Micha S. Liberty
LIBERTY LAW
California Bar No. 215687
1999 Harrison Street, Ste. 1800
Oakland, CA 94612
Tel: (510) 645-1000
Email: micha@libertylaw.com

James R. Marsh (pro hac vice to be filed)
Margaret E. Mabie (pro hac vice to be filed)
Helene M. Weiss (pro hac vice to be filed)
MARSH LAW FIRM PLLC
31 Hudson Yards, 11th Fl
New York, NY 10001
Tel: (212) 372-3030
Email: jamesmarsh@marsh.law
margaretmabie@marsh.law
heleneweiss@marsh.law

Hillary Nappi (pro hac vice to be filed)
HACH ROSE SCHIRRIPA & CHEVERIE LLP
112 Madison Avenue, 10th Fl
New York, NY 10016
Tel : (212) 213-8311
Email: hnappi@hrsclaw.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

"AMY" and "JESSICA" on behalf of themselves and others similarly situated, Plaintiffs, v. APPLE, INC., Defendant.	**Case No: 5:24-cv-8832** **COMPLAINT** **CLASS ACTION** Jury Trial Demanded

Amy of the Misty Series and Jessica of the Jessica Series (hereinafter "Plaintiffs") on their behalf and on behalf of those similarly situated, by and through their attorneys of record Micha Liberty of Liberty Law, James R. Marsh, Margaret E. Mabie, Helene M. Weiss of Marsh Law Firm PLLC ("MLF"), and Hillary Nappi of Hach Rose Schirripa & Cheverie LLP ("HRSC"), allege for their complaint as follows:

NATURE OF THE ACTION

1. This is a suit for damages arising out of the Defendant's violations of federal criminal child pornography statute 18 U.S.C. §§ 2252 (a)(4)(B) and (b)(2).

2. 18 U.S.C. § 2255(a) allows victims of child pornography crimes to recover liquidated damages in the amount of $150,000 and the cost of the action, including reasonable attorney's fees and other litigation costs reasonably incurred. The Court may also award punitive damages and grant such other preliminary and equitable relief as the Court determines to be appropriate.

3. All manufacturers must construct and sell products that are safe to use. Further, manufacturers are expected to disclose the truth to consumers when they discover or know of a likelihood that there exists a safety issue with a product they cause to enter the stream of commerce. This is especially true and applicable when the products are marketed and intended for use by children.

4. The instant action seeks relief on behalf of Plaintiffs and similarly situated individuals, defined below (the "Class"), who were harmed by iPhone, MacBook, iPad, and iCloud products manufactured, marketed, promoted, and sold by Apple Inc. ("Defendant" or

"Apple") and who, as a result of Apple's defective products, suffered damages as a result of Apple's defective design and design features which Apple knew to be unsafe.

5. Apple not only failed to properly manufacture and design products that harmed the Plaintiffs, but once it was aware of the dangers inherent in its products, it then failed to disclose these safety hazards to consumers.

6. Before August 2021, Apple knew its products contained defects as customers, law enforcement, and non-governmental watchdogs reported various concerns about Apple's failure to stop or limit the spread of known child pornography images and videos ("child pornography" or "CSAM") through its products despite available alternative designs and widespread technological solutions.

7. Having taken unnecessary risks in the design and manufacture of its products and knowing of those risks to consumers, Apple addressed the faulty design of its products with a widely touted improved design aimed at protecting children, including Plaintiffs and members of the proposed class, but then failed to implement those designs or take any measures to detect and limit CSAM on iCloud or any other Apple product.

8. Because Apple failed to stop or limit the spread of known CSAM, the vast majority of the Class, as victims of CSAM, continue to suffer harm caused and facilitated by Apple's defectively designed products and defective features.

9. Plaintiffs and members of the proposed Class, as CSAM victims, experience lifelong harm and trauma because of the known design defects Apple failed to remedy.

10. Not only did Apple fail to stop or limit the spread of known CSAM through its products, but it publicly announced that it affirmatively would not implement product design

changes to stop or limit the spread of known CSAM through its products, thereby amplifying the already significant risk and harm to the Plaintiffs and Class members.

PARTIES

11. "Amy" is an adult residing outside the Northern District of California.

12. "Amy" is a pseudonym for the victim depicted in the Misty child pornography series.

"Jessica" is an adult residing outside the Northern District of California.

13. "Jessica" is a pseudonym for the victim depicted in the Jessica child pornography series.

14. Each Plaintiff was sexually abused as a child, with such sexual abuse depicted in CSAM circulating on the internet worldwide, including on Apple devices and iCloud.

15. Defendant Apple is a California Corporation with its principal place of business in Cupertino, California.

16. Apple is a global technology company that designs, produces, manufactures, sells, and distributes technology products in the United States and across the globe, including smartphones, computers, tablets, and other electronic devices.

JURISDICTION AND VENUE

17. Federal subject matter jurisdiction is proper pursuant to 28 U.S.C. § 1331 because this is a civil action arising under 18 U.S.C. § 2255.

18. Federal diversity jurisdiction is proper pursuant to 28 U.S.C. § 1331 because both Plaintiffs in this action reside outside California, and the amount in controversy exceeds the minimum value required for diversity jurisdiction.

19. The Court also has jurisdiction pursuant to 28 U.S.C. § 1332(d) because this is a class action involving common questions of law or fact in which the aggregate amount in controversy exceeds $5,000,000, there are more than 100 members of the Class, and at least one member of the proposed Class is a citizen of a state different from that of the Defendant.

20. This Court also has supplemental jurisdiction over Plaintiffs and the Class pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Plaintiffs because Plaintiffs submit to the Court's jurisdiction.

22. This Court has personal jurisdiction over the Defendant because the Defendant conducts substantial business in this district and is headquartered in this district. Apple has engaged in sufficient minimum contacts with the United States, this judicial district, and California, and it has intentionally availed itself of the laws of the United States and California by conducting a substantial amount of business throughout the State.

23. Venue is appropriate and proper in the Northern District of California pursuant to 28 U.S.C. §§ 1391 (b)(1) and (2) because: (i) this civil action is brought in the judicial district where the Defendant is headquartered and where Apple conducts its primary business operations; and (ii) a substantial part of the events or omissions giving rise to the Plaintiffs' claims occurred in this judicial district.

24. Defendant has conducted and continues to conduct business based in this district at all relevant times. Accordingly, Defendant is a corporation that resides in this district pursuant to 28 U.S.C. § 1391(d).

FACTS

Apple's Mobile Devices and iCloud Products

25. Apple was founded in 1976 as Apple Computer Company.

26. Apple is one of the world's most valuable public companies, with over $2.5 trillion market capitalization.

27. In fiscal year 2023, Apple generated annual net revenues of $383 billion and net income of $97 billion.

28. Apple's net income exceeds any other company in the Fortune 500 and the gross domestic products of more than 100 countries.

Apple Designs Devices Without Sufficient Child Protection Safeguards

29. In 2007, Apple launched its most successful product, the iPhone, a cell phone with a mobile operating system that mimicked a computer's functionality and ease of use, including internet connectivity.

30. The iPhone is Apple's signature product. As of 2023, Apple has sold over 2.6 billion iPhones worldwide since the first iPhone was released in 2007.

31. Apple developed and supports iMessage, an instant text messaging product through Apple's Messages application that allows Apple smartphone and Apple computer users to send text, images, video, and audio messages to other users.

32. Apple's messaging product, through the iMessage application, runs on Apple desktop computers, laptops, tablets, and mobile devices running Apple's operating systems.

33. Apple customers cannot download applications for their iPhones or iPads except through the Apple App Store because Apple maintains rigorous control over applications that can be placed on their devices.

34. Apple's U.S. smartphone market share exceeds 65 percent for all smartphones.

35. Apple's devices and services are accessible by logging into a user's account credentials, an Apple Account, formerly called AppleID.

36. An Apple Account requires a valid email address and password.

37. Since 2021, Apple has attempted to differentiate itself from its competitors by promoting its commitment to privacy. Recently, Apple launched a worldwide ad campaign, erecting 40-foot billboards featuring the iPhone and a simple slogan, "Privacy. That's iPhone."[1]

[1] *Apple and Privacy,* APPLEINSIDER, https://appleinsider.com/inside/apple-and-privacy (last visited Nov. 20, 2024).

38. Other billboards are similarly plastered with Apple's purported commitment to privacy. "What happens on your iPhone, stays on your iPhone," announced one billboard in Las Vegas.[2] "Your iPhone knows a lot about you. But we don't," announced another in New York.[3]

Apple Products

39. Mobile devices, including smartphones and tablets, rely increasingly on cloud storage to host abundant data users accumulate through ordinary use. The apps, pictures, videos, messages, and other data files users amass often vastly exceed the storage capacity of their device, but users can upload them to a cloud platform.

---

[2] Hamza Shaban, *Apple Stars at Giant Tech Confab CES — Without Actually Being There*, WASH. POST (Jan. 7, 2019) https://www.washingtonpost.com/technology/2019/01/07/apple-burns-google-giant-billboard-touting-privacy-ces/.

[3] Richard B. Levine, Photograph of A Billboard on the Side of a Building in Midtown Manhattan on Tuesday, July 9, 2019 Informs Viewers of the Privacy Afforded by Using Apple Devices, https://www.alamy.com/a-billboard-on- the-side-of-a-building-in-midtown-manhattan-on- tuesday-july-9-2019-informs-viewers-of-the-privacy-afforded-by-using-apple-devices-richard-b-levine-image260045682.html (last accessed Nov. 20, 2024).

40. Apple designed iCloud such that it failed to adequately safeguard child victims of online sexual exploitation and abuse.

41. In 2011, Apple launched iCloud, a cloud computing product that permits data storage and synchronization across multiple devices and stores data on remote computer servers.

42. iCloud has since become a profit center for Apple, generating billions in annual revenues. By any metric, iCloud dominates all other cloud platforms accessible on Apple's mobile devices. Reports indicate that Apple had at least 850 million iCloud users by 2020 and iCloud has become a significant profit center for the company.[4]

43. Apple's iCloud was initially partially hosted on Amazon Web Services and Microsoft Azure. By 2016, Apple began hosting iCloud on the Google Cloud Platform.[5]

44. Apple's iCloud capabilities are built into each Apple device, and every Apple Account comes with 5 GB of free storage, with additional storage space available for subscription purchase.

45. While users can disable iCloud on their devices, they will lose access to key features if they choose not to use at least basic iCloud.

---

[4] Jannik Lindner, *Apple iCloud Statistics Reveal Massive User Base and Revenue Growth*, WIFITALENTS, https://wifitalents.com/statistic/apple-icloud/ (Aug. 5, 2024).

[5] Chris Davies, *Apple Confirms iCloud Uses Google Servers (But Don't Panic)*, SLASHGEAR (Feb. 26, 2018, 9:57 AM EST), https://www.slashgear.com/apple-confirms-icloud-uses-google-servers-but-dont-panic-26521087/.

46. Most users find the free basic iCloud insufficient for their storage needs and purchase an iCloud storage plan.[6] Apple's gross profit margins for iCloud approach 80 percent.

47. According to Apple, iCloud uses strong security methods and strict policies to protect user information and leads the industry in using privacy-preserving security technologies like end-to-end encryption for user data.

48. Apple boasts that "the security of [user] data in iCloud starts with the security of [user's] Apple Account. All new Apple Accounts require two-factor authentication to help protect [the user] from fraudulent attempts to gain access to [the user's] account."[7] Two-factor authentication is also required for many features across Apple's ecosystem, including end-to-end encryption.

49. Apple offers two options to encrypt and protect the data a user stores in iCloud: standard data protection and advanced data protection.

50. Standard data protection is the default setting for an account. iCloud data is encrypted, and the encryption keys are secured in Apple data centers so Apple can assist a user with data recovery. Only certain data is end-to-end encrypted.

51. Advanced Data Protection for iCloud is an optional setting that offers Apple's customers the "highest level of cloud data security." If a user chooses to enable Advanced Data

[6] Sidney Ho, Ross Seymore, dbDIG Primary Research Survey on Apple Services, DEUTSCHE BANK (Oct. 24, 2023).
[7] APPLE, *iCloud Data Security Overview*, https://support.apple.com/en-us/102651 (last accessed Nov. 20, 2024).

Protection, their trusted devices retain sole access to the encryption keys for most iCloud data, thereby protecting it using end-to-end encryption.

52. Some metadata and usage information stored in iCloud remains under standard data protection, even when Advanced Data Protection is enabled. For example, dates and times a file or object was modified are used to sort user information, and checksums of file and photo data are used to help Apple de-duplicate and optimize iCloud and device storage — all without Apple having access to the files and photos themselves.

53. This metadata is always encrypted, but Apple still stores the encryption keys. Apple explains that it is "committed to ensuring more data, including this kind of metadata, is end-to-end encrypted when Advanced Data Protection is enabled."[8]

54. For photos, with the standard data protection plan, the following information is always protected: (i) the raw byte checksum of the photo or video; (ii) whether an item has been marked as a favorite, hidden, or marked as deleted; (iii) when the item was initially created on the device; (iv) when the item was originally imported and modified; and (v) how many times an item has been viewed.

55. In 2019, Apple introduced iCloud to Windows devices to permit iCloud access from non-Apple devices.

56. iCloud.com provides access to user's iCloud data via any web browser. All sessions at iCloud.com are encrypted in transit between Apple's servers and the user's browser.

[8] *Id.*

57. When Advanced Data Protection is enabled, access to a user's data via iCloud.com is disabled by default.

58. An iCloud user can also turn on data access on iCloud.com, which allows the web browser being used and Apple to have temporary access to data-specific encryption keys provided by the device to decrypt and view user information.

Apple Knows its Products Harm CSAM Victims

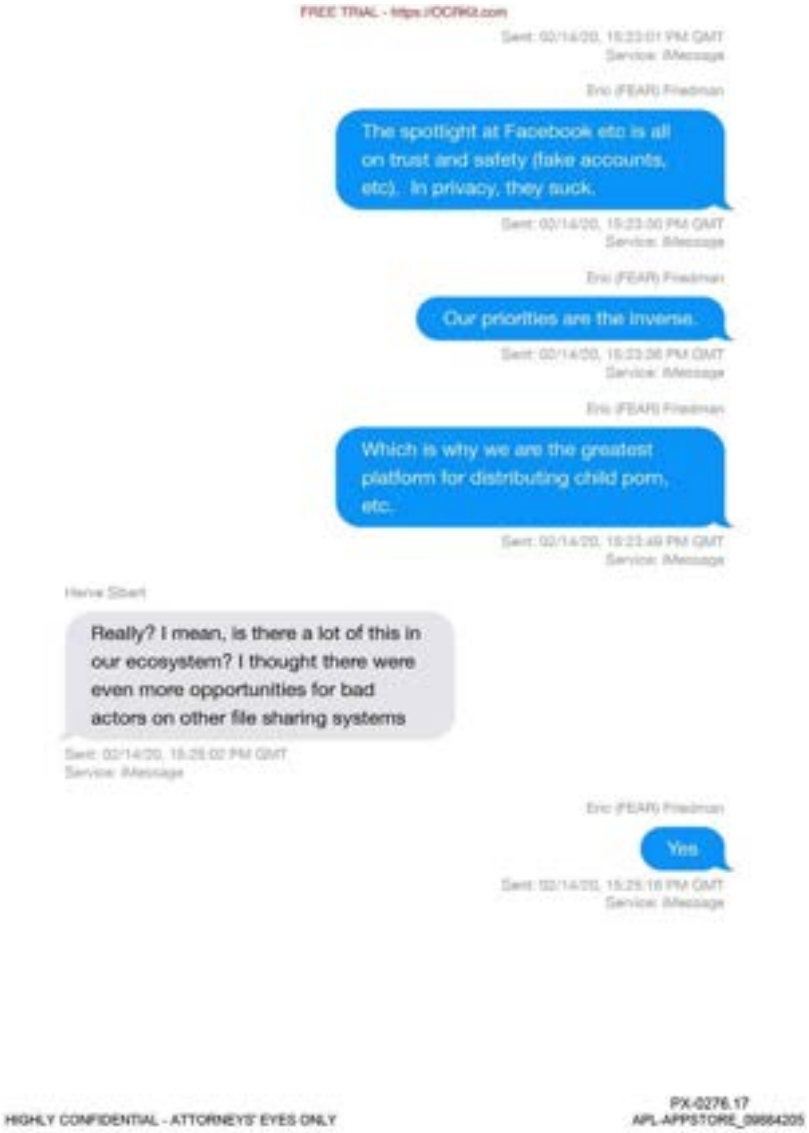
59. Apple and its leadership, including but not limited to Eric Friedman and Herve Sibert, had actual knowledge that Apple defectively designed its products in a manner that Apple touted as "the greatest platform for distributing child porn."[9]

60. In an iMessage conversation about whether Apple might be putting too much emphasis on privacy and not enough on trust and safety, Friedman boasted that iCloud is "the greatest platform for distributing child porn" and that Apple has "chosen to not know in enough places where we really cannot say[.]"[10]

[9] Malcolm Owen, *Apple Exec Said iCloud was the "Greatest Platform" for CSAM Distribution*, APPLEINSIDER (Aug. 20, 2021), https://appleinsider.com/articles/21/08/20/apple-exec-said-icloud-was-the-greatest-platform-for-csam-distribution.

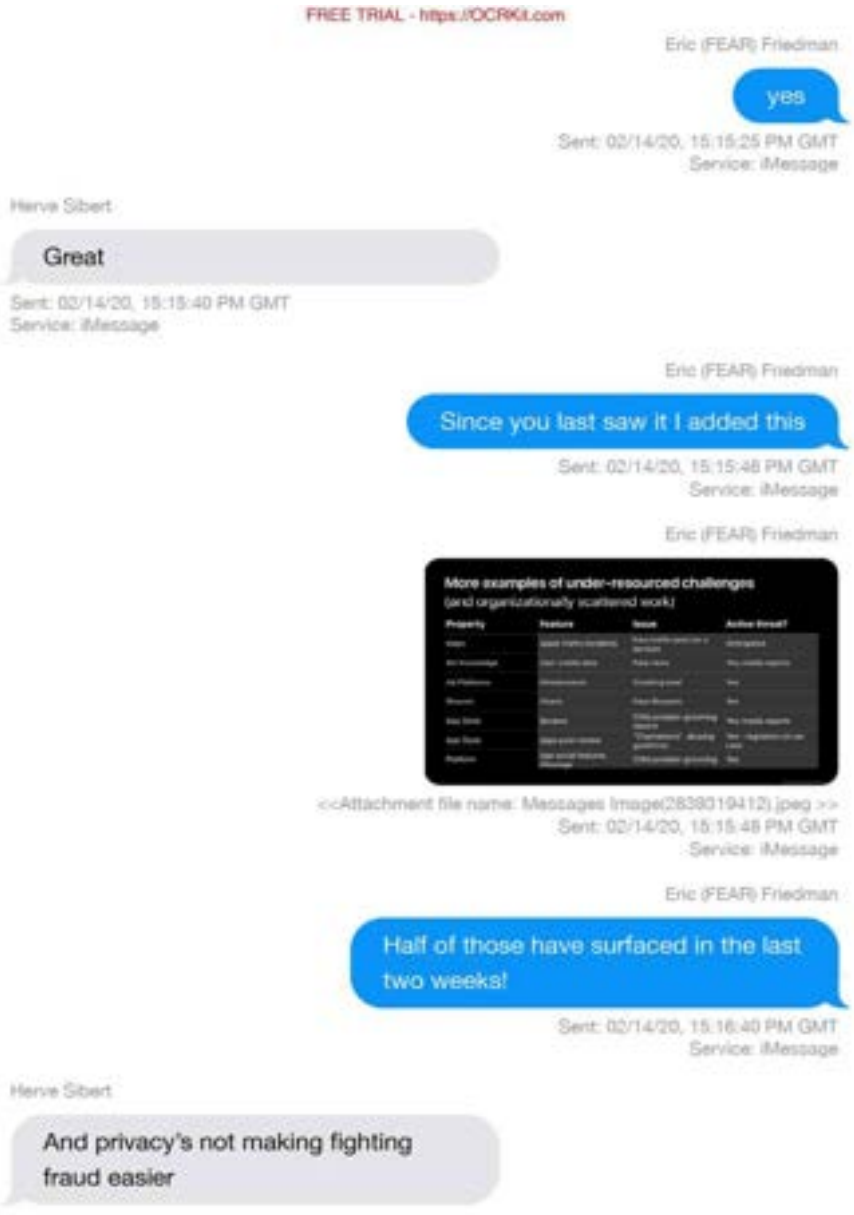
[10] Sean Hollister, *Sweetheart Deals and Plastic Knives: All The Best Emails From The Apple vs. Epic Trial,* VERGE (Aug. 19, 2021, 10:00 AM EDT), https://www.theverge.com/c/22611236/epic-v-apple-emails-project-liberty-app-store-schiller-sweeney-cook-jobs.

61. In the same conversation, Friedman referred to a New York Times article about CSAM detection and revealed that he suspects Apple is underreporting the size of the CSAM issue it has on its products.[11]



[11] *Id.; See generally* Gabriel J.X. Dance & Michael H. Keller, *Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse*, N.Y. TIMES, https://www.nytimes.com/2020/02/07/us/online-child-sexual-abuse.html (last updated Feb. 20, 2020).

62. In or after 2020, Apple and its executives consciously decided to ignore the Plaintiffs' exploitation and "chose not to know" about CSAM shared on iCloud and Apple products.



HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

PX-0276.11
APL-APPSTORE_09884199

63. Apple knowingly and intentionally designed products with conscious disregard for the highly preventable harms Apple caused Plaintiffs and all victims of known hashed CSAM.

64. Apple knowingly and intentionally designed its products with deliberate indifference to the highly preventable harms Apple caused Plaintiffs and all victims of known hashed CSAM.

Apple's CSAM Detection Tool – NeuralHash

65. In or about 2008, Professor Hany Farid developed a CSAM detection tool called PhotoDNA in collaboration with Microsoft.

66. Child safety tools and features are necessary components of digital product design, and failing to implement them falls below industry standards and accepted practices.

67. Tools like PhotoDNA are image comparison technologies that detect matches between modified versions of the same image or images.

68. Consider two versions of the same image: one in full color, the other in black and white. The human eye knows these images depict the same thing, but they are entirely different to a computer. Tools like PhotoDNA generate values indicating the "closeness" between two images.

69. This process, sometimes called "robust" matching or "perceptual hashing," looks at the visual content of the image instead of the exact binary image data (*i.e.*, the digital fingerprint or cryptographic hash). In other words, CSAM detection technologies can match images to known and identified CSAM.

70. Apple does not utilize any CSAM detection or child safety tools such as PhotoDNA on its products, including iCloud.

71. Even though its competitors, such as Microsoft, Google, and DropBox utilize proactive CSAM detection technologies like PhotoDNA to detect, report, and remove known hashed child pornography,[12] Apple fails to use these standardly accepted industry-wide child protection tools.[13]

72. Apple's purported rationale for not implementing PhotoDNA or any other proactive tools to detect, report, and remove known hashed CSAM prior to August 5, 2021, primarily involved prioritizing privacy as well as limited technological capabilities.

73. Apple publicly claimed to have resolved these issues by August 2021.

Apple Publicly Launches NeuralHash and Promises Plaintiffs Safer Apple Products

74. At some point in 2021, Apple developed a proactive detection tool called NeuralHash to detect known hashed CSAM.

75. On or before August 4, 2021, Apple consulted with child safety experts to preview its planned expanded child protection measures.

---

[12] Susan Jasper, *How We Detect, Remove and Report Child Sexual Abuse Material*, THE KEYWORD (Oct. 28, 2022), https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/.

[13] *See* Frank Bajak & Barbara Ortutay, *Apple to Scan U.S. iPhones for Images if Child Sexual Abuse*, ASSOCIATED PRESS (Aug. 6, 2021), https://perma.cc/9YCJ-KG6Y (describing how "Apple has been under government pressure for years to allow for increased surveillance of encrypted data"). *See generally* Nicholas Kristof, *The Children of Pornhub*, N.Y. TIMES (Dec. 4, 2020), https://perma.cc/8CZJ-2T22 (giving accounts of child pornography victims and arguing that search engines, banks and credit card companies should be proactive in in impeding sites that share child pornography, like Pornhub).

76. On or before August 5, 2021, Apple publicly announced three new child safety features on its products: (a) CSAM Detection in iCloud Photos; (b) Communications Safety in iMessage; and (c) Interventions in Siri and search.

77. Apple's child pornography detection tool in iCloud, named NeuralHash, enabled Apple to finally begin to identify and report iCloud users who store known CSAM in their iCloud accounts.

78. Apple's NeuralHash is a CSAM detection tool similar in concept to PhotoDNA but with additional security-oriented features that ultimately fail to protect the privacy of known CSAM victims.

79. Apple explained that NeuralHash is a perceptual hashing tool designed to ensure that distinct images produce distinct hash values.

80. Apple stated that NeuralHash was designed to ensure that identical and visually similar images result in similar hash values. For example, NeuralHash was designed so that the hash value of an image slightly cropped or resized from its original form will have a similar hash.

81. Based on information and belief, Apple collaborated with the National Center for Missing and Exploited Children (NCMEC) to develop, implement, and train NeuralHash technologies.

82. Based on information and belief, Apple trained NeuralHash using raw images of CSAM accessible only at NCMEC and, in turn, created a library of known CSAM hashes intended to be continually updated through ongoing collaboration with NCMEC.

83. Apple's NeuralHash was purportedly designed to detect known CSAM on physical Apple devices (e.g., iPhone, MacBook, iPad) at the moment the device connects to iCloud, but not a moment sooner. Apple claimed that NeuralHash was designed to operate in a fully encrypted environment and, thus, the tool would detect child pornography material on a device only after it is connected to iCloud.

84. Apple claimed that NeuralHash was designed to operate in a fully encrypted environment, and thus, the tool would detect CSAM on a device only after it connected to iCloud.

85. In other words, Apple designed NeuralHash to allow Apple users who do not upload files to iCloud to evade the detection of CSAM on their devices.

86. Indeed, Apple stated in its rollout of NeuralHash that it "ensures the device does not know the result of the match, but it can encode the result of the on-device match process before uploading to the server."

87. In keeping with Apple's stated privacy and security goals, it designed NeuralHash to perform on-device hash matching in a fully encrypted digital environment.

88. Apple consistently designs its products with the false choice of either privacy or CSAM detection, and NeuralHash was created to serve both goals.[14]

[14] *See* Dr. Hany Farid, *Briefing: End-to-End Encryption and Child Sexual Abuse Material*, 5RIGHTS FOUNDATION (Dec. 2019), https://5rightsfoundation.com/uploads/5rights-briefing-on-e2e-encryption--csam.pdf.

89. In developing NeuralHash to allow detection despite image re-sizing and cropping, Apple failed to engineer it to adequately generate distinct hash values for non-similar images with the same accuracy as PhotoDNA.

90. To make up for this imprecision, Apple designed NeuralHash with an artificial "false-positive" collision rate which would not trigger a report to Apple unless 30 images or more were detected as CSAM.[15]

91. Based on information and belief, without the 30-image threshold, Apple's NeuralHash maintained a false-positive rate of approximately 1 in 100,000 or less, which pales in comparison to PhotoDNA's false-positive rate of approximately 1 in 50 billion.

92. Based on information and belief, Apple deliberately designed NeuralHash with a threshold higher than necessary to reach the same level of precision as PhotoDNA.

93. Upon information and belief, Apple failed to design NeuralHash with a threshold match that resulted in a false-positive rate similar to PhotoDNA's.

94. Apple raised the threshold for reasons related to public relations and brand image rather than child safety to advertise that NeuralHash maintained a false-positive rate of 1 in 1 trillion.

95. NeuralHash was designed to trigger an internal human review by Apple once a 30-image threshold of potential CSAM was met.

[15] Todd Spangler, *Apple Says Its iCloud Child-Porn Scanning System Won't Trigger Alerts Until it Detects at Least 30 Images*, VARIETY (Aug. 13, 2021, 11:54 AM PT), https://variety.com/2021/digital/news/apple-child-porn-image-threshold-privacy-1235041363/.

96. By design, Apple's NeuralHash technology would not trigger a mandatory report to NCMEC for less than 30 images of CSAM.

97. As implemented by Apple, NeuralHash would not trigger an NCMEC reporting requirement without a human analyst first reviewing the material.

NeuralHash's Threshold Secret Sharing Design Feature Reflects Apple's Deliberate Indifference to CSAM Victims and its Legal Requirement to Report CSAM to NCMEC

98. On August 13, 2021, Apple's Chief Software Engineer, Craig Federighi, was interviewed by the Wall Street Journal and defended NeuralHash: "This is about images that are stored in the cloud and an architecture for identifying in the most privacy protecting way we can imagine performing that process, and in the most auditable and verifiable way possible."[16]

99. Apple designed NeuralHash with arbitrary thresholds, which, if implemented, would have failed to detect known CSAM adequately and failed to meet essential child protection and legal standards.

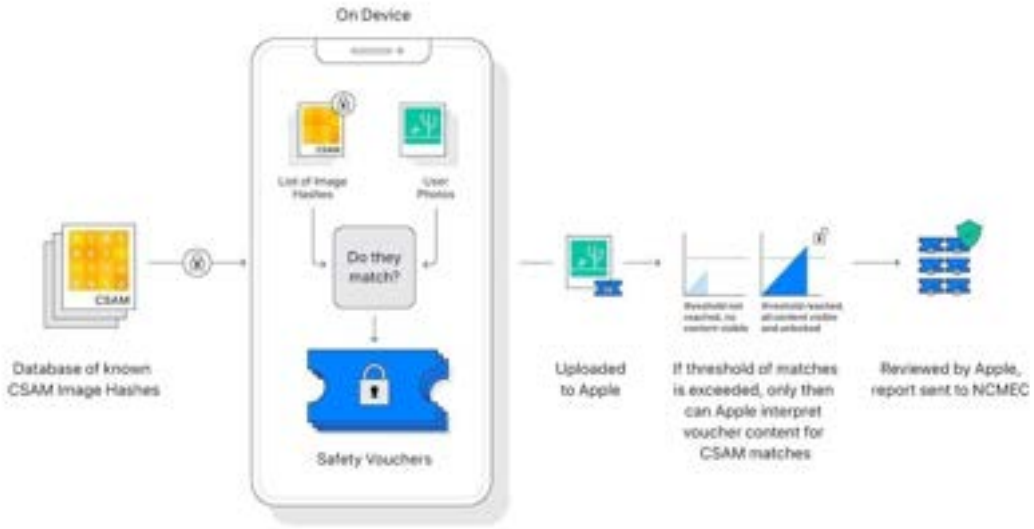
[16] Joanna Stern & Tim Higgins, *Apple Executive Defends Tools to Fight Child Porn, Acknowledges Privacy Backlash*, WALL ST. J. (Aug. 13, 2021, 9:00 AM ET), https://www.wsj.com/articles/apple-executive-defends-tools-to-fight-child-porn-acknowledges-privacy-backlash-11628859600.

100. By design, Apple's NeuralHash tool disregards the requirement outlined in 18 U.S.C. 2258A(a)(2) to report all apparent and imminent violations of child pornography laws to NCMEC.[17]

101. Indeed, Apple's NeuralHash failed to adequately report all the CSAM it detected.

102. While the industry-wide standard tool for CSAM detection, PhotoDNA, achieves a 1 in 50 billion false positive rate, Apple designed NeuralHash with an added cryptographic feature called threshold secret sharing which only permits the decryption of hash-matched materials if the number of materials matched exceeds a designated threshold. Only then does NeuralHash decrypt the materials, and Apple's agents conduct a human review of the materials, disable the offender's account, and report the CSAM to NCMEC.

[17] (2) Facts or circumstances.—
(A) Apparent violations.—
The facts or circumstances described in this subparagraph are any facts or circumstances from which there is an apparent violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography, of section 1591 (if the violation involves a minor), or of 2422(b).
(B) Imminent violations.—
The facts or circumstances described in this subparagraph are any facts or circumstances which indicate a violation of any of the sections described in subparagraph (A) involving child pornography may be planned or imminent.



103. Apple's NeuralHash also utilized synthetic match vouchers to hide the number of CSAM images detected in the hash-match process.

104. To evade requirements under 18 U.S.C. 2258A to report any imminent or apparent CSAM violations, Apple designed NeuralHash with synthetic vouchers to register as matches. These intentional false positives inject uncertainty about the actual number of known CSAM hash matches until a threshold is exceeded.

105. These synthetic vouchers were designed to give Apple plausible deniability; Apple could never be sure any NeuralHash hit was indeed CSAM because of the false positive hits baked into NeuralHash. This design feature was purposely created to enable Apple to avoid its legal obligation to report any imminent or apparent CSAM violations.

106. In effect, NeuralHash effectively ignored the first 29 images of CSAM it detected in any user's iCloud account.

107. Apple designed NeuralHash to detect known hashed CSAM on a user's device without decrypting the images until a designated threshold was reached for reasons unrelated to child safety and Apple's legal requirements. This design resulted in a false positive rate of 1 in 1 trillion, allowing Apple to maintain its public image, marketing, and branding around privacy and security.

108. Apple's design choices related to NeuralHash superseded industry standards, legal requirements, and internal and external concerns for child safety and effective CSAM detection.

109. Apple knowingly designed NeuralHash to fail to report at least 29 detected images of known CSAM despite the extremely low risk of false positives when searching for known CSAM using image-match tools and hashing technologies such as PhotoDNA.[18]

Apple Advertises NeuralHash

110. Apple's announcement concerning NeuralHash declared, "Apple servers flag accounts exceeding a threshold number of images that match a known database of CSAM image hashes so that Apple can provide relevant information to NCMEC."[19]

111. Despite the industry-wide practice of proactively detecting known CSAM since approximately 2008, Apple first launched its initial effort to implement proactive detection in August 2021.

[18] *CSAM Detection: Technical Summary*, APPLE (Aug. 2021), https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf.
[19] *Id.* at p. 3.

112. Apple prioritized privacy, security, and encryption over child safety in designing its products, including NeuralHash.

113. On August 10, 2021, less than a week after NeuralHash was launched, Apple privacy head Erik Neuenschwander publicly addressed concerns about NeuralHash.[20]

114. In August 2021, Apple published a comprehensive review of its proposed child safety features, including NueralHash.[21]

115. At the same time, Apple's chief software engineer, Craig Federighi, exclaimed his confidence in Apple's ability to achieve a solution that balanced user privacy and child safety equally, announcing that "[Apple] feel[s] very positive and strongly about what we're doing."[22]

116. Apple led Plaintiffs, and those similarly situated Class members, to believe that it would finally act on its duty to provide safe products and report known detectable CSAM.[23]

---

[20] *See* Matthew Panzarino, *Interview: Apple's Head of Privacy Details Child Abuse Detection and Messages Safety Features*, TECHCRUNCH (Aug. 10, 2021, 8:00 AM PDT), https://techcrunch.com/2021/08/10/interview-apples-head-of-privacy-details-child-abuse-detection-and-messages-safety-features/.

[21] *Security Threat Model Review of Apple's Child Safety Features*, APPLE (Aug. 2021), https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf.

[22] See generally Joanna Stern, Apple's Software Chief Explains 'Misunderstood' iPhone Child-Protection Features, Wall St. J. (Aug. 13, 2021), https://www.wsj.com/video/series/joanna-stern-personal-technology/apples-software-chief-explains-misunderstood-iphone-child-protection-features-exclusive/573D76B3-5ACF-4C87-ACE1-E99CECEFA82C.

[23] Bobby Allyn, *Survivors Laud Apple's New Tool to Spot Child Sex Abuse But the Backlash is Growing*, NPR, https://www.npr.org/2021/08/13/1027314728/survivors-laud-apples-new-tool-to-spot-child-sex-abuse-but-the-backlash-is-growi (last updated Aug. 13, 2021, 3:31 PM ET).

117. Apple ultimately ignored and disregarded its promises to victims and survivors of known detectible CSAM in the design and implementation of NeuralHash in August of 2021.[24]

Apple Delays its Implementation of NeuralHash

118. On September 3, 2021, Apple announced that it would delay its initial NeuralHash rollout.[25]

119. On the same day, the children's rights NGO Thorn issued a statement criticizing Apple's change of plans: "[o]ur expectation of Apple is that they publish a detailed timeline and clear deliverables to demonstrate how they will maintain their commitment to improve their child safety measures and implement scalable detection of child sexual abuse material (CSAM) in iCloud Photos."[26]

120. Apple nonetheless failed to publicize any such timeline or deliverables.

121. From September 2021 to December 2022, Apple misled Plaintiffs and the public about the NeuralHash implementation.

---

[24] Mark Gurman, *Apple Races to Temper Outcry Over Child-Porn Tracking System*, BLOOMBERG, https://www.bloomberg.com/news/articles/2021-08-13/apple-warns-staff-to-be-ready-for-questions-on-child-porn-issue (last updated Aug. 13, 2021, 6:31 PM EDT).

[25] Zack Whittaker, *Apple Delays Plans to Roll Out CSAM Detection in iOS 15 After Privacy Backlash*, TECHCRUNCH (Sept. 3, 2021, 6:14 AM PDT), https://techcrunch.com/2021/09/03/apple-csam-detection-delayed/.

[26] *Thorn Statement on Apple's Pause of Implementing Child Safety Measures*, THORN (Sept. 3, 2021), https://www.thorn.org/blog/thorn-statement-on-apples-pause-of-implementing-child-safety-measures/.

Apple Cancels NeuralHash

122. On or about December 7, 2022, Apple announced it would not implement NeuralHash or any other child pornography detection tools on its products.

123. In explaining the reason why it chose to abandon the development of an iCloud CSAM detection feature, Apple executives stated:

> "We've chosen a very different path—one that prioritizes the security and privacy of our users. Scanning every user's privately stored iCloud content would in our estimation pose serious unintended consequences for our users . . . [s]canning for one type of content, for instance, opens the door for bulk surveillance and could create a desire to search other encrypted messaging systems across content types (such as images, videos, text or audio) and content categories..."[27]

124. By December 16, 2022, Apple had quietly removed several references to NeuralHash from its website.[28]

125. Apple solicited customers, including Plaintiffs and the public, on the open market and encouraged the use of its defective products.

126. Apple sells its products to the consumer with dangerous standardized features and designs that users, like Plaintiffs, cannot bargain to change.

127. Plaintiffs and millions of other U.S. consumers confer a benefit to Apple in exchange for using their products.

---

[27] Emails between Erik Neuenschwander, Director of User Privacy and Child Safety at Apple, and Sarah Gardner, CEO at Heat Initiative (Aug. 30-31, 2023), https://s3.documentcloud.org/documents/23933180/apple-letter-to-heat-initiative.pdf.

[28] Dominik Bärlocher, *Neuralhash: Apple Removes All Mentions of CSAM detection from Website*, DIGITEC (Dec. 16, 2021), https://www.digitec.ch/en/page/neuralhash-apple-removes-all-mentions-of-csam-detection-from-website-22203.

128. Apple could have, but purposefully failed to, design its products to protect and avoid injury to victims of known hashed CSAM, such as Plaintiffs.

129. Apple knew or should have known that known hashed CSAM depicting Plaintiffs would continue to spread through Apple's products without implementing proactive detection technologies.

130. Apple knew or should have known that the design of its products attracts, enables, and facilitates child predators and that such predators use its apps to recruit and sexually exploit children for CSAM production and distribution using Apple's products.

131. Despite this knowledge, Apple avoided design changes that would have increased the safety of CSAM victims. Apple nonetheless pressed ahead with selling its products without these changes.

132. Apple was in a superior position to control the risks of harm, ensure the safety of its products, insure against defects, and spread the costs of any harm resulting from the defects.

133. Plaintiffs and the public did not have, and could not have, as much knowledge as Apple about Apple's products and how they were defectively designed.

134. Consumers, including Plaintiffs, could not have inspected the products before accepting them to learn of the defects or the harms that flow from them.

Apple's Child Safety Employees Depart the Company

135. Shortly after Apple failed to implement NeuralHash or other child safety technologies to detect CSAM, Apple's director of investigations and child safety, Melissa Marrus Polinsky, and its trust and safety director, Margaret Richardson, left the company.[29]

136. Around the same time, Apple's chief privacy officer, Jane Horvath, iCloud lead, Michael Abbott, and the purported lead engineer on CSAM detection software, Abhishek Bhowmick, also left the company.[30]

137. Upon information and belief, had Apple implemented NeuralHash or other tools designed to detect known CSAM, these offenders' accounts would have been disabled and reported to NCMEC to prevent further distribution of CSAM depicting Plaintiffs Amy, Jessica, and all others similarly situated.[31]

138. Apple's failure to implement NeuralHash or any other CSAM detection features is a design defect. Apple can safely implement readily available features to prevent the spread of Plaintiffs' CSAM but fails to do so.

Plaintiff Amy of the Misty Child Pornography Series

139. Plaintiff "Amy" was first identified by NCMEC in the early 2000s, and since then, thousands of files from the "Misty" child pornography series have been included in thousands of law enforcement submissions to NCMEC for child victim identification.

[29] *Id.*
[30] *Id.*
[31] *See id.*

140. Plaintiff "Amy" has elected to receive notices via the United States Department of Justice Victim Notification System (VNS), which alerts her representatives when she is a potential victim in federal and state law enforcement agency investigations.

141. Analysts at NCMEC match CSAM images found in criminal circulation to CSAM images of "Amy" in NCMEC's database and notify the government of its findings in a Child Victim Identification report (hereinafter "CVIP").

142. Amy was under 10 years old when she was repeatedly raped and sexually exploited by an adult male relative to produce child pornography. The child sex abuse images and videos of her memorialize Amy being forced to endure sexual abuse and bodily penetration as a young child.

143. Amy was sexually abused as a minor specifically to produce CSAM to share on the internet.

Plaintiff Jessica of the Jessica Child Pornography Series

144. Plaintiff "Jessica" was first identified by NCMEC in the early 2000s, and since then, thousands of files from the "Jessica" child pornography series have been included in thousands of law enforcement submissions to NCMEC for child victim identification.

145. Plaintiff "Jessica" has elected to receive notices via the United States Department of Justice VNS, which alerts her representatives when she is a potential victim in federal and state law enforcement agency investigations.

146. Analysts at NCMEC match CSAM found in criminal circulation to CSAM of Plaintiffs in NCMEC's database and notify the government of its findings in a CVIP.

147. The Jessica series shows Jessica being sexually abused and exploited as a minor by one or more adult male relatives.

148. Jessica was forced to endure sexual abuse and bodily penetration as a minor specifically to produce CSAM to share on the internet.

Plaintiffs Amy and Jessica are Victims of Repeated and Preventable CSAM Crimes Occurring on Apple's Products

149. The unending collection and trading of CSAM depicting Amy and Jessica has caused them long-lasting and permanent harm.

150. Unlike victims of time-limited trauma, CSAM victims are aware that CSAM depicting them will never cease to exist.

151. Amy and Jessica have been and will be repeatedly re-victimized by criminal individuals who regularly possess, trade, and/or distribute the CSAM depicting them.

152. After Apple failed to implement NeuralHash or any other child safety features to detect known CSAM on Apple's products, the Plaintiffs were victimized because the CSAM depicting them was received, possessed, and distributed using Apple products.

153. The following criminal offenders are examples of the many hundreds of individuals who were charged and/or convicted for possessing the same known detectible CSAM depicting known class members, all similarly situated to Plaintiffs, involving Apple's products:

Last	First	Middle	Docket #
Ahr	Mark	M.	2:18.cr.00053
Aiken	Michael		1:19.CR.00096
Ainslie	Justin		21-CR-00082
Alcock	David		21.CR.00162

Angwin	John	C.	19.CR.00335
Bagley	Tonya		9:20.cr.80069
Batt	Michael	John	22.CR.00164
Bates, Jr.	Christopher		24-CR-00033
Behravesh	Bardia		2:22-CR-20069
Bianco	Nicholas	Anthony	2:21.CR.00627
Black	Mark	Alan	1:23-CR-00146
Boyet	Jason		20.CR.00051
Broadhurst	Kyle	Scott	11-CR-00121
Browne, Jr.	Charles	F.	3:20.CR.00965
Burch	Seth		18-00144-01
Calle	Ruben	Eric	19.CR.00613
Carawan	Zachary		1:21.cr.00153
Castillo	Carlos		8:20.CR.00166
Cassidy	Paul	Joseph	2:19.cr.00357
Castro	Carlos	Rafael	1:20.CR.00035
Cerda	Eric	Anthony	8:20-CR-00192
Chin	Parrish		1:18.CR.00222
Christian	Max		1:22.cr.00183
Clark	Brian	Michael	4:20-CR-00329
Clark	Michael	B.	2:18.cr.00048
Clarke	Jaden	Nicholas	22.CR.60149
Coates Jr.	Larry		6:21-CR-10037
Cooney	Bryan	Matthew	18.CR.00273
Cope-Gass	Tyler	Wayne	5:24-cr-20115
Crews	Travis	Ray	23.CR.03134
Currie	Charles		8:21.cr.00142
Daly	Michael		23-CR-00041
Das	Abhijeet		2:18-CR-25
Demarais	Jacob	Bradley	1:21.CR.00130
Demers	Sebastian		22-CR-00133
Desilva	Matthew	Dean	1:21.CR.00065
Durel	Timothy	James	2:23-CR-00132
Edgerly	Shane	Allen	18-CR-00124
Elizondo	Theodore	H.	1:20-CR-00850
Ernest	Matthew		21-CR-00108
Ferguson	John	A.	4:22-cr-00190
Fuentes	Luis	Daniel	23-CR-00049
Galpin	Edward		3:20.MJ.00553
Gates	William		1:18-CR-10374
Gilmore	Dakotah	James	22.CR.05003

Gilreath	Wesley	David	1:19.CR.00384
Gomez	David		2:22-CR-00020
Guillette	Sean		19.cr.00122
Hazouri	Thomas	Lester	20.cr.00119
Hertz	Peter	Henry	14-CR-00146
Hogan	Cody	Dillon	3:20-CR-00143
Holm	Michael		21.CR.00153
Hook	Keith	E.	5:18-MJ-00381
Horwath	Timothy	Allen	2:19.CR.00216
Hutson	James	Alexander	21-CR-00431
Jasperse	Carl	Lee	9:21.CR.80025
King	Benjamin	Nicholas	19.CR.00062
Kovacs	James	D.	18.cr.00588
Kuhns	Travis		2:20.CR.00090
Lukassen	Gregory		8:20.CR.00268
Martinez	Mario	F.	21.cr.00009
Martinez	Timothy		20.CR.00098
McReynolds	Christopher		1:20.cr.00331
Miozza	Todd		22.CR.10237
Mollick	Joseph	Andrew	21.CR.00452
Moore	Roger	W	2:21.cr.00040
Morozewicz	Daniel		21.CR.00152
Morrow	Brian	Kevin	1:22-cr-00231
Novak	Stephen	J.	19-CR-00475
O'Connor	Richard		23-CR-00027
Osinski	Ryan		21.MJ.07003
Ostrowski	Matthew		1:20.CR.00183
Paulino	Eric		1:19.CR.00434
Piontek	Andrew	Nathaniel	0:19-cr-00093
Ramirez	Armando		21.cr.00260
Reyna	Ricardo		5:22.CR.00685
Riedesell	Shawn		24-CR-00012
Risso	Brian		5:22-CR-00343
Sabol	Brandon		3:21.CR.00020
Salas, Jr.	Salvador		0:21.CR.00077
Sheehan	Dustan	David	23-CR-00155
Spencer	Ryan	Michael	3:17-cr-00259
Stacy	Nicholas	James	3:18.CR.00638
Taylor	Donnie		2:18-CR-7
Thompson	Robert	James	1:22.CR.00077
Towle	Hunter	A.	4:21.CR.03019

Villatoro	Isaac	Alberto	2:22.CR.00002
Voegele	Patrick	A.	3:19.CR.00040

154. Victims discovered in the above cases include Alice (depicted in the At_Dawn child pornography series), Andy (depicted in the SpongeB child pornography series), Angela (depicted in the Angela child pornography series), Anna (depicted in the MiddleModelSister child pornography series), April (depicted in the AprilBlonde child pornography series), Carrie (depicted in the FaceBaby child pornography series), Casseaopeia (depicted in the Lighthouse 3 child pornography series), Chelsea (depicted in the 2crazygurls child pornography series), Dipper (depicted in the Jester child pornography series), Emily (depicted in the Tightsngold child pornography series), Erika (depicted in the PinkHeartSisters1 child pornography series), Fiona (depicted in the BluesPink1 child pornography series), Ivy (depicted in the JBN Flowers2 child pornography series), Jack (depicted in the Rap72 child pornography series), Jane (depicted in the CinderBlockBlue child pornography series), Jenny (depicted in the Jenny child pornography series), Jordan (depicted in the BluesPlaid4 child pornography series), Julie (depicted in the JBN Flowers1 child pornography series), Kiera (depicted in the BluesPink3 child pornography series), Lana (depicted in the Youngest Model Sister child pornography series), Matthew (depicted in the BlueButterfly and Honeycomb child pornography series), Raven (depicted in the Teal&PinkPrincess2 child pornography series), Sarah (depicted in the MarineLand1 child pornography series), Sloane (depicted in the Tara child pornography series), Taylor (depicted in the RedGlassesCry child pornography series), Tori (depicted in the PinkHeartSisters2 child pornography series), and Wyatt (depicted in the HarleyDude1 child pornography series), are all members of the Class and were similarly victimized by the easily

identified criminal offenders listed in the chart who were charged and/or convicted for possessing the same known detectible CSAM depicting them

155. "Ava" (depicted in the Sweet Purple Sugar child pornography series), "Mya" (depicted in the Sweet Pink Sugar child pornography series), and "Pia" (depicted in the Sweet White Sugar child pornography series), are sisters who were sexually abused by an adult male. "Pia" was a toddler when the abuse began, while her sisters were approximately 5 and 6 years old. The abuse continued over several years. The children were groomed and encouraged to engage in sexual acts for and with an adult male who recorded and shared the images of their sexual abuse with others. The images include photographs and videos of the children in the nude, in provocative poses, and being sexually assaulted. Each of them suffers profound emotional injury due to the circulation of their child sexual abuse material on the internet. Ava, Mya, and Pia are members of the proposed Class.

156. "Lily" (depicted in the Vicky child pornography series) was sexually abused from approximately ten to eleven years old in several scripted and costumed vignettes, which have included graphic sex as well as bondage. She has been stalked on the internet and through email by apparent pedophiles and child pornography enthusiasts who have propositioned her and made lewd inquiries about her. Lily is a member of the proposed Class.

157. "Maureen" (depicted in the Lighthouse1 child pornography series) was a toddler when her abuse began, and the abuse continued for several years until she was approximately eight years old. An unrelated adult male, known as "Uncle Charlie," would wake Maureen and sexually abuse her during the night. Her abuse was filmed, and the images created show

Maureen being vaginally and anally penetrated, being forced to perform oral sex on an adult male, and being dressed up in costumes, then undressed and sexually assaulted for viewers. Maureen is a member of the proposed class.

158. "Maria" (depicted in the BestNecklace child pornography series) was approximately ten years old when a child abuser reached through the internet to groom and then extorted her to send him self-produced sexual videos of herself. She has been humiliated and sunk into a profound depression. Her videos continue to circulate frequently on the internet. Maria is a member of the proposed Class.

159. "Sally" (depicted in the Jan_Socks4 child pornography series), "Savannah" (depicted in the Jan_Socks2 child pornography series), and "Skylar" (depicted in the Jan_Socks3 child pornography series), all sisters, were forced from a young age by adults to have sexual encounters, including digital and penile penetration and oral copulation with an adult male and minor male to produce child pornography images and videos. Skylar, Savannah, Sally, and Sierra each have and will continue to suffer personal injury by the distribution and possession of child pornography depicting them by persons, including the Defendant. Sally, Savannah, and Skyler are members of the proposed Class.

160. "Donatello" (depicted in the Feb212 child pornography series), "Solomon" (depicted in the J_Blonde child pornography series), "Jessy" (depicted in the Sufer Hair child pornography series), and "Kuazie" (depicted in the RapJerseys child pornography series), were each abused and photographed by adult males who insinuated themselves into the confidence of these young men and seduced them into performing erotic and sexual acts for the camera. These images have been circulated on the internet for years, all to the great distress and injury

of the victims depicted. Donatello, Solomon, Jessy, and Kuazie are members of the proposed Class.

161. "Violet" (depicted in the At School child pornography series) was sexually abused by an adult male from approximately four to seven years old. She suffered vaginal penetration, oral penetration, and other humiliating sexual acts forced upon her. These instances of abuse are the subject of videos and images circulating currently on the internet. Violet is recognizable today as the child she was in these images and videos. She is subject to significant psychological injury should her legal name be in the public record associated with these images and videos. Violet is a member of the proposed Class.

162. "Henley"(depicted in the BluePillow1 child pornography series) was sexually abused approximately between the ages of five and twelve years old by an adult male who forced her to perform penetrative sexual acts, provocative posing for the camera, and exposure of her genitals, some of which occurred while she was drugged or sleeping. Images and videos of Henley's sexual abuse circulate on the internet, causing her anxiety, fear, depression, and other forms of emotional distress. Henley is a member of the proposed Class.

163. "Cara" (depicted in the MotorCoach1 child pornography series) was a child between the approximate ages of eight and ten when an adult male sexually abused her by committing acts of penetration, forcing exposure of her genitals and breasts, and engaging in ejaculation on her body; some of these things occurred while she was drugged or sleeping. Images and videos of Cara's sexual abuse have circulated on the internet for twenty or more years, generating significant and continuing emotional injury for her. Cara is a member of the proposed Class.

164. Plaintiffs and all members of the Class were similarly victimized by other easily identified criminal offenders who were also charged and/or convicted for possessing the same known detectible CSAM depicting them.

165. Upon information and belief, the number of known hashes matched would have surpassed Apple's threshold and triggered a report to NCMEC regarding CSAM depicting Amy, Jessica, and others similarly situated.

166. On or about August 28, 2019, a senior user experience designer for Apple submitted a letter of support for criminal Defendant James Kovacs, who was charged with possessing Plaintiff Amy's CSAM. This letter stated: "I have read the information provided by Jimmy's lawyer that details that he has been convicted of possession of child pornography, and that Jimmy has admitted he possessed more than 600 images or videos, and that those images and videos contained prepubescent minors and the sexual exploitation of toddlers. Considering the above paragraph's details, I believe that Jimmy is at his core a decent man[.]"

167. Similarly, proposed class members "Jenny" of the "Jenny" child pornography series, "Raven" of the "Teal&PinkPrincess2" child pornography series, "Anna" of the "MiddleModelSister" child pornography series, "Cara" of the "MotorCouch" child pornography series, "Lily" of the "Vicky" child pornography series, "Sarah" of the "Marineland1" child pornography series, "Savannah" of the "Jan_Socks2" child pornography series, "Skylar" of the "Jan_Socks3" child pornography series, "Maureen" of the "Lighthouse1" child pornography series, "Violet" of the "At School" child pornography series, "Jesy" of the "Surfer Hair child" pornography series, "Mya" of the "Sweet Pink Sugar" child pornography series, and "Maria" of the "Best Necklace" child pornography series were all victimized by child

pornographer Joseph Andrew Mollick who was charged in the United States District Court, Northern District of California, in *United States v. Joseph Andrew Mollick,* (NDCA) Case No. 3:21-cr-00452-VC-1, with the crime of Possession of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). On January 9, 2023, Mollick pleaded guilty to Possession of Child Pornography as charged and was sentenced on May 24, 2023.

168. A related Forbes review of Mollick's case found that Apple's systems have been used to store and transmit thousands of items of CSAM between 2014 and 2023. Indeed, Forbes recognized "That Apple didn't flag the illegal material isn't surprising."[32]

Apple Continues to Fail Child Victims

169. To date, Apple does not proactively detect child pornography, including storage or communications, to assist law enforcement in stopping child exploitation.

170. In 2023, while four leading tech companies submitted over 32 million reports of CSAM to NCMEC, Apple submitted only 267 reports of known, suspected, or apparent violations of child pornography laws.[33]

[32] Thomas Fox-Brewster & Alexandra S. Levine, *Inside Apple's Impossible War on Child Exploitation*, FORBES (Sept. 7, 2023, 2:01 PM EDT), https://www.forbes.com/sites/thomasbrewster/2023/09/07/apple-icloud-child-sexual-abuse-material-privacy/.

[33] *2023 CyberTipline Reports by Electronic Service Providers*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, https://www.missingkids.org/content/dam/missingkids/pdfs/2023-reports-by-esp.pdf (last accessed Nov. 20, 2024).

171. In 2023, Apple's reporting numbers to NCMEC were in stark contrast to its big tech peers, with Google reporting to NCMEC more than 1.47 million instances of apparent violations of child pornography laws and Meta reporting more than 30.6 million.[34]

172. Data investigations by the National Society for the Prevention of Cruelty to Children ("NSPCC") revealed that Apple was implicated in 337 recorded offenses of CSAM between April 2022 and March 2023 in England and Wales.[35]

173. The NSPCC found that "Apple is failing to effectively monitor its platforms or scan for images and videos of the sexual abuse of children, child safety experts allege, which is raising concerns about how the company can handle growth in the volume of such material associated with artificial intelligence."[36]

174. Although Apple is required to report all apparent violations of child pornography crimes to NCMEC pursuant to its reporting requirements prescribed by 18 U.S.C. 2258A, Apple nonetheless fails to report known and detected CSAM depicting Plaintiffs and Class members.

175. Representatives of the NSPCC further stated, "[t]here is a concerning discrepancy between the number of UK child abuse image crimes taking place on Apple's

[34] *UK Watchdog Accuses Apple of Failing to Report Sexual Images of Children*, GUARDIAN (July 22, 2024, 3:00 EDT), https://www.theguardian.com/technology/article/2024/jul/22/apple-security-child-sexual-images-accusation.
[35] *Id.*
[36] *Id.*

services and the almost negligible number of global reports of abuse content they make to authorities[.]"[37]

176. In 2024, Apple rolled out a child safety feature within the iOS 18.2 beta update, which, for the first time, allows minor children to report CSAM or inappropriate content directly to Apple.[38] When the minor attempts to report the content, the child is presented with intervention popups explaining how to contact the local authorities and inform their parents.[39] This feature is not available to users within the United States.

177. Currently, Apple's child safety reporting feature is only available in Australia. Thus, this feature is unavailable to Plaintiffs or members of the United States-based similarly situated class.[40]

CLASS ACTION ALLEGATIONS

178. Plaintiffs bring this proposed class action for damages and injunctive relief pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and 23(c)(4), on behalf of themselves and the following "Class":

> **Nationwide Class:** All persons who were under eighteen years of age at the time they were depicted in any child pornography that has been hashed by the National Center for Missing and Exploited Children and which has been made

---

[37] *See id.*
[38] Amber Neely, *Apple Testing Out New Child Safety Measures in Australia*, APPLEINSIDER (Oct. 24, 2024), https://appleinsider.com/articles/24/10/24/new-feature-allows-children-to-report-inappropriate-content-directly-to-apple.
[39] *Id.*
[40] *Id.*

available on Apple's products, including iCloud, from August 5, 2021, to the date of class notice.

Cvajs bcb **from the Class:** Defendant herein and any person, firm, trust, corporation, or other entity related to or affiliated with Defendant.

Numerosity: The class members are so numerous that joining all members is impracticable. While the exact number of Class Members remains unknown at this time, upon information and belief, Defendant, through their actions alleged herein, victimized thousands of users. The actual number of CSAM survivors will be ascertained through discovery.

Predominance of Common Questions of Law and Fact: There are questions of law and fact that are common to the Class that predominate over any questions affecting only individual members, including the following:

- Whether Plaintiffs and the other Class Members have been harmed by Apple's conduct as alleged herein;
- Whether Apple's defectively designed products resulted in the distribution of known hashed CSAM depicting the Plaintiffs and class members.
- Whether Apple was unjustly enriched by its deceptive practices;
- Whether Plaintiff and members of the proposed class are entitled to declaratory or injunctive relief to halt Apple's practices and to their attorney fees, costs, and expenses; and

- Whether Plaintiff and members of the proposed class are entitled to any damages or restitution incidental to the declaratory or injunctive relief they seek or otherwise, and to their attorney fees, costs, and expenses related to any recovery of such monetary relief.

Adequacy of Representation: Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the other Class Members, and the infringement of their rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Plaintiffs' counsel is competent and has a wealth of experience litigating claims regarding sex abuse, sex trafficking and exploitation of minors, complex commercial litigation, and class actions. Plaintiffs and counsel intend to prosecute this case vigorously and will fairly and adequately protect the Class's interests. Neither Plaintiffs nor their counsel have any interests adverse to those of the other members of the Class

Typicality: Plaintiffs' claims are typical of those of the other Class Members because, inter alia, all Class members were injured through the common misconduct described above and were subject to Apple's unlawful conduct. Plaintiffs are advancing the same claims and legal theories on behalf of

themselves and all Class members and were subject to Apple's unlawful conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all Class members.

The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, establishing incompatible standards of conduct for the party opposing the Class.

Insufficiency of Separate Actions: Absent a class action, Plaintiffs and Class members will continue to suffer the harm described herein, for which they would have no remedy. Even if individual consumers could bring separate actions, the resulting multiplicity of lawsuits would cause undue burden and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated plaintiffs, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendant. Finally, Class treatment would minimize the trauma that Class members would experience because of litigating their claims individually, and further promotes the remedial purposes of the federal statutes under which the claims are brought.

179. Plaintiffs reserve the right to modify or amend the definition of the proposed Class and (alternative) state classes before the Court determines whether certification is appropriate and as the parties engage in discovery.

180. **Injunctive Relief:** Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and all members of the Class, thereby making appropriate final injunctive relief, as described below, concerning the members of the Class as a whole. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication concerning individual members, establishing incompatible standards of conduct for the Defendant. And adjudications of claims of the individual members of the Class and Subclasses against Defendant would, as a practical matter, be dispositive of the interests of other members of the putative Classes who are not parties to the adjudication and may substantially impair or impede the ability of other members to protect their interests.

181. Plaintiffs broadly plead all Causes of Action of this Complaint, pursuant to all laws that may apply under choice-of-law principles. To the extent applicable to specific Causes of Action, Plaintiffs plead these Causes of Action under all applicable product liability acts, statutes, and laws of their respective states.

182. Notice of a certified class action and any result or resolution of the litigation can be provided to Class Members by first-class mail, email, publication, or such other notice methods as deemed appropriate by the Court.

183. Plaintiffs do not anticipate any difficulty in managing this litigation.

COUNT I

CIVIL REMEDY FOR VICTIMS OF CHILD PORNOGRAPHY FOR VIOLATIONS OF 18 U.S.C. §§ 2252, 2252A, AND 2255
(Plaintiffs and the Nationwide Class)

184. Plaintiffs repeat and reallege all prior paragraphs as if fully incorporated herein.

185. Plaintiffs and Class members were minors and victims of violations of Sections 2252 and 2252A and suffered personal injury because of such violations and are eligible to sue and recover damages and other forms of relief under 18 U.S.C. § 2255.

186. Defendant committed violations of 18 U.S.C. §§ 2252 and 2252A.

187. Defendant knowingly received, possessed, and distributed CSAM depicting Class members, including Plaintiffs.

188. Defendant's receipt, distribution, advertising, and possession of CSAM occurred in or affected interstate or foreign commerce.

189. The Plaintiffs were each a victim of Defendant Apple's violations of 18 U.S.C. § 2252.

COUNT II

STRICT LIABILITY – DESIGN DEFECT
(Plaintiffs and the Class Against Apple)

190. Plaintiffs repeat and reallege all prior paragraphs as if fully incorporated herein.

191. At all relevant times, Defendant designed, developed, managed, operated, tested, produced, labeled, marketed, advertised, promoted, controlled, sold, supplied, distributed, and benefitted from its products used by Plaintiffs and criminals circulating Plaintiffs' known hashed CSAM.

192. Apple's products are designed and intended to be technology products.

193. Apple's products are distributed and sold to the public through retail channels (i.e., physical Apple stores, online retail channels such as websites, and the Apple App Store).

194. Apple's products are marketed and advertised to the public for personal use by the end-user/consumer.

195. Apple defectively designed its products to permit the ongoing spread and circulation of Plaintiffs' and class members' known hashed CSAM.

196. The defects in the design of Apple's products existed before the release of these products to Plaintiffs and the public, and there was no substantial change to Apple's products between the time Apple made them available to the public or retail channels and the time of their distribution to Plaintiffs and criminal offenders.

197. Plaintiffs used these products as intended, and Apple knew or, by exercising reasonable care, should have known that Plaintiffs and criminal offenders would use these products without inspection.

198. Apple defectively designed its products to permit, promote, and acquiesce the ongoing circulation of known hashed CSAM.

199. Apple failed to test the safety of its products. While Apple performed some product testing and knew of ongoing harm to the Plaintiffs, it failed to adequately remedy its respective product's defects or warn the Plaintiffs.

200. Apple's products are defective in design and pose a substantial likelihood of harm for the reasons set forth herein because the products fail to meet the safety expectations of ordinary consumers when used in an intended or reasonably foreseeable manner and because the products are less safe than an ordinary consumer would expect when used in such a manner.

201. Apple's products are likewise defectively designed in that they create an inherent risk of danger; specifically, a risk of failing to stop the spread and circulation of CSAM depicting the Plaintiffs and a risk of revictimization and repreparation of CSAM crimes against Plaintiffs, which can lead to a cascade of harms. Those harms include but are not limited to exposure to predators, sexual exploitation, dissociative behavior, withdrawal symptoms, social isolation, damage to body image and self-worth, increased risky behavior, and profound mental health issues, including but not limited to depression, anxiety, suicidal ideation, self-harm, insomnia, eating disorders, death, and other harmful effects.

202. The risks inherent in the design of Defendant's products significantly outweigh any benefit of such design.

203. Apple could have utilized cost-effective, reasonably feasible alternative designs, including algorithmic changes and changes to the addictive features described above, to minimize the harms described herein, including, but not limited to:

- Implementing pro-active CSAM detection measures and systems on iCloud;
- Implementing freely available and industry-proven child protection API tools such as Project Arachnid Shield to help limit and prevent child sexual exploitation, sextortion, and distribution of known CSAM through their products;

- Implementing the legal definition of child pornography under 18 U.S.C. § 2256(8) and related case law when reviewing detected CSAM to prevent underreporting of known CSAM;
- Implementing all available, proactive detection measures to detect and report known CSAM on iCloud and Apple devices.

204. Alternative designs were available to reduce the spread of known hashed CSAM on Apple products and would have served the same purpose as Defendant's products while reducing the gravity and severity of the danger posed by those products' known defects.

205. Plaintiffs and criminals trafficking in Plaintiffs' CSAM used Defendant's products in reasonably foreseeable ways.

206. Plaintiffs' physical, emotional, and economic injuries were reasonably foreseeable to Apple during their products' development, design, advertising, marketing, promotion, and distribution.

207. Apple's products were defective and unreasonably dangerous when they left Apple's possession and control. The defects continued to exist through the products' distribution to and use by consumers, including Plaintiffs, who used the products without any substantial change in the product's condition.

208. Plaintiffs were injured as a direct and proximate result of each of Apple's defectively designed products as described herein. The defective design was a substantial factor in causing harm to the Plaintiffs.

209. As a direct and proximate result of Apple's defective design, the Plaintiffs suffered serious and dangerous injuries.

210. As a direct and proximate result of Apple's products' defective design, Plaintiffs require and/or will require more healthcare and services and did incur medical, health, incidental, and related expenses.

211. The Plaintiffs' injuries cannot be wholly remedied by monetary relief, and such remedies at law are inadequate.

212. The nature of the fraudulent and unlawful acts that created safety concerns for Plaintiffs is not the type of risk immediately apparent from using Apple's products. Plaintiffs are continuing to use Apple's products. When Plaintiffs use Apple's products, they cannot independently verify that Apple's products continue to pose an unreasonable risk, nor will they rely on Apple's representations in the future.

213. Apple's conduct, as described above, was intentional, fraudulent, willful, wanton, reckless, malicious, fraudulent, oppressive, extreme, and outrageous, and displayed an entire want of care and conscious and depraved indifference to the consequences of its conduct, including to the health, safety, and welfare of its customers, and warrants an award of punitive damages in an amount sufficient to Apple and deter others from like conduct.

214. Plaintiffs demand judgment against Apple for injunctive relief and compensatory, treble, and punitive damages, together with interest, costs of suit, attorney's fees, and all other relief as the Court deems proper.

COUNT III

NEGLIGENCE PER SE
(Plaintiffs and the Class Against Apple)

215. Plaintiffs repeat and reallege all prior paragraphs as if fully incorporated herein.

216. Apple had an obligation to comply with applicable statutes and regulations, including but not limited to the PROTECT Our Children Act (18 U.S.C. §§ 2258A, 2258B).

217. Apple owed a heightened duty of care to CSAM victims to implement effective proactive detection measures that would prevent the distribution of known hashed CSAM.

218. Apple's actions, as described herein, violated these statutes and regulations and other federal laws.

219. Apple failed to meet the requirements of 18 U.S.C. § 2258A by not reporting to NCMEC the violations of child pornography laws they knew existed within their respective products.

220. Specifically, Apple intentionally designed its products to limit and avoid its reporting requirements under federal law.

221. Apple also failed to minimize the number of its respective employees with access to visual depictions of Plaintiffs in violation of 18 U.S.C. § 2258B(c).

222. Plaintiffs are within the class of persons these statutes and regulations are intended to protect. This includes Plaintiffs who, as victims of child pornography, are within the scope of persons the PROTECT Our Children Act is intended to protect.

223. Plaintiffs' injuries and/or symptoms are the type of harm these statutes and regulations intend to prevent.

224. Violations of the foregoing statutes and regulations, among others, by Apple constitute negligence per se.

225. As a direct and proximate result of each of Apple's statutory and regulatory violations, Plaintiffs suffered serious injuries and/or sequelae thereto, including but not limited to emotional distress, diagnosed mental health conditions, loss of income and earning capacity, reputational harm, physical harm, past and future medical expenses, and pain and suffering.

226. As a direct and proximate result of each of Apple's statutory and regulatory violations, Plaintiffs require and/or will require more healthcare and services and did incur medical, health, incidental, and related expenses.

227. Plaintiffs may also require additional medical and/or hospital care, attention, and services in the future.

228. As a result of Apple's negligence per se, Plaintiffs suffered severe mental harm, leading to physical and psychological injury, from use of and exposure to Apple's products.

229. Plaintiffs suffered severe damages in the form of emotional distress, diagnosed mental health conditions, medical expenses, loss of income and earning capacity, pain and suffering, and reputational harm.

230. Plaintiffs have suffered and will continue to suffer physical harm, emotional distress, past and future medical expenses, and pain and suffering.

231. Apple's conduct, as described above, was intentional, fraudulent, willful, wanton, reckless, malicious, fraudulent, oppressive, extreme, and outrageous, and displayed an entire want of care and conscious and depraved indifference to the consequences of its conduct, including to the health, safety, and welfare of their customers, and warrants an award

of punitive damages in an amount sufficient to punish Apple and deter others from like conduct.

232. Apple is further liable to Plaintiffs and Consortium Plaintiffs for punitive damages based upon its willful and wanton conduct toward victims of child pornography, including Plaintiffs whom they knew would be seriously harmed by Apple's products.

COUNT IV

NEGLIGENCE
(Plaintiffs and the Class Against Apple)

233. Plaintiffs repeat and reallege all prior paragraphs as if fully incorporated herein.

234. Apple had a duty to exercise reasonable care in the design, manufacture, testing, marketing, and distribution into the stream of commerce of Apple's innovative technology products, including iCloud, iPhone, MacBook, and iPad. Apple's duty to exercise reasonable case included ensuring that Apple's products, including iCloud, did not pose a significantly increased risk of injury to victims of known detectible CSAM depicting the Plaintiffs and those Class members similarly situated.

235. Apple failed to exercise reasonable care in the design, manufacture, testing, marketing, and distribution into the stream of commerce of Apple's innovative technology products, including iCloud, iPhone, MacBook, and iPad. Apple knew or, in the exercise of reasonable care, should have known that such products put into the stream of commerce without appropriate industry-proven child safety protection features could present a danger if child predators and child abusers used their products, and therefore were not safe for use.

236. Even though Apple knew or should have known that its innovative technology products, including iCloud, iPhone, MacBook, and iPad would fail to stop the spread of known detectible CSAM and therefore create pain and suffering, Apple continued to market as safe its innovative technology products, including iCloud, iPhone, MacBook, and iPad.

237. As a direct and proximate result of Apple's negligence, Plaintiffs and the Class have suffered significant damages, including but not limited to physical injury, pain and suffering, and further treatment, and will continue to suffer such damages in the future. In taking the actions and omissions that caused these damages, Defendant was guilty of malice, oppression, and fraud, and Plaintiff is therefore entitled to recover punitive damages.

COUNT V

NEGLIGENT MISREPRESENTATION
(Plaintiffs and the Class Against Apples)

238. Plaintiffs repeat and reallege all prior paragraphs as if fully incorporated herein.

239. At common law, the elements of negligent misrepresentation are: (1) the defendant had a duty, as a result of a special relationship, to give correct information; (2) the defendant made a false misrepresentation that it should have known was incorrect; (3) the information supplied in the representation was known by the defendant to be desired by the plaintiff for a serious purpose; (4) plaintiff intended to rely and act upon it; and (5) the plaintiff reasonably relied on it to his detriment. This differs from a fraudulent misrepresentation because the party making the misrepresentation need not be aware that the representation is false and need not intend the other party to act on it.

240. Plaintiffs and the Class engaged in business transactions with Defendant to purchase goods from Apple and other third-party retailers. These purchases were made and induced based on Apple's misrepresentations as set forth herein.

241. Plaintiffs and the Class reasonably relied on said misrepresentations when making their purchases. As a result, Plaintiff and the Class suffered monetary damages.

RELIEF REQUESTED

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court enter a judgment on their behalf and against Defendant and further grant the following relief:

A. Certify the proposed Class pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4);

B. Designate Plaintiffs as representatives of the proposed Class and Plaintiffs' counsel as counsel for the Class;

C. Award injunctive or any other equitable relief to Plaintiffs and the Class, requiring Defendant to identify, remove, and report CSAM on iCloud and implement policies, practices, and procedures to prevent continued dissemination of CSAM or child sex trafficking on Apple devices and services.

D. Award all available damages, including but not limited to compensatory and punitive damages, in favor of Plaintiffs and the Class;

E. Award Plaintiffs and the Class prejudgment interest, costs, and attorney's fees;

F. Require restitution and disgorgement of profits and unjust enrichment obtained as a result of Defendant's unlawful conduct;

G. Retain jurisdiction of this matter to ensure all forms of relief it deems appropriate; and

H. Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury.

Dated: December 7, 2024.

Respectfully submitted,

/s/

Micha S. Liberty
Liberty Law
California Bar No. 215687
1999 Harrison Street, Ste. 1800
Oakland, CA 94612
Tel: (510) 645-1000
Email: micha@libertylaw.com

/s/

James R. Marsh (pro hac vice to be filed)
Margaret Mabie (pro hac vice to be filed)
Helene Weiss (pro hac vice to be filed)
Marsh Law Firm PLLC
31 Hudson Yards, 11th Fl
New York, NY 10001
Tel: (212) 372-3030
Fax: (833) 210-3336
Email: jamesmarsh@marsh.law
margaretmabie@marsh.law
heleneweiss@@marsh.law

/s/

Hillary Nappi (pro hac vice to be filed)
Hach Rose Schirripa & Cheverie LLP
112 Madison Avenue, 10th Fl.
New York, NY 10016
Tel : (212) 213-8311
Fax : (212) 779-0028
Email: hnappi@hrsclaw.com

Attorneys for Plaintiffs