

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

MATTHEW SCHOOLFIELD, on behalf of  
himself and all others similarly situated,

Plaintiff,

vs.

WYZE LABS, INC.,

Defendant.

NO.

**CLASS ACTION COMPLAINT FOR  
DAMAGES, EQUITABLE,  
DECLARATORY AND INJUNCTIVE  
RELIEF**

DEMAND FOR JURY TRIAL

Plaintiff Matthew Schoolfield (“Plaintiff”), individually, by and through his undersigned counsel, brings this class action lawsuit against Wyze Labs, Inc. (“Defendant,” or “Wyze”), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of his counsel as follows:

I. INTRODUCTION

1 “We’ve Always Taken Security Very Seriously, And We’re Devastated That We Let Our  
2 Users Down Like This”<sup>1</sup>

3 1. Wyze is a security and safety company that manufactures, markets and sells an  
4 array of home security cameras and accessories at prices significantly below competitive  
5 products such as those offered by Ring or Nest.

6 2. Wyze cameras are Wi-Fi enabled and controlled through an application on a  
7 user’s smart device. In order to use Wyze products, customers must provide, and allow Wyze to  
8 collect their personally identifiable information (“PII”).<sup>2</sup> Wyze subsequently assures users that  
9 it employs commercially reasonable security measures to prevent the loss, misuse or alteration  
10 of this information.

11 3. Despite this promise, however, and a correlative legal obligation to protect such  
12 information from misuse, Wyze exposed the sensitive PII of 2.4 million customers over a 23-  
13 day period, allowing an untold number of miscreants access to its customers’ valuable and  
14 private PII (“Data Breach”).

15 4. According to Twelve Security, the cyber security company that discovered the  
16 Data Breach, the exposed information resided on a cloud-based database owned by Wyze and  
17 included PII such as: usernames, email addresses, camera nicknames, device models, firmware  
18 information, Wi-Fi SSID details, API tokens for iOS and Android, and Alexa tokens. The  
19 database also included a huge array of health information including height, weight, bone  
20 density, and daily protein intake of Wyze users.

21 <sup>1</sup> See The Verge, December 30, 2019, available at  
22 <https://www.theverge.com/2019/12/30/21042974/wyze-server-breach-cybersecurity-smart-home-security-camera> (last visited February 5, 2020).

23 <sup>2</sup> PII generally incorporates information that can be used to distinguish or trace an individual's  
24 identity, either alone or when combined with other personal or identifying information 2 CFR  
25 § 200.79. At a minimum, it includes all information that on its face expressly identifies an  
26 individual. PII also is generally defined to include certain identifiers that do not on their face  
27 name an individual, but that are considered to be particularly sensitive and/or valuable if in the  
wrong hands.

1           5.       Not only does the exposed data make Wyze customers more susceptible to  
2 identity theft and financial fraud in the future, it is now possible for any individual anywhere in  
3 the world to access the live video feeds of every single Wyze camera that was online.

4           6.       Plaintiff, on behalf of all others similarly situated, alleges claims for negligence,  
5 invasion of privacy, breach of implied contract, breach of implied warranty and unjust  
6 enrichment. In addition, Plaintiff seeks damages, injunctive and declaratory relief.

7  
**II. PARTIES**

8           7.       Plaintiff Matthew Schoolfield is a resident of Tarrant County, Texas. He  
9 purchased a Wyze camera for his house in December 2018 for approximately \$34.99. Once Mr.  
10 Schoolfield was notified of the breach, he immediately changed his password. As a result of the  
11 Data Breach, Mr. Schoolfield remains concerned about the safety and security of his family, the  
12 integrity of his PII that he provided to, and was collected by, Wyze, and the fact that his camera  
13 may now be accessible to unauthorized users. Mr. Schoolfield continues to spend time  
14 addressing these safety concerns—time he would not otherwise have to spend but for the Data  
15 Breach.

16           8.       Defendant Wyze Labs, Inc. makes budget smart home-security cameras and  
17 accessories including the Wyze Cam, Cam Pan, Lock, Sense and Bulb. It is a Delaware  
18 corporation with its principal place of business at 4030 Lake Washington Blvd., Suite 200,  
19 Kirkland, Washington, 98033.

20  
**III. JURISDICTION AND VENUE**

21           9.       This Court has subject matter jurisdiction over this action under the Class Action  
22 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive  
23 of interest and costs. There are millions of putative class members, many of whom have  
24 different citizenship from Defendant.  
25  
26  
27

1 10. This Court has jurisdiction over the Defendant which operates in this District.  
2 Through its business operations in this District, Defendant intentionally avails itself of the  
3 markets within this District to render the exercise of jurisdiction by this Court just and proper.

4 11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a  
5 substantial part of the events and omissions giving rise to this action occurred in this District  
6 and Wyze is headquartered in this District.

7 **IV. STATEMENT OF FACTS**

8 **A. Wyze Products and Wi-Fi Connectivity**

9 12. Wyze sells a series of smart home products, including the Wyze Cam wireless  
10 smart home camera, Wyze Cam Pan wireless smart home camera, and Wyze Sense smart  
11 sensor (collectively “Wyze Products”). They are connected to the internet and allow users to  
12 view information captured by the Wyze Products. For example, Wyze Cam and Wyze Pan  
13 cameras can record 12-second alert videos, display a live video/audio stream, and enable two-  
14 way audio between users and the camera.



21 13. Wyze Products communicate with users through the Wyze application (“App”)  
22 and its software platform. To use a Wyze Product, users must: (a) download the Wyze App and  
23 install it on a smart phone, tablet, or other compatible device; (b) register for an account by  
24 providing an email/user name and password; (c) provide personally identifiable information  
25 and consent to its collection and proper use by Wyze; (d) associate Wyze Products to the App  
26 and user account; (e) provide Wi-Fi network information to connect Wyze Products to the  
27

1 Internet; and (f) adjust settings for each connected Wyze Product to enable desired  
2 functionality.

3 14. In addition to PII provided directly from the user as a precondition for using  
4 Wyze Products, Wyze collects a wide array of additional confidential PII including: (a)  
5 information that identifies, relates to, describes, is reasonably capable of being associated with  
6 or reasonably can be used to identify an individual or household and other data that is linked to  
7 personal data, and includes App Account and App Login information; (b) setup information  
8 and settings; (c) information generated by Wyze Products that is sent to the Wyze Cloud, such  
9 as videos from a Wyze camera, status notifications from a Wyze Sense, and device location  
10 information; (d) technical information about each enabled Wyze Product, such as its device  
11 model, serial number, MAC address, firmware version, the SSID of user wireless network,  
12 device name, device connectivity status, and IP address (“Device Technical Information”); and  
13 (e) records, data and statistics generated by use of the Wyze Product and App collected by  
14 Wyze Labs (“Usage Data”), such as the instances that the Wyze Cloud authenticated a user’s  
15 App or Wyze Product, and the times a user contacted customer support.<sup>3</sup>

16 15. Wyze specifically limits how such sensitive information will be utilized and  
17 assures users of its Products, website, and App that their PII will remain secure and used only  
18 for intended purposes by Wyze and selected affiliates. Wyze further claims to “employ[]  
19 security measures to prevent the loss, misuse or alteration of information collected....”<sup>4</sup>

20 16. Despite these promises, the sensitive personally identifiable information of  
21 Wyze’s 2.4 million customers was publicly exposed for more than 3 weeks in December 2019.<sup>5</sup>

---

22  
23 <sup>3</sup> See <https://wyze.com/privacy-statement-wyze-products#a2> (last visited February 5, 2020).

24 <sup>4</sup> See <https://wyze.com/privacy-statement-wyze-site-2019-05-08>; <https://wyze.com/privacy-statement-wyze-products> (last visited February 5, 2020).

25  
26 <sup>5</sup> See Twelve Security, December 26, 2019, available at <https://blog.12security.com/wyze-essay-2-aresflare/> (last visited February 5, 2020).

1 **B. The Wyze Data Breach**

2 17. On December 26, 2019, the cybersecurity firm Twelve Security revealed on its  
3 blog that the personal data of 2.4 million Wyze users had been publicly exposed from  
4 December 4, through December 27, 2019.<sup>6</sup> “Personally, in my ten years of sysadmin and cloud  
5 engineering . . . I never encountered a breach of this magnitude. . . . In this case, both the  
6 company’s production databases were left entirely open to the internet. A significant amount of  
7 sensitive information generated by 2.4 million users, all coincidentally outside of China, was  
8 the result.” *Id.*

9 18. The exposed information included:

- 10 a. Username and email of those who purchased cameras and then  
11 connected them to their home;
- 12 b. Email of anyone with whom a user ever shared camera access, such as a  
13 family member;
- 14 c. Lists of all cameras in the home, the nicknames for each camera, device  
15 model and firmware;
- 16 d. Wi-Fi SSID, internal subnet layout, last on time for cameras, last login  
17 time from app, last logout time from the app;<sup>7</sup>
- 18 e. API Tokens for access to the user account from any iOS or Android  
19 device;
- 20 f. Alexa Tokens for 24,000 users who have connected Alexa devices to  
21 their Wyze camera;
- 22 g. Height, Weight, Gender, Bone Density, Bone Mass, Daily Protein  
23 Intake, and other health information for a subset of users.

24 \_\_\_\_\_  
25 <sup>6</sup> See Twelve Security, December 26, 2019, available at <https://blog.12security.com/wyze/> (last  
26 visited February 5, 2020).

27 <sup>7</sup> SSID is short for service set identifier, the name for a Wi-Fi network.

1 19. Importantly, the tokens (*i.e.*, API Tokens and Alexa Tokens) exposed in the  
2 Data Breach allow, depending on the permissions levels, malicious actors to access potentially  
3 a user’s entire account and all of the information inside that account, expanding the exposure.

4 20. The Twelve Security Blog concluded, “[g]iven this, they owe us an explanation.  
5 The database is currently live and open. Anyone can access it.” *Id.*

6 21. “Just *one* of those bullet points would be enough for concern, but the volume of  
7 compromised user data is staggering—if true. If you use any of Wyze’s products, you need to  
8 change your password and update your security options immediately so that no one can break  
9 into your account using leaked info. (You might also want to manually log out of your account  
10 and log back in, and make sure you disable and reenable any connected services, if  
11 applicable).”<sup>8</sup>

12 22. With the exposed data, “it is [now] possible for any individual anywhere in the  
13 world to access the live video feeds of every single Wyze camera that was online.”<sup>9</sup>

14 23. Not only has the privacy of Wyze Product users been unacceptably  
15 compromised and their PII exposed, the ongoing possibility of their data being used to further  
16 compromise their Wyze camera, renders those products useless for their intended purposes.

17 **C. Wyze’s Response**

18 24. On December 31, 2019, Wyze issued the following response to its users:

19 Wyze Users,

20 There is nothing we value higher than trust from our users. In fact,  
21 our entire business model is dependent on building long-term trust  
22 with customers that keep coming back.

23 We are reaching out to you because we’ve made a mistake in  
24 violation of that trust. On December 26th, we discovered

25 <sup>8</sup> See <https://lifehacker.com/how-to-protect-your-wyze-account-after-the-recent-data-1840727973> (last visited February 5, 2020).

26 <sup>9</sup> See <https://blog.12security.com/wyze-essay-2-aresflare/> (last visited February 5, 2020).

1 information in some of our non-production databases was  
2 mistakenly made public between December 4th - December 26th.  
3 During this time, the databases were accessed by an unauthorized  
4 party.

5 The information did not contain passwords, personal financial  
6 data, or video content.

7 The information did contain Wyze nicknames, user emails, profile  
8 photos, Wi-Fi router names, a limited number of Alexa integration  
9 tokens, and other information detailed in the link below.

10 If you were a user with us before we secured this information on  
11 December 26th, we regretfully write this email as a notification  
12 that some of your information was included in these databases. If  
13 you are receiving this email and joined us after December 26th, we  
14 write this email because you use our products and deserve to know  
15 how your data is being handled.

16 Upon finding out about the public user data, we took immediate  
17 action to secure it by closing any databases in question, forcing all  
18 users to log in again to create new access tokens, and requiring  
19 users to reconnect Alexa, Google Assistant, and IFTTT  
20 integrations. You can read in more detail about the data leak and  
21 the actions we took at this link:  
22 <https://forums.wyzecam.com/t/updated-12-30-19-data-leak-12-26-2019>

23 As an additional security measure, we recommend that you reset  
24 your Wyze account password. Again, no passwords were  
25 compromised, but we recommend this as a standard safety  
26 measure. You may also add an additional level of security to your  
27 account by implementing two-factor authentication inside of the  
28 Wyze app. Finally, please be watchful for any phishing attempts.  
29 Especially watch any communications coming from Wyze and  
30 ensure they come from official @wyze.com and @wyzecam.com  
31 email addresses.

32 We are deeply sorry for this oversight. We promise to learn from  
33 this mistake and will make improvements going forward. This will  
34 include enhancing our security processes, improving  
35 communication of security guidelines to all Wyze employees, and  
36 making more of our user-requested security features our top  
37 priority in the coming months. We are also partnering with a third-  
38 party cyber security firm to audit and improve our security  
39 protocols.



1 As we continue our investigation into what happened, we will post  
2 future updates to the forum link above. More details will follow  
3 and we appreciate your patience during this process. Please reach  
4 out with any questions or concerns to our customer support team  
5 by going to support.wyze.com.

6 Sincerely,

7 Yun Zhang

8 CEO @ Wyze<sup>10</sup>

9 25. “We didn’t properly communicate and enforce our security protocols to new  
10 employees,” said Mr. Dongsheng Song, co-founder of Wyze. “We should have built controls,  
11 or a more robust tool and process to make sure security protocols are followed,” he added.<sup>11</sup>

12 26. “Our whole business model is built on trust,” added Dave Crosby Wyze co-  
13 founder. “It was an accident” for which “[w]e are very, very sorry and taking it very seriously.”

14 *Id.*

#### 15 **D. Wyze Failed To Comply With FTC Requirements**

16 27. The Federal Trade Commission (“FTC”) has issued numerous guidelines for  
17 businesses highlighting the importance of reasonable data security practices. According to the  
18 FTC, the need for data security should be factored into all business decision-making.<sup>12</sup>

19 28. In 2016, the FTC updated its publication, *Protecting Personal Information: A  
20 Guide for Business*, which established guidelines for fundamental data security principles and

21  
22 <sup>10</sup> See <https://forums.wyzecam.com/t/updated-01-06-20-data-leak-12-26-2019/79046> (last  
23 visited February 5, 2020).

24 <sup>11</sup> See <https://www.nytimes.com/2019/12/30/business/wyze-security-camera-breach.html> (last  
25 visited February 5, 2020).

26 <sup>12</sup> See Federal Trade Commission, *Start With Security*, available at  
27 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last  
visited February 5, 2020).

1 practices for business.<sup>13</sup> The guidelines note businesses should protect the personal customer  
2 information that they keep; properly dispose of personal information that is no longer needed;  
3 encrypt information stored on computer networks; understand their network's vulnerabilities;  
4 and implement policies to correct security problems.

5 29. The FTC has brought enforcement actions against businesses for failing to  
6 adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate  
7 measures to protect against unauthorized access to confidential consumer data as an unfair act  
8 or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C.  
9 § 45. Orders resulting from these actions further clarify the measures businesses must take to  
10 meet their data security obligations.

11 30. Wyze's failure to employ reasonable and appropriate measures to protect against  
12 unauthorized access to confidential consumer data constitutes an unfair act or practice  
13 prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

14 **E. Plaintiff and Class Members Suffered Damages**

15 31. PII in all its forms has become a valuable commodity among computer hackers.  
16 Once acquired, it is quickly sold on the black market where it can often be re-traded among  
17 miscreants for years. As the FTC recognizes, with PII, identity thieves can commit an array of  
18 crimes, the ramifications of which can be long lasting and severe.

19 32. There often is a time lag between when harm occurs versus when it is  
20 discovered, as well as between when PII is stolen and when it is used. According to the U.S.  
21 Government Accountability Office ("GAO"), which conducted a study regarding data breaches  
22 found that stolen data may be held for years before being used to commit identity theft.

---

25 <sup>13</sup>See Federal Trade Commission, *Protecting Personal Information: A Guide for Business*,  
26 available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-  
personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited February 5, 2020).

1           33.     The PII belonging to Plaintiff and Class Members is private and sensitive in  
2 nature and was left inadequately protected by the Defendant. Defendant did not obtain  
3 Plaintiff's or Class Members' consent to disclose their PII to any other person as required by  
4 applicable law and industry standards.

5           34.     The Data Breach was a direct and proximate result of Defendant's failure to  
6 properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access,  
7 use, and disclosure, as required by various state and federal regulations, industry practices, and  
8 the common law.

9           35.     Defendant had the resources necessary to properly secure the PII acquired from  
10 its users but neglected to do so. Had Defendant taken such steps and adopted basic security  
11 measures, it would have prevented the Data Brach and the exposure of Plaintiff's and Class  
12 Members' PII.

13           36.     As a direct and proximate result of Defendant's wrongful actions and inactions,  
14 Plaintiff and Class Members have been placed at an imminent, immediate, and continuing  
15 increased risk of harm from malicious third parties who gained unauthorized access to their PII.

16           37.     As a direct and proximate result of Defendant's wrongful actions and inactions,  
17 Plaintiff and Class Members have been placed at an imminent, immediate, and continuing  
18 increased risk of harm from identity theft and fraud, requiring them to take the time which they  
19 otherwise would have dedicated to other life demands such as work and family in an effort to  
20 mitigate the actual and potential impact of the Data Breach on their lives.

21           38.     As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and  
22 Class Members have suffered, will suffer, or are at increased risk of suffering:

- 23                   a.    The compromise, publication, theft and/or unauthorized use of their PII;  
24                   b.    Out-of-pocket costs associated with the prevention, detection, recovery  
25                         and remediation from identity theft or fraud;

- 1 c. Lost opportunity costs and lost wages associated with efforts expended  
2 and the loss of productivity from addressing and attempting to mitigate  
3 the actual and future consequences of the Data Breach, including but not  
4 limited to efforts spent researching how to prevent, detect, contest and  
5 recover from identity theft and fraud;
- 6 d. The continued risk to their PII, which remains in the possession of  
7 Defendant and is subject to further breaches so long as Defendant fails to  
8 undertake appropriate measures to protect the PII in its possession; and
- 9 e. Current and future costs in terms of time, effort and money that will be  
10 expended to prevent, detect, contest, remediate and repair the impact of  
11 the Data Breach for the remainder of the lives of Plaintiff and Class  
12 Members.

13 **V. CLASS ACTION ALLEGATIONS**

14 39. Plaintiff seeks relief on behalf of himself and as representative of all others who  
15 are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff  
16 seeks certification of a Nationwide class defined as follows:

17 All persons in the United States who purchased Wyze Products  
18 within the applicable statute of limitations periods (the “Class”).

19 40. Excluded from the Class are Wyze and any of its affiliates, parents or  
20 subsidiaries; all persons who make a timely election to be excluded from the Class; government  
21 entities; and the judges to whom this case is assigned, their immediate families, and court staff.

22 41. Plaintiff hereby reserves the right to amend or modify the class definitions with  
23 greater specificity or division after having had an opportunity to conduct discovery.

24 42. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2),  
25 (b)(3) and (c)(4).  
26  
27

1           43.     **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the  
2 members of the Class are so numerous and geographically dispersed that the joinder of all  
3 members is impractical. The Data Breach exposed the PII of 2.4 million Wyze customers.  
4 Wyze has physical and/or email addresses for Class Members who therefore may be notified of  
5 the pendency of this action by recognized, Court-approved notice dissemination methods,  
6 which may include U.S. mail, electronic mail, internet postings, and/or published notice.

7           44.     **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule  
8 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions  
9 of law and fact that predominate over any questions affecting individual Class Members. The  
10 common questions include:

- 11                   a. Whether Wyze's security measures and protocols to protect customer PII  
12                   were reasonable;
- 13                   b. Whether Wyze was negligent in failing to implement reasonable and  
14                   adequate security procedures and practices;
- 15                   c. Whether Wyze's failure to implement adequate security measures  
16                   resulted in the unlawful exposure of customer PII;
- 17                   d. Whether Plaintiff and Class Members were injured and suffered damages  
18                   or other losses because of Wyze's failure to reasonably secure and  
19                   protect their PII; and
- 20                   e. Whether Plaintiff and Class Members are entitled to relief.

21           45.     **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's  
22 claims are typical of those of other Class Members. Plaintiff is a purchaser of a Wyze Product,  
23 registered with Wyze through its App, and in so doing provided Wyze his PII. Plaintiff's  
24 damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with  
25 the relief sought by the Class.

1           46.       **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is  
2 an adequate representative of the Class because Plaintiff is a member of the Class he seeks to  
3 represent; is committed to pursuing this matter against Wyze to obtain relief for the Class; and  
4 has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and  
5 experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends  
6 to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

7           47.       **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class  
8 action is superior to any other available means for the fair and efficient adjudication of this  
9 controversy, and no unusual difficulties are likely to be encountered in the management of this  
10 class action. The quintessential purpose of the class action mechanism is to permit litigation  
11 against wrongdoers even when damages to an individual plaintiff may not be sufficient to  
12 justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively  
13 small compared to the burden and expense required to individually litigate their claims against  
14 Wyze, and thus, individual litigation to redress Wyze's wrongful conduct would be  
15 impracticable. Individual litigation by each Class member would also strain the court system.  
16 Individual litigation creates the potential for inconsistent or contradictory judgments and  
17 increases the delay and expense to all parties and the court system. By contrast, the class action  
18 device presents far fewer management difficulties and provides the benefits of a single  
19 adjudication, economies of scale, and comprehensive supervision by a single court.

20           48.       **Injunctive and Declaratory Relief.** Class certification is also appropriate under  
21 Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds  
22 generally applicable to the Class as a whole, making injunctive and declaratory relief  
23 appropriate to the Class as a whole.

24           49.       Likewise, particular issues under Rule 23(c)(4) are appropriate for certification  
25 because such claims present only particular, common issues, the resolution of which would  
26 advance the disposition of this matter and the parties' interests therein.

27

1 50. Finally, all members of the proposed Classes are readily ascertainable. Wyze has  
2 access to customer names and addresses. Using this information, Class Members can be  
3 identified and ascertained for the purpose of providing notice.

4 **FIRST CAUSE OF ACTION**

5 **NEGLIGENCE**

6 51. Plaintiff restates and realleges the paragraphs above as if fully set forth herein.

7 52. Defendant had full knowledge of the purpose for which its Products, especially  
8 its security cameras, were being used and the sensitivity of the people and things the cameras  
9 were designed to secure and protect. Defendant also knew the types of harm that Plaintiff and  
10 Class Members could and would suffer if the integrity of their PII were compromised.

11 53. Defendant had a duty to exercise reasonable care in ensuring its customer PII  
12 was secure and inviolable by unauthorized parties. This duty includes, among other things,  
13 ensuring that reasonable and proper protocols and safeguards were in place to protect the  
14 integrity of customer PII entrusted to it.

15 54. Plaintiff and Class Members were the foreseeable and probable victims of any  
16 inadequate security practices. Defendant knew of or should have known of the inherent risks of  
17 exposing customer PII without adequate security protocols and safeguards.

18 55. Plaintiff and the Class Members had no idea their PII was not properly secured  
19 and was vulnerable to exposure and misappropriation.

20 56. In contrast, Defendant was in a position to protect against the harm suffered by  
21 Plaintiff and Class Members and had a duty to do so.

22 57. Defendant, through its actions, unlawfully breached its duty to Plaintiff and  
23 Class Members by failing to ensure its cyber protocols and procedures were sufficiently robust  
24 to protect customer PII from exposure and unauthorized use.

25 58. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff  
26 and Class Members, Plaintiff and Class Members' PII would not have been exposed.  
27

1 59. As a result of Defendant’s negligence, Plaintiff and the Class Members have  
2 suffered and will continue to suffer damages and injury including, but not limited to: the cost of  
3 replacement cameras; cost of additional surveillance and protective devices and services; time  
4 spent monitoring and addressing the current and future consequences of the exposure created  
5 by Wyze; and the necessity to engage legal counsel and incur attorneys’ fees, costs and  
6 expenses.

7 **SECOND CAUSE OF ACTION**

8 **NEGLIGENCE *PER SE***

9 60. Plaintiff restates and realleges the paragraphs above as if fully set forth herein.

10 61. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting  
11 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by  
12 businesses, such as Wyze, of failing to use reasonable measures to protect PII. The FTC  
13 publications and orders described above also form part of the basis of Defendant’s duty in this  
14 regard.

15 62. Wyze violated Section 5 of the FTC Act by failing to use reasonable measures to  
16 protect patient PII and not complying with applicable industry standards, as described in detail  
17 herein. Wyze’s conduct was particularly unreasonable given the nature and amount of PII it  
18 obtained and stored, and the foreseeable consequences of a data breach including, specifically,  
19 the damages that would result to Plaintiff and Class Members.

20 63. Wyze’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

21 64. Plaintiff and Class Members are within the class of persons that the FTC Act  
22 was intended to protect.

23 65. The harm that occurred as a result of the Data Breach is the type of harm the  
24 FTC Act was intended to guard against. The FTC has pursued enforcement actions against  
25 businesses, which, as a result of their failure to employ reasonable data security measures and  
26  
27



1 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the  
2 Class.

3 66. As a direct and proximate result of Wyze's negligence *per se*, Plaintiff and the  
4 Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach  
5 including, but not limited to: damages from lost time and effort to mitigate the actual and  
6 potential impact of the Data Breach on their lives.

7 67. Additionally, as a direct and proximate result of Wyze's negligence *per se*,  
8 Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of  
9 their PII, which remains in Wyze's possession and is subject to further unauthorized disclosures  
10 so long as Wyze fails to undertake appropriate and adequate measures to protect the PII in its  
11 continued possession.

### 12 **THIRD CAUSE OF ACTION**

#### 13 **INVASION OF PRIVACY**

14 68. Plaintiff restates and realleges the paragraphs above as if fully set forth herein.

15 69. Plaintiff and Class Members had a legitimate expectation of privacy with respect  
16 to their PII as well as the people, location and subject matter of what their Wyze Products were  
17 observing and were accordingly entitled to the protection of this information against disclosure  
18 to unauthorized third parties.

19 70. Defendant owed a duty to its customers, including Plaintiff and Class Members,  
20 to ensure that the PII it was given and which it gathered from customers remained confidential  
21 and secure.

22 71. The failure to ensure the integrity of Plaintiff and Class Members' PII is highly  
23 offensive to a reasonable person.

24 72. The intrusion was into a place or thing, which was private and is entitled to be  
25 private. Plaintiff and Class Members purchased and used Wyze Products with the expectation  
26 that their PII, provided to and gathered by Wyze, including but not limited to the people, places  
27

1 and information seen and heard by Wyze cameras, would remain private and would not be  
2 disclosed without authorization.

3 73. The failure to ensure customer PII is properly protected constitutes intentional  
4 interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to  
5 their persons or as to their private affairs or concerns, of a kind that would be highly offensive  
6 to a reasonable person.

7 74. Defendant acted with a knowing state of mind when it collected customer PII,  
8 despite knowing its security practices were inadequate.

9 75. Acting with this knowledge, Defendant had notice and knew that its inadequate  
10 security practices would cause injury to Plaintiff and Class Members.

11 76. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class  
12 Members' privacy was violated causing Plaintiff and Class Members to suffer damages.

13 77. Unless and until enjoined, and restrained by order of this Court, Defendant's  
14 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class  
15 Members.

16 78. Plaintiff and Class Members have no adequate remedy at law for the injuries in  
17 that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the  
18 Class.

19 **FOURTH CAUSE OF ACTION**  
20 **BREACH OF IMPLIED CONTRACT**

21 79. Plaintiff restates and realleges the paragraphs above as if fully set forth herein.

22 80. Defendant sold Wyze Products to Plaintiff and Members of the Class for which  
23 it received a benefit in the form of monetary payment.

24 81. Defendant has acknowledged the benefit and accepted or retained the benefit  
25 conferred.

26 82. Plaintiff and Class Members were required to provide their PII to Defendant as a  
27 condition of their use of Defendant's services.

1           83. Plaintiff and Class Members paid money to Defendant in exchange for Wyze  
2 Products and services, along with Defendant's promise to protect their PII from unauthorized  
3 disclosure.

4           84. Implicit in the agreement between Plaintiff and Class Members and the  
5 Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes  
6 only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the  
7 PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all  
8 unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of  
9 Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only  
10 under conditions that kept such information secure and confidential.

11           85. Without such implied contracts, Plaintiff and Class Members would not have  
12 provided their PII to Defendant.

13           86. Plaintiff and Class Members fully performed their obligations under the implied  
14 contract with Defendant, however, Defendant did not.

15           87. Defendant breached the implied contracts with Plaintiff and Class Members by  
16 failing to acknowledge the inherent vulnerability in its cyber security systems and protocols.  
17 These circumstances are such that it would be inequitable for Defendant to retain the benefit  
18 received.

19           88. As a direct and proximate result of Defendant's breach of its implied contracts  
20 with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer  
21 injury, including but not limited to: the cost of replacement cameras; the cost of additional  
22 surveillance and protective devices and services; and time spent monitoring, addressing the  
23 current and future consequences of the exposure enabled by Wyze.

**FIFTH CAUSE OF ACTION**

**UNJUST ENRICHMENT**

1  
2  
3 89. Plaintiff restates and realleges the paragraphs above as if fully set forth  
4 herein.

5 90. As the intended and expected result of its conscious wrongdoing, Defendant has  
6 profited and benefited from the purchase of the Product by Plaintiff and the Class.

7 91. Defendant has voluntarily accepted and retained these profits and benefits, with  
8 full knowledge and awareness that, as a result of Defendant's misconduct, Plaintiff and the  
9 Class did not receive Product of the quality, nature, fitness, or value that had been represented  
10 by Defendant, and that reasonable consumers expected.

11 92. Defendant has been unjustly enriched by its fraudulent and deceptive  
12 withholding of benefits to Plaintiff and the Class at the expense of these parties.

13 93. Equity and good conscience militate against permitting Defendant to retain these  
14 profits and benefits.

15 94. As a direct and proximate result of Defendant's unjust enrichment, Plaintiff and  
16 Class Members suffered injury and seek an order directing Defendant's disgorgement and the  
17 return to Plaintiff and the classes of the amount each improperly paid to Defendant.

18 **VI. PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated,  
20 respectfully requests the following relief:

- 21 a. An Order certifying this case as a class action;  
22 b. An Order appointing Plaintiff as the class representative;  
23 c. An Order appointing undersigned counsel as class counsel;  
24 d. A mandatory injunction directing the Defendant to hereinafter  
25 adequately safeguard the PII of the Class by implementing improved  
26 security procedures and measures;  
27

- e. An award of damages;
- f. An award of costs and expenses;
- g. An award of attorneys' fees; and
- h. Such other and further relief as this court may deem just and proper.

**VII. DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial as to all issues triable by a jury.

RESPECTFULLY SUBMITTED AND DATED this 21st day of February, 2020.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759  
Beth E. Terrell, WSBA #26759  
Email: bterrell@terrellmarshall.com

By: /s/ Adrienne D. McEntee, WSBA #34061  
Adrienne D. McEntee, WSBA #34061  
Email: amcentee@terrellmarshall.com  
936 North 34th Street, Suite 300  
Seattle, Washington 98103-8869  
Telephone: (206) 816-6603  
Facsimile: (206) 319-5450

*Attorneys for Plaintiff and the Proposed Class*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

MATTHEW SCHOOLFIELD

(b) County of Residence of First Listed Plaintiff Tarrant County, Texas (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number) Beth E. Terrell, WSBA #26759, Email: bterrell@terrellmarshall.com. Terrell Marshall Law Group PLLC, 936 North 34th Street, Suite 300, Seattle, Washington 98103 (206) 816-6603

DEFENDANTS

WYZE LABS, INC.

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and business location (Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation).

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)(2)

Brief description of cause: Class Action Fairness Act

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$

CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE DOCKET NUMBER

DATE 02/21/2020 SIGNATURE OF ATTORNEY OF RECORD /s/ Beth E. Terrell, WSBA #26759

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

## INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

### Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.  
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.  
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.  
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.  
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.  
 Original Proceedings. (1) Cases which originate in the United States district courts.  
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.  
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.  
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.  
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.  
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.  
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.  
**PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.  
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.  
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Western District of Washington

MATTHEW SCHOOLFIELD on behalf of himself and
all others similarly situated,

Plaintiff(s)

v.

WYZE LABS, INC.,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

WYZE LABS, INC.
c/o VCORP SERVICES, LLC, Registered Agent
1013 Centre Road, Suite 403-B
Wilmington, Delaware 19805

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Beth E. Terrell, WSBA #26759
TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (206) 816-6603
Facsimile: (206) 319-5450

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk



Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*:

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Wyze Labs Hit with Class Action Over Three-Week 2019 Data Breach Affecting 2.4 Million Customers](#)

---