards. They also said that going forward they planned to "quickly encrypt the API between the browser and the server to avoid plaintext url display, which can effectively prevent the browser console from directly obtaining the resource URL."



eufylife support team 2:37 PM (9 minutes ago)
to me, bcc: yong.chen, bcc: john.ding

Dear Mr. Paul Moore,

Thank you for your feedback and offer eufy an opportunity to clarify and improve ourselves!

I am Yong Gates, the Eufy Cutomer Service Engineer specialized in safety and privacy.

Our team has analyzed the video reference you have provided in this case(https://www.youtube.com/watch?v=qOjiCbxP5Lc), and we would like to make a technical statement in details to address your concern:

1. To get started, please note that this event thumbnail is the image URL generated by our backend server on Amazon Cloud (AWS). The resource will not be able to leak to the public. The URL is restricted access/processed by the mobile &web application owner after login in with your own account and password. Rest assured that the URL will expire within 24 hours. Unless the user shares the link, otherwise it is impossible for a third party to obtain the link. In addition, we promised that all your video clips that are being recorded by eufy devices are stored locally. The eufy application is designed capable of showing our users all the event lists. If all the resources are saved on the user's mobile, it will take up the majority of your mobile storage. In this case, the app needs to communicate with the cloud server in real-time to gain the resources more efficiently.
2. Another good news is that we have also noticed it before. Although we encountered many technical barriers, eufy always aims and pursues to provide users with the best and safest experience. Glad to share with you that on eufy's latest generation Homebase3 product, our engineers overcame the difficulties and made a high-performance database on the Homebase 3 device, so that we don't have to upload your event list and thumbnails to Amazon cloud management, and customers can still use the product even when the device is offline. Could you please let us know if you want to help us to test our Homebase 3? If yes, please just let us know your current shipping address and we will arrange a kit for you as soon as possible.
3. The customer experience has always been the priority of eufy. After watching your video, we have thought of some ways to prevent other users from having the same misunderstanding. We plan to quickly encrypt the API between the browser and the server to avoid plaintext url display, which can effectively prevent the browser console from directly obtaining the resource URL. We will keep you posted with a further update once it is completed.

We sincerely apologize again for the unpleasant experience caused. And meanwhile, we highly appreciate your valuable voices which help us find an opportunity to protect customers' privacy in a better way. If you are willing to help us to test our new product - Eufy Homebase 3, we hope you can share with us your inputs and suggestions about this item. A perfect product requires several improvements per customer's voice and there is and always will be a "learning curve" whenever new products are brought to market. We look forward to your further input which will help us to build an excellent new product.

Reference TicketTND27394761 if contacting a CSR
Yong Gates

41. On November 29, 2022, Anker admitted to reporters at the website www.AndroidCentral.com that for users that chose "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 our error."[12]

C. The Disproving of Anker's Public Response

42. Following the revelations about its security systems and Anker's public response, the American technology news website, The Verge (www.theverge.com), independently tested the eufy Security Cameras, and on November 30, published a damning article, titled: "*Anker's eufy lied to us about the security of its security cameras.*"[13]

43. The Verge reported that it had contacted Anker to discuss the revelations about the eufy Security Cameras, and in particular the fact that "[d]espite claims of only using local storage with its security cameras, eufy has been caught uploading identifiable footage to the cloud. And it's even possible to view the camera streams using VLC.".

44. The Verge reported that "[w]hen we asked Anker point-blank to confirm or deny that, the company categorically denied it. 'I can confirm that it is not possible to start a stream and watch live footage using a third-party player such as VLC,' Brett White, a senior PR manager at Anker, told [the Verge] via email."[14]

45. Anker's statement, however, was contradicted by the Verge's independent testing that showed that the Verge reporters "repeatedly watched live footage from two of our own eufy cameras

[12] *Security researcher says Eufy has a big security problem,* Nicholas Sutrich, AndroidCentral, Dec. 2, 2022, https://www.androidcentral.com/accessories/smart-home/security-researcher-says-eufy-has-a-big-security-problem

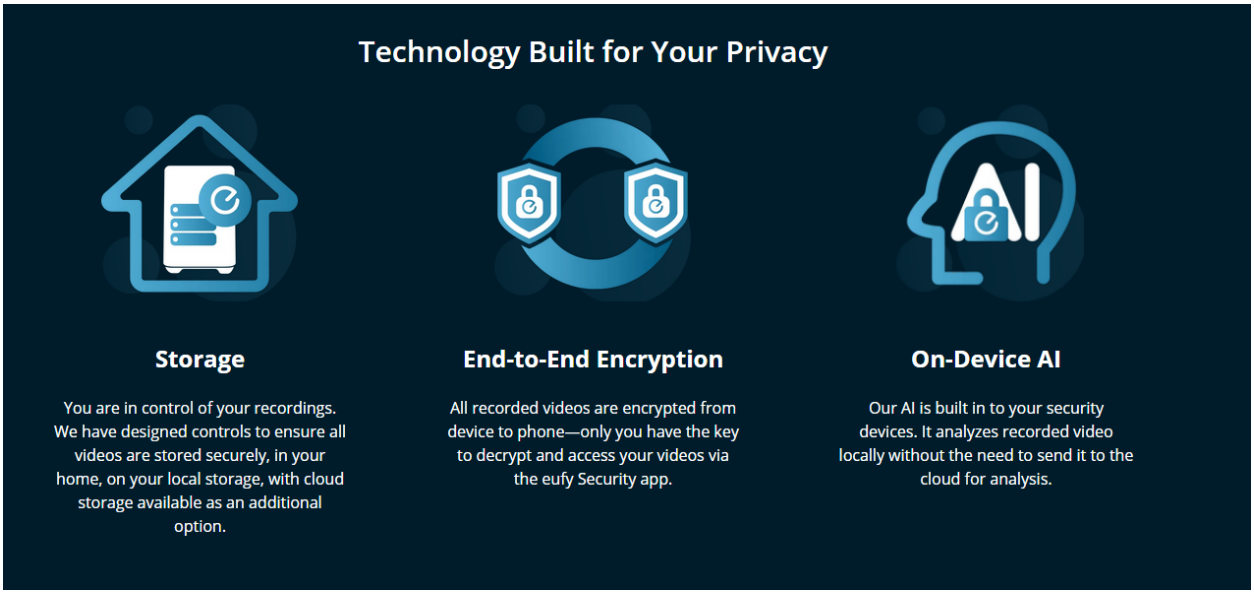
[13] *Anker's Eufy lied to us about the security of its security cameras,* Sean Hollister, The Verge, Nov. 30, 2022, *https*://www.theverge.com/2022/11/30/23486753/anker-eufy-security-camera-cloud-private-encryption-authentication-storage

[14] *Id.*

using that very same VLC media player, from across the United States — proving that Anker has a way to bypass encryption and access these supposedly secure cameras through the cloud."[15]

46. On November 24, 2022, security consulting firm SEC Consult published the results of its own two-year study of eufy Security Cameras, confirming the issues reported by Mr. Moore, and noting that "privacy issues are still a big problem in [Anker's] firmware."[16]

47. In an attempt to rectify its misconduct, Anker has since modified its published, "privacy commitment" to no longer refer to "local storage." Instead, their commitment now only guarantees "storage"[17] Anker has yet to correct its misrepresentations about its "End-to-End Encryption" or its use of cloud storage.



48. On or about December 19, 2022, Anker published a blog post on its website "To our eufy Security Customers and Partners" in which it admits that the "eufy Security's Live View

[15] *Id.*
[16] *The eufyCam Long-Term Observation,* SEC Consult, Nov. 24, 2022, https://sec-consult.com/blog/detail/the-eufycam-long-term-observation/
[17] *Privacy Commitment*, eufy Security, Dec. 9, 2022, https://us.eufy.com/pages/privacy-commitment

Feature on its Web-Portal Feature has a Security Flaw" and goes on to underwhelmingly state that "we do agree there were some key areas for improvement."[18]

49. In particular, Anker noted that it has now modified its web portal so that "users can no longer view live streams (or share active links to these streams with others) outside of eufy's secure Web portal. Anyone wishing to view these links must first log into the eufy.com Web Portal."[19] This admission confirms that prior to these revisions, people could view live streams from the eufy Security Cameras outside of Anker's secure Web Portal.

D. Named Plaintiff's Allegations

50. On or about February 18, 2021, Mr. Desai and his family purchased four (4) eufy Security eufyCam 2 wireless cameras from Amazon.com.

51. On or about September 7, 2021, Mr. Desai and his family purchased two (2) eufy Floodlight Cameras, one (1) eufy Video Doorbell 2K (Wired) and one (1) eufy Solo IndoorCam P24 (Wired) from Amazon.com.

52. On or about October 6, 2021, Mr. Desai and his family purchased a eufy Security Solo OutdoorCam c24 from Amazon.com.

53. On or about October 27, 2021, Mr. Desai and his family purchased a eufy Security Security Floodlight Camera from Amazon.com.

54. On or about December 7, 2021, Mr. Desai and his family purchased a eufy Security Solo IndoorCam P24 camera from Amazon.com.

55. On or about, April 21, 2022, Mr. Desai and his family purchased two (2) eufy SoloCam L20 cameras directly from eufy's online store

[18] *To our eufy Security Customers and Partners*, eufy Security, Dec. 19, 2022, https://community.security.eufy.com/t/to-our-eufy-security-customers-and-partners/3568215
[19] *Id.*

56. On or about November 12, 2022, Mr. Desai and his family purchased one (1) eufy HomeBase 3, one (1) eufy Solar Panel Charger, one (1) eufy SoloCam S40, and one (1) eufy Entry Sensor directly from eufy's online store.

57. Mr. Desai and his family purchased these cameras after performing online research for a home security and home monitoring option that provided safe, secure, private encrypted services.

58. Mr. Desai read and relied on Anker's representations as to its privacy, and its privacy commitments as advertised on both Anker's eufy website and on its product pages at Amazon.com when buying the aforementioned eufy Security Cameras.

59. Mr. Desai set his eufy Security Cameras up both outside and inside his house to not only help him monitor his property but to also serve as "baby monitors" so that he could keep an eye on his young children.

60. Mr. Desai proactively elected to *not* use Anker's cloud storage option, instead relying on his HomeBase and microsd cards that he provided himself and inserted into certain of his cameras to keep his camera's recordings "local" to his property.

61. Mr. Desai did elect to utilize Anker's push notification system so that his cameras would send him notifications when they captured movement, or when his doorbell was activated.

62. Mr. Desai, at all times, believed, as a result of Anker's representations both online and on the packaging of the products he purchased, that the images captured by his cameras would be solely stored locally and would not be stored in Anker's cloud in any way.

63. Mr. Desai relied on Anker's representations when he utilized the eufy' Securities live view feature on its web-portal feature to view images from his family's cameras.

64. Had Mr. Desai known his, his family's, and other people's images and biometric information would be captured and stored on the cloud by Anker or that his live camera feeds could be accessed by unknown third-parties, he would not have purchased the eufy Security Cameras or would have paid less than he did.

V. TOLLING ALLEGATIONS

65. Plaintiff and other Class members reasonably relied on Anker's representations, including their representations that eufy Security Cameras store all information locally, do not share such information with Defendants, and utilized military encryption. Plaintiff and Class members could not have discovered, through the exercise of reasonable due diligence, that Defendants were misrepresenting and concealing the true nature of eufy Security Cameras operations.

66. Not until after November 23, 2022, when security researchers published information showing that Anker's representations were false, could Plaintiff or other Class members reasonably learn such information.

67. For these reasons, all applicable statute of limitations for all claims should be tolled.

VI. CLASS ALLEGATIONS

68. Plaintiff brings this action on his own behalf, and on behalf of all persons similarly situated, pursuant to Rules 23(a) and (b)(2) or (b)(3) of the Federal Rules of Civil Procedure. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions. Plaintiff seeks to certify the following proposed classes:

The Nationwide Class:

> All persons who purchased one or more of the eufy Security Cameras within the applicable statute of limitations.

The Florida Subclass:

> All Florida citizens who purchased one or more of the eufy Security Cameras within the applicable statute of limitations.

69. Excluded from each class are Anker, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliated companies; Class Counsel and their employees; and the judicial officers and their immediate family members and associated court staff assigned to this case.

70. Plaintiff reserves the right to modify, expand, or amend the definitions of the proposed Classes following the discovery period and before the Court determines whether class certification is appropriate.

71. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

Numerosity/Manageability

72. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). The Class members number at least in the hundreds if not the thousands. Anker advertises that over 5,000,000 people use its "eufy" brand products and that they rank as an all-time best seller on Amazon."[20] Individual joinder of all Class members is impracticable.

73. The identity of Class members is ascertainable, as the names and addresses of all Class members can be identified in Anker's books and records. Plaintiff anticipates providing appropriate notice to each certified class in compliance with Fed. R. Civ. P. 23(c)(2)(A) and/or

[20] *About us,* Anker Innovations, Jan. 5, 2023, https://en.anker-in.com/about/

(B), to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

Commonality

74. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because there are questions of law and fact that are common to each of the classes. These common questions predominate over any questions affecting only individual Class members. The predominating common or Class-wide fact questions include, without limitation:

a. Whether Anker collected and stored Plaintiff and the Class members' images and biometric information without their permission;

b. Whether Anker's marketing of their camera products was likely to deceive or mislead reasonable consumers;

c. Whether Anker engaged in unfair, deceptive, unlawful and/or fraudulent acts or practices by marketing their products as for "local storage" and that it would keep Plaintiff and the Class members "privacy safe."

d. Whether Anker warranted that the data collected by the eufy Security Cameras would be encrypted;

e. Whether Anker were unjustly enriched;

f. Whether Anker violated the Florida consumer protection statutes alleged herein; and

g. Whether damages, restitution, equitable, injunctive, declaratory, or other relief is warranted.

Typicality

75. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because Plaintiff's claims are typical of the claims of each of the Class members, as all Class members were and are similarly affected and their claims arise from the same wrongful conduct of Anker.

76. Each Class member purchased one or more of Anker's eufy Security Cameras and thus as a result has sustained, and will continue to sustain, damages in the same manner as Plaintiff. The relief Plaintiff seeks in this action is typical of the relief sought for the absent Class members.

Adequacy of Representation

77. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is committed to the vigorous prosecution of this action and there is no hostility or conflict between or among Plaintiff and the unnamed Class members. Plaintiff anticipates no difficulty in the management of this litigation as a class action.

78. To prosecute this case, Plaintiff has chosen the undersigned law firms, who have substantial experience in the prosecution of large and complex class action litigation and have the financial resources to meet the costs associated with the vigorous prosecution of this type of litigation. Plaintiff and his counsel will fairly and adequately protect the interest of all Class members.

Superiority/Predominance

79. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of the rights of the Class members. The joinder of individual Class members is impracticable because of the vast number of Class members who own the eufy Security Cameras.

80. Because the monetary damages suffered by each individual Class member may be relatively small, the expense and burden of individual litigation would make it difficult or impossible for individual Class members to redress the wrongs done to each of them individually, such that most or all Class Members would have no rational economic interest in individually controlling the prosecution of specific actions. The burden imposed on the judicial system by

individual litigation, and to the Defendants, by even a small fraction of the Class Members, would be enormous.

81. In comparison to piecemeal litigation, class action litigation presents far fewer management difficulties, far better conserves the resources of both the judiciary and the parties, and far more effectively protects the rights of each Class member. The benefits to the legitimate interests of the parties, the court, and the public resulting from class action litigation substantially outweigh the expenses, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized litigation. Class adjudication is simply superior to other alternatives under Fed. R. Civ. P. 23(b)(3)(D).

82. Plaintiff is unaware of any obstacles likely to be encountered in the management of this action that would preclude its maintenance as a class action. Rule 23 provides the Court with the authority and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management challenges. The Court may, on motion of Plaintiff or on its own determination, certify nationwide and statewide classes for claims sharing common legal questions; utilize the provisions of Fed. R. Civ. P. 23(c)(4) to certify particular claims, issues, or common questions of law or of fact for class-wide adjudication; certify and adjudicate bellwether class claims; and utilize Fed. R. Civ. P. 23(c)(5) to divide any Class into subclasses.

Requirements of Fed. R. Civ. P. 23(b)(2)

83. Anker has acted or failed to act in a manner generally applicable to the Class members in the Classes, thereby making final injunctive relief or corresponding declaratory relief appropriate with respect to this class.

VII. CLAIMS FOR RELIEF

COUNT I – VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § § 2510-2522, *et seq.*
(On behalf of Plaintiff and the Nationwide Class)

84. Plaintiff incorporates by reference paragraphs 1 through 83 as though fully set forth herein.

85. 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.

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

87. In 18 U.S.C. § 2520(a), the Federal Wiretap Act provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

88. As set forth above, Defendants represent, through advertising, labeling, marketing, and packaging, that eufy Security Cameras used military-grade encryptions to store all data locally.

89. However, when electronic notifications are sent between eufy Security Cameras and a user's device (such as via someone ringing a video doorbell or the camera sending a notification that movement has been spotted on the camera), such communications are contemporaneously intercepted and sent to Anker's third party-hosted cloud storage.

90. The communications intercepted by Anker included images associated with the communications made between the eufy Security Camera and Plaintiff and other Class members, as well as biometric information.

91. The communications intercepted by Anker included "contents" of electronic communications made between eufy Security Cameras and Plaintiff and other Class members, such as the image associated with the notification and any facial recognition information.

92. The personal data, which Anker transmitted without Plaintiff's and Class members' authorization and/or consent included photographic and video footage which Plaintiff reasonably expected to be confidential and safely and locally secured. Plaintiff and Class members had a legally protected informational privacy interest in the personal and sensitive information as well as an autonomy privacy interest in conducting their personal activities without observation, intrusion, or interference.

93. The transmission of data between the Class members' smart phones, computers, and/or tablets and their eufy Security 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).

94. The eufy Security Cameras, Class members' smart phones, computers, and/or tablets, Anker's third party-hosted cloud storage servers, and the code used by Anker to direct communications to their servers are "devices" within the meaning of 18 U.S.C. § 2510(5).

95. After intercepting the communications, Anker 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)

96. Plaintiff and Class members were not aware that Anker redirected their data for Anker's thumbnail notification system. Nor did Plaintiff and Class members authorize Anker to redirect their data for the thumbnail notification system.

WHEREFORE, 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.

COUNT II – VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA"), Fla. Stat. § 501.201 *et seq*.
(On behalf of Plaintiff and the Florida Subclass)

97. Plaintiff incorporates by reference paragraphs 1 through 83 as though fully set forth herein.

98. Plaintiff and the Class members are "consumer[s]" engaged in "trade or commerce" within the meaning of FDUTPA. Fla. Stat. § 501.203 (7), (8).

99. Anker engages in "trade or commerce" within the meaning of FDUTPA. Fla. Stat. § 501.203(8).

100. FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

101. Anker engaged in unfair and deceptive trade practices that violated FDUTPA, by representing that their security cameras have safety and privacy characteristics that they do not have, including but not limited to the following:

a. Anker misrepresented that user's data will only be stored locally;

b. Anker misrepresented that user's data "never leaves the safety of your home";

c. Anker misrepresented that footage from the eufy Security Cameras only gets transmitted with "end-to-end" military-grade encryption, and that it will only send that footage "straight to your phone; and

d. Anker misrepresented that the user's private data will "never leave the safety of your home."

102. Anker knew that its representations of privacy and security were false but failed to disclose this information to consumers.

103. Anker knew that such information was material to consumer transactions and consumer's decision to purchase the eufy Security Cameras.

104. Anker actively concealed and misrepresented the true nature of how their eufy Security Cameras operated.

105. Anker intended for Mr. Desai and Florida Subclass members to rely on their misrepresentations and omissions so that Plaintiff and the Florida Subclass members would purchase their products.

106. Anker's unfair or deceptive acts or practices, including concealing, omitting, or suppressing material facts about the operation of the eufy Security Cameras had a tendency or capacity to mislead; tended to create a false impression in consumers; and were likely to, and did in fact, deceive reasonable consumers, including Mr. Desai and the Florida Subclass members, about the security and privacy of the eufy Security Cameras as well as the quality and true value of the eufy Security Cameras.

107. Anker intentionally and knowingly misrepresented or omitted material facts regarding the eufy Security Cameras' security and privacy with an intent to mislead Plaintiff and the Florida Subclass members.

108. Anker knew or should have known that its conduct violated the FDUTPA.

109. Plaintiff and the Florida Subclass members were and are injured as a result of Anker's conduct because they paid to own eufy Security Cameras that would protect their information and privacy by only storing the information "locally." Instead, Plaintiff and the Florida Subclass members received and overpaid for eufy Security Cameras that transmitted and stored unencrypted information over the internet.

110. Anker's failure to disclose, and active concealment of, these features were material to Plaintiff and the Florida Subclass members.

111. Plaintiff and the Florida Subclass members have suffered ascertainable losses as a result of Anker's misrepresentations and omissions about the eufy Security Cameras. Had they been aware of the true nature of how the eufy Security Cameras operated, they either would have paid less for the cameras or would not have purchased the cameras. Mr. Desai and the Florida Subclass members did not receive the benefit of their bargain due to Anker's misconduct.

112. As a direct and proximate result of Anker's violations of FDUTPA, Plaintiff and the Florida Subclass members have suffered injury-in-fact and actual damages.

113. Plaintiff and the Florida Subclass members are entitled to recover their actual damages under Fla. Stat. § 501.211(2) and attorneys' fees under Fla. Stat. § 501.2105(1).

114. Plaintiff and the Florida Subclass members have suffered and will continue to suffer irreparable harm if Anker continues to engage in such deceptive, unfair, and unreasonable practices.

115. Plaintiff, on behalf of the Florida Subclass, requests that the Court award them actual damages and issue an order requiring Anker to properly notify the Florida Subclass members of the true nature of how their security cameras operate, as well as award Plaintiff and Class members' attorneys' fees; and any other just and proper relief available under FDUTPA.

COUNT III – NEGLIGENT MISREPRESENTATION
(On behalf of Plaintiff and the Florida Subclass)

116. Plaintiff incorporates by reference paragraphs 1 through 83 as though fully set forth herein.

117. Anker represented on its website that its products provided for "local storage," were "for your eyes only," and that "your private data never leaves the safety of your home."

118. Anker further misrepresented that "no one has access to your data but you."

119. Anker continued to make these misrepresentations of material facts up until December 8, 2022, when these material misrepresentations were made public.

120. At the time, Anker either knew or should have known it was making misrepresentations of material facts or made the representations without knowledge of their truth or falsity.

121. Anker's misrepresentations were made with the intent to induce consumers to purchase its products over Anker's competitors who did not provide these privacy/safety features.

122. These misrepresentations of fact concerned the type of information upon which Plaintiff and other reasonable consumers would be expected to rely in making their decisions to purchase Anker's products.

123. Consequently, Plaintiff and the Florida Subclass have suffered injury by purchasing Anker's products and not receiving what was advertised.

WHEREFORE, Plaintiff, on behalf of himself and those similarly situated, requests this Court enter judgment in their favor and against Anker for compensatory damages, costs, and such other relief as this Court deems just and proper.

COUNT IV – UNJUST ENRICHMENT
(On behalf of Plaintiff and the Florida Subclass)

124. Plaintiff incorporates by reference paragraphs 1 through 83 as though fully set forth herein.

125. Plaintiff and the Florida Subclass members conferred benefits upon Anker.

126. Plaintiff and the Florida Subclass members paid money for their eufy Security Cameras, which they would not have purchased or would not have purchased on the same terms,

had they known that their eufy Security Cameras shared data with cloud servers and lacked adequate data security.

127. Anker has unjustly retained the benefits conferred upon by Plaintiff and the Florida Subclass members.

128. Anker retained those benefits under circumstances that make it inequitable for Anker to retain such benefits.

129. Anker retained these benefits even though the eufy Security Cameras shared data with cloud servers and lacked adequate data security.

130. If Plaintiff and Florida Subclass members had known the true nature of the eufy Security Cameras, they would not have purchased the products.

WHEREFORE, Plaintiff, on behalf of himself and those similarly situated, requests this Court enter judgment in their favor and against Anker for compensatory damages, costs, costs, and such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a jury trial for any and all issues triable by a jury.

Respectfully submitted: January 6, 2023.

/s/ *Benjamin Widlanski*
Benjamin Widlanski, Esq.
Florida Bar No. 1010644
bwidlanski@kttlaw.com
Robert J. Neary, Esq.
Florida Bar No. 81712
rn@kttlaw.com
KOZYAK TROPIN & THROCKMORTON LLP
2525 Ponce de Leon Blvd., 9th Floor
Coral Gables, FL 33134
Tel: (305) 372-1800
Fax: (305) 372-3508

Counsel for Plaintiff and the putative Classes

/s/ *Daniel S. Maland*
Robert M. Stein, Esq.
Florida Bar No. 93936
rstein@rvmrlaw.com
Daniel S. Maland, Esq.
Florida Bar No. 114932
dmaland@rvmrlaw.com
RENNERT VOGEL MANDLER & RODRIGUEZ, P.A.
100 SE 2nd Street, 29th Floor
Miami, FL 33131
Tel: (305) 577-4177
Fax: (305) 376-6176

Counsel for Plaintiff and the putative Classes