

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SUMMER CHRISTINE DUFFIELD, on
behalf of herself and all others similarly
situated,

Plaintiff,

v.

THE WALT DISNEY COMPANY and
DISNEY DTC LLC,

Defendants.

X

:

:

:

:

:

:

:

:

:

:

:

:

X

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff SUMMER CHRISTINE DUFFIELD, (“Plaintiff”) brings this class action complaint (the “Action”) on behalf of herself and all others similarly situated under state and common law against Defendants THE WALT DISNEY COMPANY and DISNEY DTC LLC (collectively, the “Defendant” or “Disney”) for violations of state, and common law upon personal knowledge as to herself and her own actions, upon information and belief and upon the investigation of counsel, seeking actual damages, statutory damages, restitution, disgorgement of profit into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys’ fees, a declaratory judgment, injunctive relief and any other relief this Court deems just and proper, and alleges as follows:

INTRODUCTION

1. Plaintiff and Class members are adults and minor children during the statutory period through the present day (the “Class Period”) who visited one of Disney’s theme parks and had their biometric information – in the form of facial recognition templates (the “biometric information”) – in violation of privacy laws and without adequate consent (the “Class”).

2. By way of background, Disney is ubiquitous and has theme parks located in California and Florida, these theme parks include Walt Disney World (which is in Florida), Disneyland Park (which is in California), and Disney California Adventure Park (which is also in California) (collectively, the “Disney Theme Parks”). Plaintiff visited both on May 10, 2026.

3. Beginning as late as April 28, 2026, Disney began to implement facial recognition collection at entrances of the Disney Theme Parks which are located in California.¹ Unfortunately, for visitors of Disney Theme Parks, including Plaintiff Duffield and Class members, they have no idea whatsoever that their biometrics – data which are more permanent

¹ <https://privacy.thewaltdisneycompany.com/en/resortfr/>, (last accessed May 10, 2026).

than a Social Security number and which cannot be changed or altered – were collected without adequate consent. In fact, Disney does not adequately disclose the use of their biometric collection, so consumers – which almost always include children – have no idea that Disney is collecting this highly sensitive data. Indeed, according to the LA Times, “[m]ost visitors opt into the technology over alternative entrances, [] unaware of the policy. Some express concern, especially parents worried about their children’s privacy.”²

4. Guests should be able to expressly opt in to this type of sensitive facial recognition technology with written consent – the onus of privacy rights should not be on the victim. Given how sensitive facial recognition data is, explicit written consent should be required to protect the privacy guests at Disney Theme Parks, like Plaintiff Duffield.

5. Further, Disney’s popularity compounds these issues because of how ubiquitous Disney Theme Parks are, as well as the experiences that are tailored around them. While Disney publicly states “[t]he security, integrity, and confidentiality of your information are extremely important to us, no security measures are perfect or impenetrable,”³ it appears visitors cannot discern which of the entrances into Disney Theme Parks actually are the ones to clearly avoid to “opt-out” of facial recognition.⁴ Disturbingly, Disney states that it collects facial recognition from children so long as they have consent of their parent – but children, who are the primary visitors at Disney Theme Parks, cannot consent to such a profound invasion of privacy given they cannot

² <https://www.latimes.com/california/story/2026-04-28/disneyland-rolls-out-facial-recognition-at-park-entrances-heres-how-it-works>, (last accessed May 14, 2026).

³ <https://nypost.com/2026/04/23/lifestyle/disneyland-loosens-up-on-facial-recognition-upon-theme-park-entry/>, (last accessed May 10, 2026).

⁴ https://techstory.in/security-news-disneyland-california-rolls-out-facial-recognition-entry-systems/#google_vignette, (last accessed May 10, 2026).

consent to contract away their privacy rights.⁵ Disney’s sophistication as a corporation and Disney’s cognizance of facial recognition laws should be well known – in fact, Disney admits as such, as they claim not to collect biometric information from visitors for other Disney purposes which are from “Illinois, Portland, Oregon, Washington, Nevada, and Texas.”⁶ Notably, Illinois, Portland, Oregon, Washington, Nevada, and Texas are all states or jurisdictions which have strict biometric privacy laws – which is presumptively why Disney does not and will not offer certain services in those states.⁷ Disney even states that those who “opt-out” of biometric information collection “may still have their photographs taken” – but photographs are always the basis for facial recognition data collection.⁸

6. Finally, Disney claims not to retain any biometric data after 30 days. However, as the LA Times reports, the images of visitors which are run through facial recognition technology are re-compared with pictures taken when a customer first use their ticket or an annual pass – which would suggest this 30-day retention policy is a farce.⁹

7. Consumer privacy laws are codified to protect consumers from this type of behavior, including those of children, especially given how sensitive biometric information is.

⁵ <https://privacy.thewaltdisneycompany.com/en/resortfr/>, (last accessed May 10, 2026).

⁶ <https://disneyworld.disney.go.com/photopass-terms-conditions/>, (last accessed May 10, 2026).

⁷ See, the Illinois Biometric Information Privacy Act (“BIPA”) (Illinois); Chapter 34.10 (Private Entity Shall Not Use Facial Recognition in Places of Public Accommodation) (Portland, Oregon); Chapter 19.375 RCW (Agency Ban on Collect, Capture, Purchase, or Otherwise Obtain a Biometric Identifier without Notice and Individual Consent) (Washington); Nevada’s Consumer Health Data Privacy Law, NRS: Chapter 603A (Nevada); and Texas’ Capture or Use of Biometric Identifier Act (“CUBI”) (Texas).

⁸ <https://www.helpnetsecurity.com/2026/05/07/disney-facial-recognition-entrance-lanes/>, (last accessed May 10, 2026); <https://privacy.thewaltdisneycompany.com/en/resortfr/>, (last accessed May 10, 2026).

⁹ <https://www.latimes.com/california/story/2026-04-28/disneyland-rolls-out-facial-recognition-at-park-entrances-heres-how-it-works>, (last accessed May 14, 2026).

8. At bottom, this is especially true here, where parents did not anticipate, invite or adequately consent to the presence of Disney collecting their unchangeable biometric information when attending Disney's Disney Theme Parks – places which are allegedly the safest place to bring their children and families for (expensive) outings. This issue is compounded by the fact that Disney does not disclose the collection of biometric information anywhere in their Privacy Policy – but rather within patchworks of random website pages which offer little clarity as to what Disney is actually doing with Plaintiff and Class members' biometric information and other privacy rights. Disney's conduct has ignited a firestorm of privacy concerns in the media¹⁰ and is entirely consistent with the type of behavior that violates guidance under the Article 5 of the Federal Trade Commissions' FTC Act.¹¹ As such, Disney invaded Plaintiff's and Class members' privacy rights.

9. Against this backdrop, Plaintiff Duffield, on behalf of herself and all others similarly situated seeks to rectify these harms under state, and common law causes of action, pursuing actual damages, statutory and/or liquidated damages, restitution, disgorgement of profit into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys' fees, a declaratory judgment, injunctive relief and any other relief this Court deems just and proper.

¹⁰ See, e.g. <https://www.helpnetsecurity.com/2026/05/07/disney-facial-recognition-entrance-lanes/>, (last accessed May 10, 2026).

¹¹ https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf, (last accessed May 10, 2026).

JURISDICTION AND VENUE

10. This action arises under federal, state and common law. Specifically, Plaintiff Duffield and Class members seek relief under the Class Action Fairness Act of 2005 (28 U.S.C. § 1332(d), *et seq.*), including: statutory and/or liquidated damages, costs of suit, reasonable attorneys' fees, as well as any other appropriate relief permitted by statute. With respect to state and common law violations, Plaintiff Duffield and Class members seek declaratory and injunctive relief, as well as a measure of damages (including punitive or exemplary damages, as well as statutory and trebled damages), disgorgement of profit into a constructive trust, costs of suit, pre- and post-judgment interest and reasonable attorneys' fees, as this Court deems necessary and proper.

11. *Subject Matter and Supplemental Jurisdiction.* Plaintiff brings this Action under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). Pursuant to CAFA, the amount in controversy well exceeds the sum of \$5,000,000 exclusive of interests and costs, there are over 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than at least one Defendant. Namely, Plaintiff Duffield is domiciled in California whereas one of the Defendants is headquartered in both California and New York.

12. *Personal Jurisdiction.* This Court has personal jurisdiction over the litigants because Defendant The Walt Disney Company maintains a co-headquarters in New York (which contains Defendant's technology-based, streaming, and video line of business operations), Defendant's acts or practices were directed toward this State (Defendant thus intentionally availed itself of this jurisdiction by choosing to do business here), Defendant is registered to do business in New York, and Defendant knew or should have known that their conduct as alleged herein

would impact minor children in this State, as their website is used throughout the United States, including here. Additionally, Defendant's data controller, Defendant Disney DTC LLC, chooses this forum for all conflicts as well as New York as its choice of law.

13. *Venue.* Venue is proper because the Defendant conducts business in this District, Defendant has a headquarters located in this District, because Class members were harmed here, and a substantial part of the events, acts and omissions giving rise to Class members' claims occurred here.

PARTIES

PLAINTIFF

Plaintiff Summer Christine Duffield

14. Plaintiff Duffield is domiciled in Riverside County, California.

15. During the Class Period, Plaintiff Duffield visited a Disney Theme Park and had her biometric information collected through the mechanism as described both above and below. Specifically, Plaintiff visited a Disney Theme Park on May 10, 2026 located in California and, without adequate consent, had her facial recognition template collected by Disney for use, processing, and retention.

16. Plaintiff Duffield has suffered the following from (1) the interception of her private and valuable biometric data without adequate consent, (2) the disclosure of her private and valuable data for purposes not clearly defined by the Disney Privacy Policy, and (3) the loss of value of her personal information and biometric data from which Disney unlawfully profited.

DEFENDANTS

Defendant The Walt Disney Company

17. Defendant The Walt Disney Company is a Delaware corporation with its principal place of business located in Burbank, California as well as in New York, New York.

Defendant Disney DTC LLC

18. Defendant Disney DTC LLC is a Florida limited liability company with its principal place of business located in Burbank, California; Defendant Disney DTC LLC is the data controller for The Walt Disney Company, and is a subsidiary or otherwise an affiliate of The Walt Disney Company. Defendant Disney DTC LLC selects this District as its forum and New York for choice of law for disputes such as this one.

FACTUAL ALLEGATIONS

Background and Disney's Unlawful Collection of Facial Recognition Data

19. Founded in 1923 by Walt and Roy Disney, Disney is one of the largest and most well-known corporations in the United States with over 225,000 employees as well as an annual revenue in excess of \$91 billion.

20. Disney initially rose to popularity through multiple lines of business, including its many theme parks and cartoon shows. In the century that has passed, Disney has become a ubiquitous presence in the homes of millions of Americans serving numerous different lines of business.

21. But as times have changed, so has Disney.

22. Disney's theme park business has grown into a leviathan within its industry – and so has its hunger for personal data on the visitors who enter into the Disney Theme Parks. And while Disney Theme Parks are the most visited theme park company worldwide today (157.3

million guests total), Disney’s consumers should not have to shed their privacy rights at the gates of the “Happiest Place on Earth.”

23. Beginning as late as April 28, 2026, Disney began to collect facial recognition data from guests’ faces at the entrance to Disneyland and California Adventure (which Plaintiff Duffield visited).¹² According to the LA Times, the way this occurred was by collecting photos of the faces of guests, like Plaintiff Duffield, is “to covert the images into unique numerical values [...] the images can then be compared with pictures when a customer first used the ticket or annual pass.”¹³

24. According to the LA Times, there are small signs nearby the security checkpoints which notify guests of the new facial recognition policy, but the sign is adorned with red, green, yellow, and blue Mickey Mouse silhouettes and is very easy to miss.¹⁴

25. For guests who wish to avoid this invasive technology, there are unclear separate entrances which have a slash through a silhouette of a head and shoulders as if that constitutes a meaningful way to opt out from facial recognition collection.¹⁵

26. There are dozens of lines which allow guests to enter the parks, but only four out of the many lines claim not to use facial recognition through their unclear signage.¹⁶ Guests, let

¹² <https://www.latimes.com/california/story/2026-04-28/disneyland-rolls-out-facial-recognition-at-park-entrances-heres-how-it-works>, (last accessed May 14, 2026).

¹³ *Id.*

¹⁴ *Id.*

¹⁵ <https://www.latimes.com/california/story/2026-04-28/disneyland-rolls-out-facial-recognition-at-park-entrances-heres-how-it-works>, (last accessed May 14, 2026).

¹⁶ *Id.*

alone children, cannot make a conscientious choice to avoid having their facial recognition data collected.

27. Further, there are concerns about how transparent Disney is being with the use of the technology; logically, if images of pictures taken when a customer first used a ticket or annual pass are then compared with another image, there must be some sort of biometric software in the first instance collecting facial recognition data to ascertain whether the two comparable images are in-fact a match. At bottom, Disney's claims that the data is only collected for 30 days simply cannot be true given the biometric information is compared to when guests first bought tickets or annual passes and associated their pictures with those tickets or passes.

28. According to Disney, the reason the technology is used is because it prevents fraud and re-entry (of persons who may not have purchased tickets to be able to do so).¹⁷

29. Additionally, privacy advocates are concerned about the use of the technology.

30. As stated by Ari Waldman, a law professor at University of California Irvine, "[t]he normalization of facial surveillance is really problematic. We can't go around life hiding out faces, so this isn't just the next step in surveillance; its qualitatively different. In a world of facial recognition, when people leave their house, it means they're automatically identified."¹⁸

The Sensitivity of Biometric Information

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

¹⁷ <https://www.privacyguides.org/news/2026/05/06/disneyland-california-rolls-out-facial-recognition/>, (last accessed May 14, 2026).

¹⁸ *Id.*

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

33. Faceprints generated by facial recognition technology systems may be used by the system to verify a person's identity by conducting a one-to-one comparison. For example, U.S. Customs and Border Protection uses facial recognition technology to biometrically confirm the identity of travelers that come to the United States by comparing a photo taken of the traveler at arrival against the passport photo presented by the traveler. Facial recognition technology systems may also compare an individual's face print against a larger database of face prints in order to determine whether the individual matches any person included in the database.

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

35. Two main classes of biometrics data can be collected from individuals: (i) behavioral characteristics and (ii) physiological characteristics.¹⁹ Behavioral characteristics track the conduct and actions of an individual, which may include an individual's keystroke, signature,

¹⁹ Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589–592 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; see generally, “What is Biometrics?,” IDEMIA, www.morpho.com/en/biometrics (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable) (last visited May 15, 2026).

and voice recognition.²⁰ Physiological characteristics examine the size, shape, or composition of the individual's face and body, including hand geometry and facial recognition.²¹ "Biometric identification has expanded from describing basic physical attributes to now include fingerprint scans, iris scans, retinal scans, voice recognition," and DNA.²²

36. Biometric identifiers come in a variety of forms that are unique (and largely unchangeable) to each person. This sensitivity prompts a critical need to protect and secure biometric identifiers that may: specifically link an individual to a data record; create digital identities that can be used for fraudulent purposes;²³ and, be compromised by their immutability and limitations to modification.

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

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

39. Personally identifiable information ("PII") has intrinsic value; however, biometric data often carries significantly greater value than other forms of PII—such as an address or passport

²⁰ *See id.*

²¹ *Id.*

²² Center for Global Development, *Biometrics FAQs*, CGD, 2019, <https://www.cgdev.org/page/biometrics-faqs> (last visited May 15, 2026).

²³ <https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity> (last accessed May 26, 2026).

number—because it is generally immutable and cannot be changed once compromised. According to the Richmond Journal of Law and Technology (Volume XV, Issue 4):

PII is an exceptional resource that companies can use for internal purposes or to sell to other companies.... Due, in part to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII. The value of the data increases when combined to provide information, such as consumer preferences that are not discernable from the data points individually.

As a result, companies are maintaining, sharing and selling dossiers of millions of consumer preferences... The potential for increased profits and cost savings serve as a substantial impetus for companies to ensure and cost savings serve as substantial impetus for companies to ensure that their actions do not compromise access to this valuable resource.

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

41. Recognizing the need to protect consumers and citizens, the Federal Trade Commission’s (“FTC”) Policy Statement on Biometric Information and Section 5 of the Federal Trade Commission Act provides:

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

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

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

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

Disney Violates Federal Trade Commission Guidance

44. Additionally, Disney's collection, retention, and use of biometric information without adequate consent demonstrates that Disney violates Section 5 of the Federal Trade Commission Act – which protects against deceptive and unfair trade practices.

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

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

Harm to Plaintiff Duffield and Class Members

47. Plaintiff Duffield and Class members suffered concrete harm when Disney collected and converted her facial recognition data for profit. Plaintiff Duffield’s facial recognition data was used for profit because, as Disney states, it is used for fraud prevention and the re-entry of guests. Additionally, it is used for profit because it allows Disney collect to facial recognition data instead of going through the process of hiring enough employees to manually validate guests or security staff to secure the premises.

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

49. To make matters worse, Disney connects biometric information with an assigned numerical identifier, as well as Plaintiff’s ticketing information – which is essentially a highly valuable package of information that would have tremendous worth to Disney in other ways including using biometric information for payment profiles and scanning entrance into other areas of Disney Theme Parks. In fact, Disney does use consumer biometric information for other purposes: Disney collects biometric information at their other Disney Theme Parks through collecting fingerprints when a Disney visitor uses a Disney “Magic Band” which gives access to Disney Theme Parks²⁴ and it also collects biometric information during specific user experiences which collect images of visitors to Disney Theme Parks as part of the Disney PhotoPass program which has occurred as late as January of 2025.²⁵ Ironically, Disney is much more thorough about the descriptions of how the Magic Band and PhotoPass programs collect and use biometric data

²⁴ <https://plandisney.disney.go.com/question/create-fingerprints-scanned-parks-visiting-first-time-520378/>, (last accessed May 10, 2026).

²⁵ <https://disneyworld.disney.go.com/photopass-terms-conditions/>, (last accessed May 10, 2026).

– with more robust disclosures and explanations – but does not do the same for the conduct as alleged here.

50. This type of combined information is a gold mine for hackers, and a data breach of biometric information would be devastating for Plaintiff and Class members – and Disney suffered a massive data breach as recently as 2024 and also settled an action with the Federal Trade Commission for issues regarding collection of children’s digital data through online channels for \$10 million.

51. The severity of this violation is heightened by the immutable nature of biometric identifiers; once an individual’s facial data is captured and linked to identity, it cannot be changed or revoked. Thus, when Disney collects facial recognition from minor class members – whom cannot adequately consent to having their privacy rights violated – that facial recognition data does not and cannot change.

CLASS ACTION ALLEGATIONS

52. This Action is properly maintainable as a class action pursuant to Federal Rule of Civil Procedure 23, Rules 23(a), 23(b)(1) and 23(b)(2). Plaintiff brings this class action on behalf of herself and all other similarly situated individuals. The classes which Plaintiff seeks to represent are defined as follows

Nationwide Class: All individuals who had their facial recognition collected, stored, retained, or otherwise used by Disney without consent during the applicable statutory period.

California Sub-Class: All individuals who had their facial recognition collected, stored, retained, or otherwise used by Disney without consent during the applicable statutory period.

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

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

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

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

state laws;

- b. Whether Defendant's acts and practices violated state consumer protection laws;
- c. Whether Plaintiff and the Class are entitled to equitable relief, including but not limited to injunctive relief, restitution, and disgorgement; and,
- d. Whether Plaintiff and the Class are entitled to actual, statutory, punitive and/or other forms of damages, and other monetary relief.

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

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

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

59. Plaintiff may revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT ONE

VIOLATIONS OF CALIFORNIA CONSTITUTION’S RIGHT TO PRIVACY

ARTICLE I, § 1

(ON BEHALF OF THE CALIFORNIA SUB-CLASS)

60. Plaintiff re-alleges and incorporates paragraphs 1 through 58 with the same force and effect as if fully restated herein.

61. Article I, Section 1 of the California Constitution provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” California Constitution, Article I, Section 1. Plaintiff Duffield is a California resident whose privacy rights are protected by the California Constitution.

62. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

63. The right to privacy in California’s constitution creates a right of action against private and government entities.

64. Plaintiff and California Sub-Class Members have and continue to have a reasonable expectation of privacy in their personal information and private data, pursuant to Article I, Section I of the California Constitution. This includes biometric information. The manner in which Disney collected biometric information —without adequately obtaining consent — defeats established

privacy-mechanisms and social norms.

65. This conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person. Reasonable individuals do not expect that they are having their biometric information collected, retained for some non-specific amount of time, and weaponized against them to "prevent fraud" at a Disney Theme Park.

66. Disney's conduct violated the privacy of California Sub-Class Members, including Plaintiff Duffield. Disney did not have consent to intercept, collect, retain, use, or otherwise have possession of their private biometric information, let alone use it for profit.

67. Plaintiffs and California Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Disney as a result of its intrusion upon seclusion.

68. Disney's conduct was intentional, knowing, and carried out with a conscious disregard for Plaintiff's and California Sub-Class Members' rights, Plaintiff and California Class members are entitled to punitive and exemplary damages.

69. Plaintiffs and California Sub-Class Members also seek any other relief the Court may deem just and proper.

COUNT TWO

INTRUSION UPON SECLUSION

(ON BEHALF OF THE NATIONWIDE CLASS AND CALIFORNIA SUB-CLASS)

70. Plaintiff re-alleges and incorporates paragraphs 1 through 58 with the same force and effect as if fully restated herein.

71. Under California common law, an individual has the right to control and protect their private information.

72. Disney’s collection, retention and otherwise use of Plaintiff’s and Class Members’ identifiable information and biometric information constitutes an intentional invasion of privacy.

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

74. This expectation is particularly heightened given that there were no adequate disclosures of Disney’s involvement in collection, retention, and otherwise use of biometric information – even through Disney is sophisticated to know how sensitive it is and maintains more stringent protections for the other ways it collects biometric data (*Infra.*, at ¶ 49).

75. Plaintiff and Class Members did not consent to, authorize, or understand Disney’s collection, retention, and use of their private data.

76. Disney’s conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they go into public places including those that are constructed for children and families, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

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

78. Indeed, that Disney went out of its way to claim the data is collected, retained and used was meaningfully “opt in”—when it was not—also makes its conduct especially offensive.

79. Disney’s conduct caused Plaintiff and Class Members harm and injury, including a

violation of their privacy interests.

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

81. Disney's conduct was intentional, knowing, and carried out with a conscious disregard for Plaintiff's and Class Members' rights. Thus, Plaintiff and Class Members are entitled to punitive and exemplary damages.

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

COUNT THREE

VIOLATIONS OF CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

Cal. Bus. & Prof. Code § 17200

(ON BEHALF OF THE CALIFORNIA SUB-CLASS)

83. Plaintiff re-alleges and incorporates paragraphs 1 through 58 with the same force and effect as if fully restated herein.

84. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200.

85. **Unfairness Prong.** Disney engaged in unfair business practices by collecting biometric information from Disney Theme Park guests without adequate consent, including from Plaintiff and California Class members. Additionally, Disney engaged in unfair business practices by claiming that the biometric collection process is an "opt-in" process when it is not – Disney Theme Parks lack adequate disclosures which would allow Plaintiff and California Class members from meaningfully opting into biometric data collection.

86. Finally, Disney engaged in unfair business practices by collecting biometric information and misleading Plaintiff and California Class Members about retention schedules – while Disney says it only retains data for 30 days, this cannot be true given that the data is compared to pictures taken concurrently with annual park passes, which are, at a minimum, kept for at least an annual period.

87. Had Plaintiff known that Disney was collecting, retaining, and using her biometric data without adequate consent she would have avoided doing business with Disney – including paying for tickets to Disney Theme Parks.

88. **Unlawful Prong.** Disney engaged in unlawful acts and practices by violating each of the laws described herein, including the California Consumer Legal Remedies Act, Section 5 of the FTC Act, California Consumer Privacy Act (“CCPA”) and, as described above, the California Constitution’s Right to Privacy as well as intrusion upon seclusion/the common law right to privacy. Disney violated the CCPA because it broadly protects consumer privacy rights, including alerting consumers that their private data – including biometric data – is being collected through a “notice at collection” process. Additionally, the CCPA requires that businesses limit the amount of personal information they collect to prevent potential dangers associated with data breaches; and there are alternative methods to collecting consumers’ biometric data in order to protect Disney Theme Parks from fraud and other legal concerns, including hiring more security and improving security protocols.

89. Further, Plaintiff and California Class members remain concerned about the potential presence of third parties which may be processing Plaintiff and California Class members’ pictures into the biometric and numerical data as stated above – but will only be able to ascertain information about these processes through discovery.

90. Plaintiff and California Class members were completely unaware of Disney's conduct and could not have anticipated these intrusions into their privacy through these unlawful, unfair, and deceptive practices. Accordingly, Plaintiff and California Class members could not avoid the harm caused by Disney.

91. Disney's conduct was and remains immoral, unethical, oppressive, unscrupulous and substantially injurious to Plaintiff and California Class Members. The gravity of harm of Disney's collection, retention, and use of Plaintiffs' and California Class members' biometric information and private data is significant, and there is no corresponding benefit from such conduct.

92. As a result, Plaintiff and California Class members suffered a loss of property in the form of privacy violations, loss of control over their valuable data, and a failure to be compensated for the data collected and sold.

93. Disney reaped unjust profits and revenues in violation of the UCL as a result of its unlawful and unfair conduct, including profits and revenues from its use of Plaintiff's and California Class Members' data. Plaintiff and Class Members seek restitution and disgorgement of these unjust profits and revenues.

94. Plaintiff and California Class Members seek all monetary and non-monetary relief allowed under the statute and equity, including restitution; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief permissible under the UCL.

COUNT FOUR

VIOLATIONS OF CONSUMER PROTECTION LAWS

CALIFORNIA CONSUMER LEGAL REMEDIES ACT (“CLRA”)

Cal. Civ. Code § 1770, *et seq.*

(ON BEHALF OF THE CALIFORNIA SUB-CLASS AND NATIONWIDE CLASS)

95. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 58 with the same force and effect as if fully stated herein.

96. Disney is considered a “business” under state law and Plaintiff and Class members are “consumers” under the terms of the CLRA because they are individuals who seek or acquire, by purchase or lease, goods or services for personal, familial, or household purposes.

97. At all relevant times, Disney’s actions and conduct constituted transactions for the sale or lease of goods to consumers under the terms of the CLRA – including the sale of tickets to Disney Theme Parks.

98. Disney’s business acts and practices are unfair and deceptive under the California Consumer Legal Remedies Act, Cal. Civ. Code § 1770, *et seq.*, including:

- a. Cal. Civ. Code § 1770(a)(5) by the use of untrue or misleading statements and omissions – including misleading statements about biometric data retention, misleading statements about biometric data collection being “opt-in,” and omissions about the collection of biometric data by not giving consumers adequate disclosures about biometric data collection.
- b. Cal. Civ. Code § 1770 (a)(14) by representing that a transaction confers or involves rights, remedies, or obligations that it does not have – including by promising to only retain biometric data for 30 days when this cannot be the case given the

biometric data and numerical values assigned to it are compared to annual information.

99. The CLRA makes illegal unconscionable acts or practices, unfair acts, and deceptive acts or practices in the conduct of any trade or commerce.

100. California (as well as other states through their respective unfair and deceptive trade practices statutes) has a strong public policy of protecting consumers' privacy interests, especially including protecting consumers' personal data who are minor children.

101. Disney's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers – including children. The gravity of the harm of Disney collecting, retaining, and using the sensitive and highly valuable biometric data of both adults minor children without consent, including of Plaintiff and Class members, is significant, and there is no corresponding benefit resulting from such conduct. Finally, children who had their biometric data collected were completely unaware of Disney's conduct, especially because they are children and otherwise could not consent so they could not have possibly avoided the harm.

102. By unlawfully collecting, retaining, and using this valuable data, Disney took money or property from Plaintiff and Class members.

103. Plaintiff and the Class members suffered damages as a result of Disney's CLRA violations. Additionally, in the event a nationwide class cannot be maintained, Class members seek relief under every substantially similar consumer protection statute for the claims as alleged in this Action. Plaintiff will only pursue injunctive and declaratory relief under the CLRA until a 30-day window has passed after the issuance of a CLRA Notice to Cure letter before seeking leave to amend their operative pleading to seek damages under this cause of action.

104. However, under every other consumer protection law, on behalf of herself and the Nationwide Class, Plaintiff seeks all available damages including actual damages, statutory damages, as well as treble damages, reasonable costs of suit and attorneys' fees.

COUNT FIVE

UNJUST ENRICHMENT

(ON BEHALF OF THE NATIONWIDE CLASS)

105. Plaintiff re-alleges and incorporates paragraphs 1 through 58 with the same force and effect as if fully restated herein.

106. Disney received benefits from Plaintiff and Class members and unjustly retained those benefits at their expense.

107. Disney received benefits from Plaintiff and Class members in the form of the Plaintiff's and Class members' valuable biometric information which Disney wrongfully collected, retained, and/or used from Plaintiff and Class members without authorization and proper compensation.

108. Disney collected, retained, and used this data for their own gain, providing Disney with economic, intangible, and other benefits, including the benefits described above. Disney had no valid agreement with Plaintiff and Class members to collect their biometric data.

109. Had Plaintiff and Class members known of Disney's misconduct, they (or their parents) would not have provided (or allowed to be provided) any of their valuable data to Disney or have used or paid to use Disney's Theme Parks.

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

111. The benefits that Disney derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable for Disney to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

112. Disney should be compelled to disgorge profits into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Disney received, and such other relief as the Court may deem just and proper.

DEMAND FOR RELIEF

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

- A. Certifying the Class and appointing Plaintiff as the Class's representative;
- B. Finding that Disney's conduct was unlawful, as alleged herein;
- C. Awarding declaratory relief against Disney;
- D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including injunctive relief;
- E. Awarding Plaintiff and Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profit;
- F. Awarding Plaintiff and Class members pre-judgment and post-judgment interest;
- G. Awarding Plaintiff and Class members reasonable attorneys' fees, costs, and expenses; and
- H. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

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

DATED: May 15, 2026

Respectfully submitted,

By: /s/ Blake Hunter Yagman

Blake Hunter Yagman

YAGMAN PLLC

FOREST HILLS TOWER

118-35 Queens Boulevard, Suite 444

Forest Hills, New York 11375

Tel.: (929) 709-1493

blake.yagman@yagmanpllc.com

Counsel for Plaintiff and the Proposed Class