West Virginia E-Filing Notice

CC-26-2026-C-16

Judge: Richard Tatterson

To: Troy N. Giatras
troy@thewvlawfirm.com

NOTICE OF FILING

IN THE CIRCUIT COURT OF MASON COUNTY, WEST VIRGINIA
Attorney General v. APPLE, INC.
CC-26-2026-C-16

The following complaintwas FILED on 2/19/2026 8:52:38 AM

Notice Date: 2/19/2026 8:52:38 AM

Elizabeth Jones
CLERK OF THE CIRCUIT COURT
Mason County
200 6th St
POINT PLEASANT, WV 25550

(304) 675-4400
Elizabeth.Jones@courtswv.gov

E-FILED | 2/19/2026 8:52 AM
CC-26-2026-C-16
Mason County Circuit Clerk
Elizabeth Jones

COVER SHEET

GENERAL INFORMATION

IN THE CIRCUIT COURT OF MASON COUNTY WEST VIRGINIA

Attorney General v. APPLE, INC.

First Plaintiff:	□ Business ☑ Government	□ Individual □ Other	**First Defendant:**	☑ Business □ Government	□ Individual □ Other

Judge: Richard Tatterson

COMPLAINT INFORMATION

Case Type: Civil

Complaint Type: Other

Origin: ☑ Initial Filing □ Appeal from Municipal Court □ Appeal from Magistrate Court

Jury Trial Requested: □ Yes ☑ No

Case will be ready for trial by: ______________________

Mediation Requested: □ Yes ☑ No

Substantial Hardship Requested: □ Yes ☑ No

□ Do you or any of your clients or witnesses in this case require special accommodations due to a disability?

- □ Wheelchair accessible hearing room and other facilities
- □ Interpreter or other auxiliary aid for the hearing impaired
- □ Reader or other auxiliary aid for the visually impaired
- □ Spokesperson or other auxiliary aid for the speech impaired
- □ Other: ______________________

□ I am proceeding without an attorney

☑ I have an attorney: Matthew Stonestreet, 118 Capitol St Ste 400 , Charleston, WV 25301

SERVED PARTIES

Name: APPLE, INC.

Address: c/o CT CORPORATION SYSTEM 330 N. Brand Blvd., Suite 700, Glendale CA 91203

Days to Answer: 30 **Type of Service:** Filer - Secretary of State

IN THE CIRCUIT COURT OF MASON COUNTY, WEST VIRGINIA

STATE OF WEST VIRGINIA *ex rel*.,
John B. McCuskey, Attorney General,

Plaintiff,

v.

APPLE, INC.,

Defendant.

COMPLAINT

Case No.:

TABLE OF CONTENTS

Page

NATURE OF THE ACTION 1

PARTIES 4

I. PLAINTIFF 4

II. DEFENDANT 5

JURISDICTION AND VENUE 5

FACTUAL ALLEGATIONS 6

I. APPLE'S PRODUCTS 6

A. **APPLE'S MOBILE DEVICES** 6

B. **iCLOUD** 7

II. APPLE KNOWINGLY PROTECTS ABUSERS AND ITS PRODUCTS HARM CSAM VICTIMS AND THE PUBLIC AT LARGE 11

A. **APPLE KNOWINGLY DESIGNED A PRODUCT ECOSYSTEM THAT FORESEEABLY AIDS THE SPREAD OF CSAM** 14

1. **Encoding, Metadata, and Interface Tools** 14

2. **Encryption** 15

3. **iCloud** 16

B. **APPLE LACKS AN INTEGRATED, SYSTEM-WIDE MECHANISM TO REPORT CSAM IN THE UNITED STATES** 19

III. APPLE BELIEVES ITS BRAND IS PRIVACY, AND THIS REPRESENTS A DESIGN CHOICE FOR ITS ECOSYSTEM 20

IV. APPLE PREVIOUSLY PREPARED TO LAUNCH PROPRIETARY CSAM DETECTION AND REPORTING TOOLS 24

A. **INDUSTRY STANDARDS** 24

B. **APPLE'S PROPOSED CSAM DETECTION AND REPORTING TOOLS** 25

1. **NeuralHash** 26

2. **Matching-Database Setup and Private Set Interaction Protocol ("MDSP")** 27

3. **Threshold Secret Sharing ("TSS")** 28

4. Apple's CSAM Detection Tools Fall Short of the Standard of Care 29

V. APPLE ANNOUNCES AND THEN QUIETLY CANCELS CSAM DETECTION 30

A. APPLE LAUNCHES PRESS TOUR AROUND CSAM DETECTION 30

B. APPLE ABANDONS CSAM DETECTION UNDER PRIVACY ADVOCATES' PRESSURE 34

1. Public Response 34

2. Apple's Broken CSAM Promise 35

C. APPLE CONTINUES TO MISREPRESENT ITS ROLE IN FIGHTING CSAM 37

VI. APPLE'S CONDUCT FACILITATES PREVENTABLE CRIMES 38

VII. APPLE'S CONDUCT IMPACTS WEST VIRGINIA 40

VIII. LEGAL CLAIMS 42

COUNT I 42

COUNT II 45

COUNT III 49

COUNT IV 49

IX. PRAYER FOR RELIEF 51

NATURE OF THE ACTION

1. Apple, Inc. ("Apple") has described itself as the "greatest platform for distributing child porn."[1]

2. Despite that internal admission, in 2023, Apple made just 267 reports of Child Sexual Abuse Material ("CSAM") to the National Center for Missing & Exploited Children ("NCMEC"), far short of its peers, with Google making more than 1.47 million reports and Meta, more than 30.6 million.[2]

3. All manufacturers must construct and sell products that are safe to use. Further, product designers and manufacturers are expected to disclose the truth to consumers when they discover or know of a likelihood that there exists a safety issue or material risk with a product before that product is introduced into commerce.

4. Before August 2021, Apple knew its products contained defects as customers, law enforcement, and non-governmental watchdogs reported various concerns about Apple's role in facilitating the storage and safekeeping of known CSAM despite available alternative designs and technological solutions.

5. Despite internally acknowledging that Apple knowingly enables distribution of CSAM, Apple has maintained a product ecosystem that actively manages a user's content in ways that materially facilitate CSAM's persistence, accessibility, and dissemination.

[1] Sean Hollister, S*weetheart Deals and Plastic Knives: All The Best Emails From The Apple vs. Epic Trial*, VERGE (Aug. 19, 2021, 10:00 AM EDT), available at: https://www.theverge.com/c/22611236/epic-v-apple-emails-project-liberty-app-storeschiller-sweeney-cook-jobs (displaying text message conversation between Apple Anti-Fraud Chief Eric Friedman to Herve Silbert, Security Architect at Apple).

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

6. Within this ecosystem, Apple's flagship digital storage platform, iCloud, plays a pivotal role of enabling user storage of vast troves of data and seamlessly synchronizing the transfer of images across a user's devices. iCloud is not a passive storage device. Rather, it is designed to make image- and video-based content easier to locate, view, share, and retain across devices and applications. For users who traffic in CSAM, such functionality reduces friction associated with maintaining large collections of illicit material, enables repeated access and re-distribution without manual file handling, and allows such material to remain available and organized over long periods of time — thereby contributing to the ongoing circulation and safeguarding of CSAM within Apple's ecosystem.

7. Behind every sexually explicit image or video is a child's rape, molestation, or sexual abuse. CSAM is a permanent record of that child's trauma, forcing upon children a lifetime of re-victimization knowing that documentation of their sexual abuse can be available for others to access forever.[3]

8. The public interest in CSAM lies not just in criminalizing its production, distribution, and receipt, but also its very existence, its possession, and the technologies utilized by its traffickers to store and safeguard it.[4] Indeed, as Apple has itself acknowledged, CSAM is "illegal to possess in most countries, including the United States."[5]

9. Abusers "who seek to sexually exploit children through CSAM can do so from anywhere in the world by using digital devices and the internet. Modern smartphones are the ideal child exploitation tool for offenders," as they can be used to photograph, record, view, and store

[3] UNITED STATES DEPARTMENT OF JUSTICE, *Child Sexual Abuse Material* (June 2023), available at: https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf.

[4] *Id.*

[5] APPLE, *Expanded Protections for Children: Frequently Asked Questions*, v1.1 (August 2021).

CSAM. Modern smartphones also permit offenders to connect with abusers, distributors, and victims.[6]

10. In 2021, Apple announced a proprietary set of CSAM detection tools that purportedly would have limited the presence (and subsequent spread) of CSAM by automatically detecting it and reporting it to the NCMEC.[7] However, by December 2022, in an effort to protect its brand and outsized smartphone and digital storage market share, Apple shelved the update and abandoned the project.

11. The NCMEC has described Apple's record as "rotten" when it comes to child protection. After Apple rolled back its plans for CSAM detection, the NCMEC stated, "[o]ne of the greatest tragedies for survivors of child sex abuse, for families who have lost children due to that trauma, and for overall efforts to end this crime, was Apple's decision to abandon plans to detect child sex abuse material on iCloud. Apple made this decision despite the fact that 90% of Americans assert Apple has a responsibility to detect this illegal content."[8]

12. Apple's decision arrived as CSAM continues to proliferate through digital media. From 2022 to 2023, reports of child sexual abuse material on online platforms grew from 32 million in 2022 to a record high of more than 36 million in 2023.[9]

[6] UNITED STATES DEPARTMENT OF JUSTICE, *Child Sexual Abuse Material* (June 2023), available at: https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf.

[7] Megan Gates, *Apple to Roll Out Scanning to Detect Child Sexual Abuse Images*, SECURITY MANAGEMENT (August 6, 2021), available at: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/august/Apple-to-Roll-out-Photo-Scanning/?utm_source=chatgpt.com.

[8] NATIONAL CENTER ON SEXUAL EXPLOITATION, *The Dirty Dozen List '24*, available at: https://endsexualexploitation.org/apple/.

[9] Will Oremus and Cristiano Lima-Strong, *Child Sex Images Are Booming Online. Congress Wants to Know Why*, WASHINGTON POST (January 28, 2024), available at: https://www.washingtonpost.com/technology/2024/01/28/csam-ncmec-senate-hearing-child-porn/.

13. As described below, Plaintiff, State of West Virginia seeks to hold Apple accountable for its knowing misrepresentations and unlawful conduct arising from its CSAM practices and its choices in designing the iCloud infrastructure. As a direct and proximate result of its conduct, Apple is liable under multiple, independent theories of law, including strict liability for design defect, negligence for failing to implement adequate CSAM reporting technologies, creating or contributing to a public nuisance by facilitating the storage and hosting of unlawful CSAM content, and violations of the West Virginia Consumer Credit and Protection Act.

PARTIES

I. PLAINTIFF

14. Plaintiff, the State of West Virginia, by and through its Attorney General, John B. McCuskey, is charged with protecting the interests of the State and its citizens. The Attorney General is authorized by West Virginia's Constitution, West Virginia common law and by statute to bring this action.

15. John B. McCuskey is the duly elected Attorney General of West Virginia, an independent constitutional officer of the State of West Virginia and its chief law officer, with full authority to institute and prosecute all civil actions in which the State has an interest.

16. The Attorney General is charged with enforcing the West Virginia Consumer Credit and Protection Act, W. Va. Code §§ 46A-1-101, *et seq.* ("WVCCPA"). Pursuant to W. Va. Code § 46A-7-108, the Attorney General is authorized to bring a civil action for violations of the WVCCPA and obtain an injunction and other appropriate relief.

17. The Attorney General is charged with protecting the quasi-sovereign interests in the public health and general welfare of the State. To protect the public health and general welfare of the State and its citizens, prevent ongoing unlawful conduct, recover relief for past, ongoing, and future harms, and to address the possession and storage of CSAM, in part, caused by Apple's

conduct, the Attorney General, on behalf of the State, has standing as *parens patriae* to bring this action.

18. The State, as *parens patriae*, is the ultimate protector of the rights of minors. The State has a substantial interest in providing for their physical and mental health, safety, and welfare.

19. The State is entitled to the protections of sovereign immunity. Pursuant to Article VI, Section 35 of the West Virginia Constitution and W. Va. Code § 55-17-4(3), the filing of this action shall not be construed as a waiver of that immunity and no counterclaim, set-off, recoupment, cross-claim, or other form of avoidance may be asserted in this action against West Virginia.

II. DEFENDANT

20. Defendant Apple is a California corporation with its principal place of business in Cupertino, California.

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

JURISDICTION AND VENUE

22. The Circuit Court of Mason County has subject matter jurisdiction over the claims alleged, as the claims enumerated herein arise exclusively under West Virginia statutory and common law and from *parens patria*e authority of the Attorney General to act on behalf of the West Virginia and its citizens. West Virginia's claims are in excess of any minimum dollar amount necessary to establish the jurisdiction of the Court.

23. This Court has personal jurisdiction over Apple because it, through its authorized agents, servants and employees, regularly transacted business in West Virginia and further through

its acts and omissions tortiously caused injuries in West Virginia by engaging in a persistent course of conduct in West Virginia that violated federal and West Virginia law. Moreover, Apple derived substantial revenue as the result of the technology products that were distributed and/or made available to, and purchased and/or used by, West Virginia residents.

24. This Court also has personal jurisdiction over Apple because it is registered with the Secretary of State to conduct business in West Virginia and has purposefully availed itself of this forum. Apple transacted or solicited business, derived revenue from products and services, and caused tortious injury in West Virginia—both by acts committed within the State and acts committed outside the State that produced harm within it. It has sufficient minimum contacts to support the exercise of personal jurisdiction.

25. Venue is appropriate in Mason County because Apple transacts business in, maintains agents, or is otherwise found in the District., and because a substantial part of the events or omissions giving rise to this action took place, or had their ultimate injurious impact, within the District. In particular, at all times, Apple provided, offered for sale, sold, and otherwise engaged in commerce within the District, and caused injury to the State in Mason County.

26. This Court further has venue over this action pursuant to W. Va. Code § 56-1-1.

FACTUAL ALLEGATIONS

I. APPLE'S PRODUCTS

A. APPLE'S MOBILE DEVICES

27. Founded in 1976 as Apple Computer Company, Apple has steadily grown into a digital behemoth. At the time of this Complaint, Apple is second only to Nvidia as the most valuable publicly traded company in the world, with a market capitalization of approximately $3.9 trillion. Apple's market capitalization is larger than the GDP of all but seven countries.

28. In 2024, Apple generated $391 billion in revenue and $93.736 billion in net income.

29. Apple manufactures and sells a diverse range of products, including but not limited to smartphones (iPhone), tablets (iPad), computers (Mac), and other recording devices (iPod Touch), as well as digital storage products (iCloud).

30. The iPhone is Apple's signature product. As of 2025, Apple has sold over 2.6 billion iPhones worldwide since the first iPhone was released in 2007 worth an estimated $2.5246 trillion.

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

33. As of 2025, Apple controls approximately 61.26% of the smartphone market in the United States. On information and belief, Apple has a similar share of the smartphone market in West Virginia.

34. Apple devices and related products are secured by a user's account credentials, an Apple Account, formerly called AppleID.

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

36. At inception and until this day, Apple designed and chose to maintain its mobile devices without adequate safeguards to protect known child victims of online sexual exploitation and abuse.

B. iCLOUD

37. Mobile devices, including smartphones and tablets, increasingly rely on cloud storage to host the abundant data users accumulate through ordinary use. The apps, pictures,

videos, messages, and other data users amass often vastly exceed the storage capacity of their devices. Users can increase their storage capacity by uploading their device's data to a cloud platform.

38. In 2011, Apple launched iCloud, a cloud computing product that backs up, stores, manages, and synchronizes data across multiple devices using remote computer servers accessed through the internet.

39. iCloud, Apple's cloud platform, is integrated with and incorporated into any Apple device with internet access and a modern operating system — i.e., an operating system created in 2012 or later.

40. According to Apple, iCloud securely stores and organizes a user's photos, media, and files across all of the user's iCloud-enabled devices and facilitates sharing those photos and files with friends and family. When a user initiates a change on one device, that change updates on all of their devices via an action known as iCloud syncing. For example, if a user takes a photo on their iPhone, that photo will appear on other devices connected to the same iCloud account.

41. iCloud syncing occurs when the feature is enabled and a device is connected to the internet. This will automatically back up a user's iPhone, iPad, and iPod Touch daily.

42. According to Apple and third-party reports, iCloud is managed by physical data centers that house servers owned and controlled by Apple or operated through third-party servers which Apple commands and controls. These servers are physical devices on which CSAM resides.

43. At inception and until this day, Apple designed and chose to maintain iCloud without adequate safeguards to protect known child victims of online sexual exploitation and abuse, particularly insofar as Apple has declined or otherwise failed to prevent, prohibit, report,

remove, or eliminate known instances of CSAM from being stored, hosted, and maintained on its iCloud platform.

44. iCloud has since become a profit center for Apple. In 2024, iCloud reportedly generated approximately $10.4 billion in revenue for Apple, which is greater than that of many other major Apple products, including Apple Music, Apple TV+, and AppleCare.

45. By any metric, iCloud dominates all other cloud platforms accessible on Apple's mobile devices. Although Apple does not provide hard figures about the performance of its services like iCloud, it did reveal in 2023 that revenue was driven by "over 1 billion paid subscriptions."

46. Apple's iCloud was initially partially hosted on Amazon Web Services and Microsoft Azure. In 2016, Apple began hosting iCloud on the Google Cloud platform.

47. Apple's iCloud capabilities are built into each Apple device, and every Apple Account comes with 5 GB of cost-free storage. Additional storage space is available for purchase using a subscription model.

48. 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.

49. Nearly two-thirds of Apple customers in the United States opt for paid iCloud storage.

50. In 2019, Apple introduced iCloud to Windows devices to facilitate iCloud access from non-Apple devices.

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

52. Apple represents that its products and services have enhanced privacy protections — principally, end-to-end encryption ("E2E"). To simplify, end-to-end encryption makes data unreadable to anyone besides the sender and receiver; not even Apple can see data protected by end-to-end encryption, even though data will be transferred through Apple's servers. In contrast, standard encryption permits Apple to house encryption keys in its data centers, enabling Apple to review that data in certain circumstances.

53. By default, iMessages, messages sent through Apple's proprietary messaging service for its devices, are end-to-end encrypted. While most iCloud data, including photos, are only protected by standard encryption by default, users can elect for "Advanced Data Protection" that provides end-to-end encryption for many more iCloud data categories, including photos and videos. Apple began offering Advanced Data Protection for iOS 16.2, iPadOS 16.2 and macOS 13.1. Advanced Data Protection was available for iCloud as of December 2022.

54. Fundamentally, E2E encryption is a barrier to law enforcement, including the identification and prosecution of CSAM offenders and abusers. The Federal Bureau of Investigation, for instance, announced that it was "deeply concerned with the threat end-to-end and user-only-access encryption pose," according to a statement provided by an agency spokeswoman. "This hinders our ability to protect the American people from criminal acts ranging from cyberattacks and violence against children to drug trafficking, organized crime and terrorism." The FBI explained that it and law enforcement agencies need "lawful access by design."[10]

[10] Robert McMillan, Joanna Stern, Dustin Volz, *Apple Plans New Encryption System to Ward Off Hackers and Protect iCloud Data*, WALL ST. J. (updated Dec. 7, 2022, 8:47 PM EDT), available at: https://www.wsj.com/articles/apple-plans-new-encryption-system-to-ward-off-hackers-and-protect-icloud-data-11670435635.

II. APPLE KNOWINGLY PROTECTS ABUSERS AND ITS PRODUCTS HARM CSAM VICTIMS AND THE PUBLIC AT LARGE

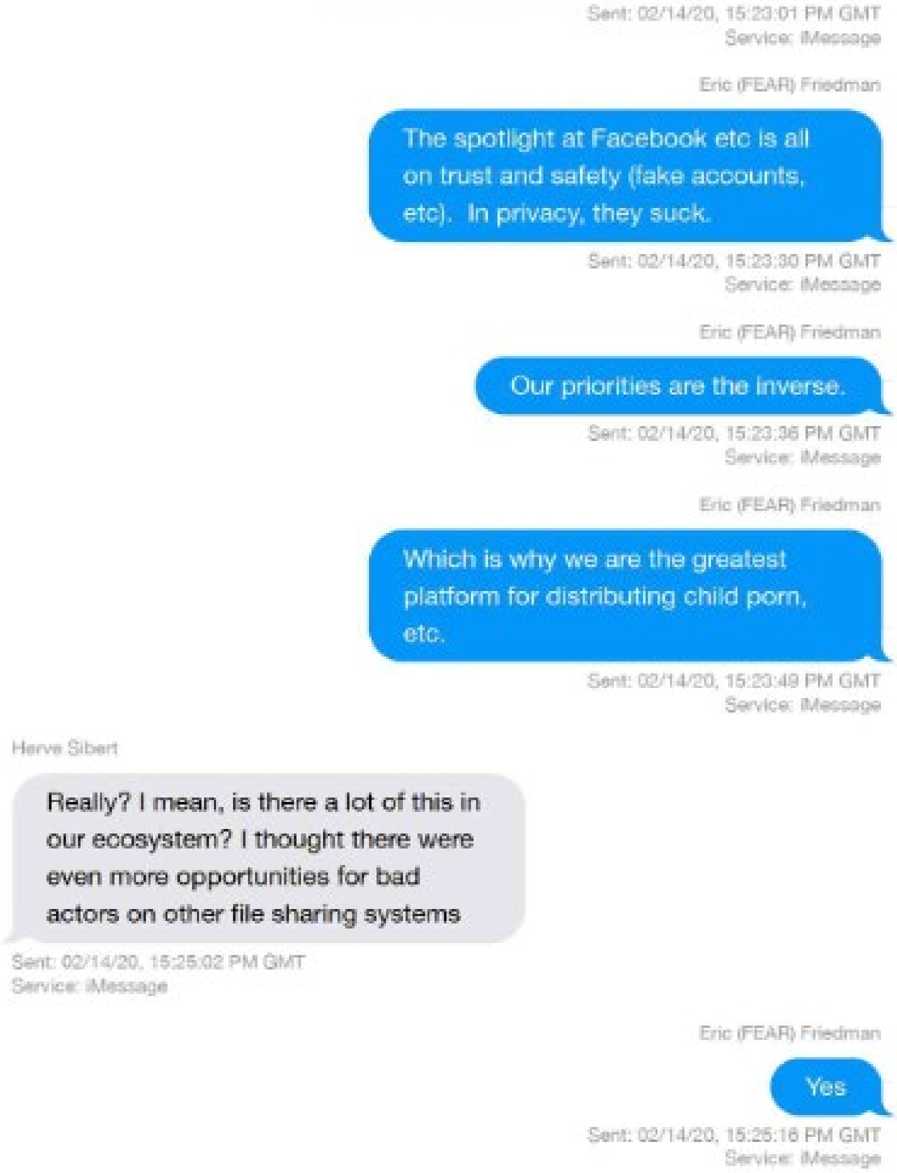
55. Apple and its leadership, including but not limited to executives Eric Friedman and Herve Sibert, have actual knowledge that Apple defectively designed its products in a manner that they admitted renders Apple "the greatest platform for distributing child porn."[11]

56. In an iMessage conversation about whether Apple might be putting too much emphasis on privacy and not enough on trust and child 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[.]"[12]

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

[12] 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), available at: https://www.theverge.com/c/22611236/epic-v-apple-emails-project-liberty-app-storeschiller-sweeney-cook-jobs.



Sent: 02/14/20, 15:23:01 PM GMT
Service: iMessage

Eric (FEAR) Friedman

The spotlight at Facebook etc is all on trust and safety (fake accounts, etc). In privacy, they suck.

Sent: 02/14/20, 15:23:30 PM GMT
Service: iMessage

Eric (FEAR) Friedman

Our priorities are the inverse.

Sent: 02/14/20, 15:23:36 PM GMT
Service: iMessage

Eric (FEAR) Friedman

Which is why we are the greatest platform for distributing child porn, etc.

Sent: 02/14/20, 15:23:49 PM GMT
Service: iMessage

Herve Sibert

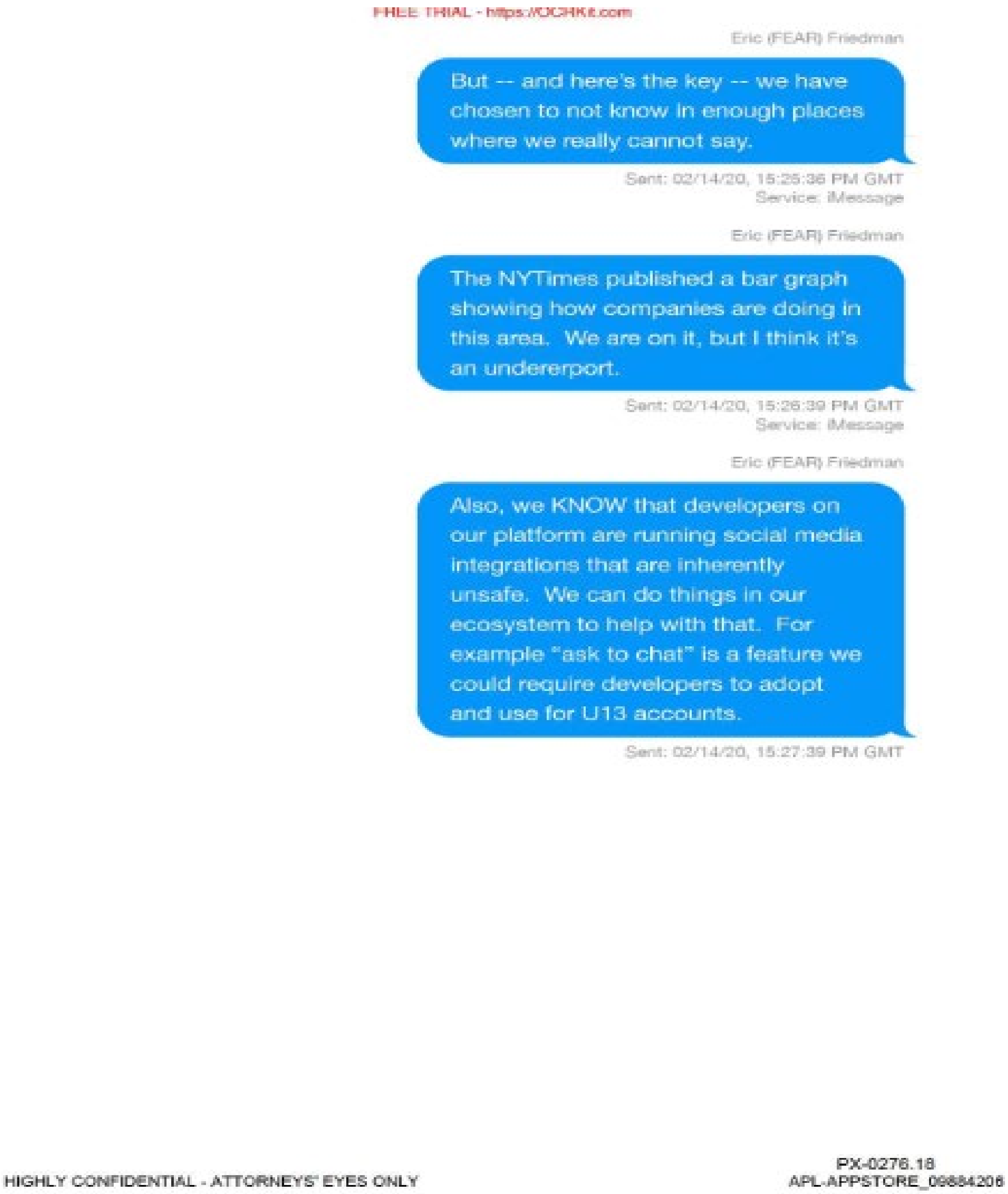
Really? I mean, is there a lot of this in our ecosystem? I thought there were even more opportunities for bad actors on other file sharing systems

Sent: 02/14/20, 15:25:02 PM GMT
Service: iMessage

Eric (FEAR) Friedman

Yes

Sent: 02/14/20, 15:25:16 PM GMT
Service: iMessage



Eric (FEAR) Friedman

But -- and here's the key -- we have chosen to not know in enough places where we really cannot say.

Sent: 02/14/20, 15:25:36 PM GMT
Service: iMessage

Eric (FEAR) Friedman

The NYTimes published a bar graph showing how companies are doing in this area. We are on it, but I think it's an undererport.

Sent: 02/14/20, 15:26:39 PM GMT
Service: iMessage

Eric (FEAR) Friedman

Also, we KNOW that developers on our platform are running social media integrations that are inherently unsafe. We can do things in our ecosystem to help with that. For example "ask to chat" is a feature we could require developers to adopt and use for U13 accounts.

Sent: 02/14/20, 15:27:39 PM GMT

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

PX-0276.18
APL-APPSTORE_09884206

58. In or after 2020, Apple and its executives consciously ignored the exploitation of children and "chose[ ] not to know" about CSAM stored or hosted on iCloud and Apple products.

59. Apple knowingly and intentionally designed its products with deliberate indifference to the highly preventable harms Apple caused.

A. Apple Knowingly Designed a Product Ecosystem that Foreseeably Aids the Spread of CSAM

60. Apple intentionally designs its products for the rapid, private distribution of information, including images and videos. Collectively, Apple's software tools are optimized for and encourage high-risk, illegal activities, including the possession and mass distribution of CSAM.

61. Because Apple does not scan its devices or cloud storage for CSAM, the risk of detection for users engaged in CSAM possession and distribution through its ecosystem is significantly lower compared to users who would attempt the same via Google or Meta's digital ecosystems because those peers scan their networks for CSAM.

62. As the following demonstrates, Apple has not built a neutral ecosystem; rather, it contains material design advantages for CSAM traffickers by offering a secure, frictionless avenue for the possession, protection, and distribution CSAM.

1. Encoding, Metadata, and Interface Tools

63. Apple's software is not user-authored, but rather, it is controlled by Apple, which determines how files are created, encoded, indexed, stored, retrieved, and transmitted. While a user can determine *when* a file is created, users do not necessarily determine *how* that file is saved.

64. When a user captures media using an iPhone, Apple's software determines the encoding format and metadata, such that the image is compatible for viewing across Apple's devices.

65. When Apple's software encodes an image and assigns metadata, it is assigning system-level identifiers that allow files to be searched, selected, shared, and exported to proprietary and third-party applications. These identifiers are also what allow a user's rapid retrieval of images from local storage and iCloud and seamless transmission through its proprietary messaging system

and third-party applications like WhatsApp and Kik. In this way, Apple's software mediates the user's interaction with file uploads in all instances.

66. Without Apple's encoding and metadata architecture, content on a user's device is functionally inert and distribution would be substantially more difficult.

67. To facilitate the rapid retrieval and distribution of documents, Apple has additionally designed numerous file management mechanisms, including:

i. System file pickers that appear when applications ask the user to choose a file or attach a photo for transmission from local files or iCloud photos. Through its software, Apple decides what content is exposed through file pickers and how easily an image can be retrieved from a device or iCloud folder;

ii. Share sheets that pop up on an image when a user taps the "share" icon, which prepare content for transmission; and,

iii. Application Programming Interfaces ("APIs") that allow a user to accept and save media attachments within applications.

2. Encryption

68. As discussed above, encryption is a key aspect of Apple's software. Encryption technology, especially E2E encryption, makes detection of CSAM technically infeasible and eliminates server-side visibility into iMessage contents or iCloud files.

69. In the last few years, E2E communication platforms have become increasingly popular for predators engaging in CSAM exchange and communication. These platforms attract predators precisely because they provide secrecy and privacy guarantees and can be operated on mobile devices without the need for any special user expertise.

70. The rise in the use of encryption communication platforms, especially E2E encryption, has coincided with the "unprecedented" acceleration of CSAM distribution.

71. In a 2023 Report to Congress, the Department of Justice discussed the problem that encryption poses for detecting child predators. In particular,

> Due to these technological advancements, the scale, complexity, and dangerousness of threats facing children today are unprecedented . . . we are sure in the knowledge that offenders are exploiting children online and in real life -- and are not getting caught because their crimes are shielded by encryption and anonymization. Although we have a qualitative picture of the nature of child sexual exploitation in encrypted and anonymous spaces, and we have evidence suggesting that the threats to children are growing, we have no fulsome quantitative information about its scope and prevalence. What we do not know haunts us.[13]

72. In 2019, then-U.S. Attorney for the Southern District of West Virginia warned about the connection between Apple's encryption technology and the ability for child predators to escape detection.

> Apple implemented warrant-proof encryption on its platforms a few years ago; unsurprisingly, that company's reporting to the NCMEC of evidence of child exploitation occurring on its platforms is laughably (and tragically) low. It's not that Apple magically runs clean platforms; it's that the company has created a lawless space where law enforcement is powerless to investigate and intervene regardless of how heinous or how despicable the crime.[14]

73. Encryption, and particularly E2E, is a design choice. By maintaining this design choice, Apple knows its tools shield CSAM possession and distribution activities from law enforcement and Apple. Apple's ecosystem is not simply *used* by bad actors; it is designed to attract them.

3. iCloud

74. Apple designed the iCloud for the management, expansion, and acceleration of a user's workflow, not simply as a passive storage mechanism. This is demonstrated by the fact that iCloud:

[13] UNITED STATES DEPARTMENT OF JUSTICE, *National Strategy for Child Exploitation & Interdiction*, (2023), available at: https://www.justice.gov/d9/2023-06/2023_national_strategy_for_child_exploitation_prevention_interdiction_-_combined.pdf.

[14] Mike Stuart, *Herald-Dispatch Op-Ed: Warrant-proof encryption threatens children* (November 24, 2019), available at: https://www.justice.gov/archives/doj/blog/herald-dispatch-op-ed-warrant-proof-encryption-threatens-children.

i. automatically syncs images across a user’s devices;

ii. remains persistently available for rapid retrieval of files;

iii. permits immediate access to the stored content via a user’s device or by shared links;

iv. contains mechanisms that allow Apple and the iCloud user to manage storage space.

75. When activated, iCloud will automatically sync to all devices connected to that iCloud account, allowing access to the same images or videos across connected devices.

76. Because iCloud synchronization results in multiple access points for the same data, it promotes persistent availability and access redundancy. This inherent property of cloud sync makes it easier for anyone storing illicit material — including CSAM — to maintain access and persistence of that material across devices as compared to local storage alone. The destruction or confiscation of a single device containing CSAM, for instance, does not guarantee that the underlying CSAM on that device has been destroyed.

77. iCloud also allows users to upload and save files that remain accessible to the user and others via a link or shared access permissions. In other words, iCloud essentially serves as remote file server for the efficient upload, storage, distribution, and retrieval of files.

78. The ability to share images via link offers a unique advantage to CSAM traffickers. CSAM distribution via “dead-drop” cloud storage links, for example, is a well-known distribution mechanism[15] because it permits traffickers to share CSAM in private groups or closed networks,

[15] RAPE ABUSE AND INCEST NATIONAL NETWORK (“RAINN”), *How Does CSAM Get Distributed?*, available at: https://rainn.org/get-the-facts-about-csam-child-sexual-abuse-material/how-does-csam-get-distributed; *see also* WEPROTECT GLOBAL ALLIANCE, *Link-sharing and child sexual abuse: understanding the threat* (February 2023), available at: https://www.weprotect.org/wp-content/uploads/Link-sharing-roundtable-paper_GCHQ-1.pdf.

allowing the persistent availability of stored CSAM that can bypass moderation or avoid public detection.

79. CSAM traffickers can use dead-drop links to distribute CSAM to selectively authorized recipients—meaning that neither law enforcement nor Apple would be able to access the information shared via an iCloud link.

80. Due to the benefits of link sharing, including ease of accessibility and the barriers it creates to law enforcement, it is now a preferred "on-demand" method of accessing CSAM.[16]

81. Apple has also designed iCloud with robust, storage-optimizing features including:

i. An "Optimize Storage" mechanism in iCloud that automatically bifurcates files into high-resolution full-images on iCloud and smaller, optimized copies on the devices to preserve on-device space;

ii. Deduplication mechanisms that use metadata to prevent the user from storing more than one full copy of the same document on the iCloud.

82. CSAM offenders often hoard and distribute CSAM en masse. This requires vast amounts of storage, including terabytes of needed space. Even smaller cases often concern criminals that retain tens of thousands of images and/or hours of video.[17]

83. Apple offers various iCloud payment tiers that provide users up to twelve terabytes of storage on iCloud.

84. The fact that Apple optimizes storage capability, offers terabytes of space for photo and video uploads, understands that iCloud is widely used to distribute CSAM, and still refuses to

[16] WEPROTECT GLOBAL ALLIANCE, *Link-sharing and child sexual abuse: understanding the threat* (February 2023), available at: https://www.weprotect.org/wp-content/uploads/Link-sharing-roundtable-paper_GCHQ-1.pdf.

[17] Jessica L. Terkovich, *A Statutory Solution to Storage Shortfalls in Child Sexual Abuse Material Investigations*, 2025 U. ILL. L. REV. ONLINE 174 (November 13, 2025), available at: https://illinoislawreview.org/online/a-statutory-solution-to-storage-shortfalls-in-child-sexual-abuse-material-investigations.

take reasonable measures to control for CSAM, especially for users that purchase terabytes of storage space, amounts to knowing and/or reckless conduct and material assistance to CSAM traffickers.

85. Taken collectively, Apple's ecosystem is not a collection of neutral tools. Rather, with Apple's explicit acknowledgement that it is the "greatest" platform for distributing CSAM, Apple has knowingly designed a set of tools that dramatically reduces friction for possessing, collecting, safeguarding, and spreading CSAM, all the while engineering an encryption shield that makes it much more likely for bad actors to use Apple to protect their illicit activities.

B. APPLE LACKS AN INTEGRATED, SYSTEM-WIDE MECHANISM TO REPORT CSAM IN THE UNITED STATES

86. Apple's proprietary applications, including iMessage and iCloud, lack integrated mechanisms for users to report CSAM to Apple or the appropriate legal authorities. In other words, if one Apple user sends another an iCloud link or iMessage containing CSAM, there is no adequate or readily available means to report CSAM to Apple or local authorities.

87. The decision not to incorporate user-facing reporting mechanisms is in contrast to the other online platforms, such as Snapchat, which allows users to flag nudity or sexual content directly within another user's photo feed with only a couple of taps of a screen.

88. In another example, the search engine Bing, which is owned by Microsoft, allows users to identify and flag as CSAM any image viewed through Bing through an integrated reporting mechanism that can appear upon a user's prompt with only a few mouse clicks.

89. Buried in Apple's iCloud Terms of Service is Apple's authorization of users to report CSAM or any other issues to Apple through the email address abuse@iCloud.com. While this is an implicit recognition by Apple that such a reporting mechanism is needed, the email

address is not a button or user-facing integrated feature nor is it specifically designed for CSAM reporting.

90. Although Apple users can manually search or ask Siri, Apple's proprietary voice-assistant tool, how to report CSAM, Siri will not report CSAM directly to Apple based on the user's prompting.

91. Although Apple has taken some steps to enhance user safety, these steps fall far short of an integrated, robust or even adequate reporting mechanism designed to encourage users to flag and report CSAM.

92. Apple's Communication Safety feature, for example, detects nudity and blurs sexually explicit images and prompts children and parents with warnings. Although Apple warns of potential explicit content, users can proceed to view that content, and there is no mechanism to directly report illegal, explicit content, such as CSAM, to Apple even with the Communication Safety feature enabled.

93. Apple's approach to child safety in Australia demonstrates that an integrated CSAM reporting mechanism is feasible and as easy as a software update.

94. There, in response to new laws such as Australia's Online Safety Act, Apple has rolled out an update that allows children to report nudity in photos or video on a device directly to Apple with only a few taps, similar to reporting on other digital platforms.

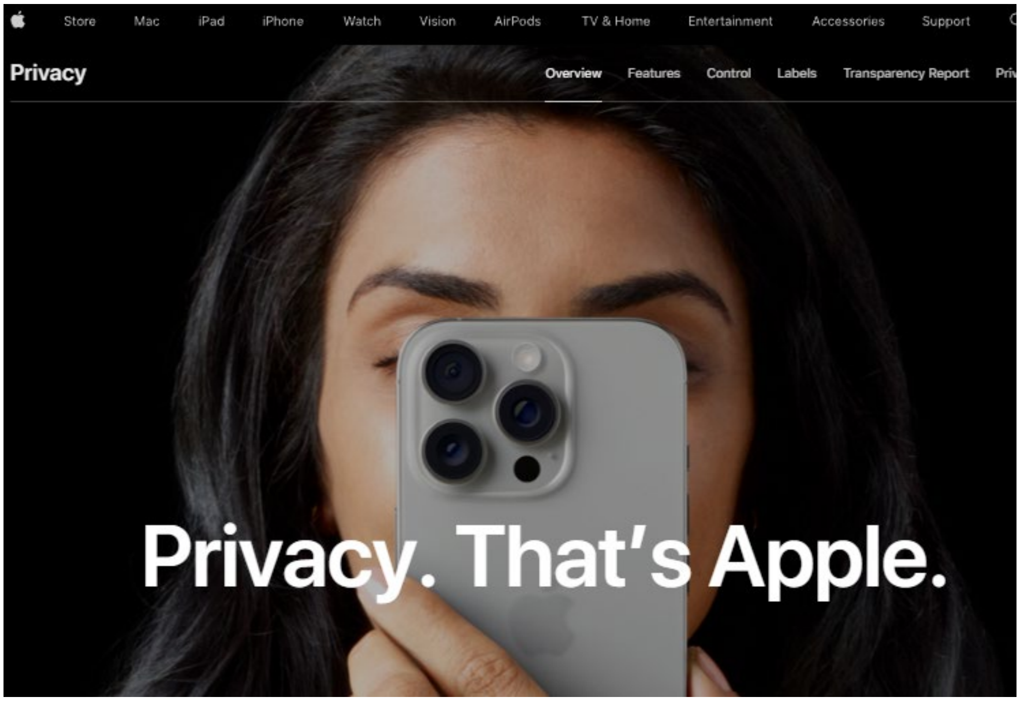
95. Although this mechanism is focused on child-users, on information and belief, it could be deployed for all users and permit them to directly report CSAM to Apple.

III. APPLE BELIEVES ITS BRAND IS PRIVACY, AND THIS REPRESENTS A DESIGN CHOICE FOR ITS ECOSYSTEM

96. Apple advertises itself as a stalwart privacy advocate and uses this position to distinguish itself from its competitors.

97. On its website, Apple states that privacy is a "fundamental human right. It's also one of our core values. [sic] Which is why we design our products and services to protect it. That's the kind of innovation we believe in."[18]

98. Apple's website also contains an advertisement equating Apple with the concept of privacy itself, stating, "Privacy. That's Apple."[19]



99. Apple has also, at various times, launched advertising campaigns around privacy, including erecting 40-foot billboards featuring the iPhone and a simple slogan, "Privacy. That's iPhone."

100. Other slogans similarly have touted Apple's purported commitment to privacy. In Las Vegas, for instance, Apple erected a billboard with the slogan, "What happens on your iPhone,

[18] https://www.apple.com/privacy/.

[19] *Id*.

stays on your iPhone."[20] In New York, Apple similarly stated on a billboard, "Your iPhone knows a lot about you. But we don't."[21]

What happens on your iPhone, stays on your iPhone.
apple.com/privacy
SpringHill Suites Marriott
Image by: Chris Velazco/Twitter

101. To maintain its brand, Apple has, at times, chosen to take public stands against countervailing social interests. For example, Apple refused to assist the FBI in unlocking an iPhone belonging to one of the terrorist perpetrators behind the 2015 San Bernardino massacre, which still remains one of the most lethal mass shootings in American history.[22] Ultimately, Apple forced the FBI to seek a judicial order for its compliance.

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

[21] 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*, available at: 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).

[22] Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NPR (December 3, 2016 1:00 PM ET), available at: https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

102. But even after a federal court in California ordered Apple to cooperate, the company appealed directly to the public, publishing an open letter to its customers on the very day the order was issued. Signed by CEO Tim Cook, the letter invoked a fear-based, slippery-slope argument (Apple's "San Bernardino Letter").[23]

> The implications of the government's demands are chilling. If the government can . . . make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge . . . . We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

103. While Apple stalled compliance with its court-ordered cooperation, the FBI obtained assistance from a third party to unlock the iPhone in question and ultimately dropped the lawsuit.

104. Privacy is not merely Apple's advertised value; it represents a series of architectural design and policy choices that shape how its platform functions and who is drawn to use it. Those choices include the decision not to implement its CSAM Detection tools as planned.

105. While Apple may believe its decisions further its narrative around privacy as a core company value, the reality is that Apple's decisions create market signals directed to users who value secrecy because they are engaged in high-risk activities.

106. Apple knows that the intrinsic design of its products draws bad actors. Eric Friedman recognized that Apple's support of privacy as a value informs its design decisions in the

[23] Tim Cook, *A Message to Our Customers*, APPLE (February 16, 2016), available at: https://www.apple.com/customer-letter/.

series of text messages alleged above. According to Mr. Friedman, these design decisions are precisely the reason why it is the "greatest" platform for distributing CSAM.

IV. APPLE PREVIOUSLY PREPARED TO LAUNCH PROPRIETARY CSAM DETECTION AND REPORTING TOOLS

A. INDUSTRY STANDARDS

107. CSAM detection tools and features are now standard components of digital product design and failing to implement them falls below industry standards and accepted best practices.

108. In or about 2008, Professor Hany Farid, a digital forensics pioneer at the University California at Berkley, developed a CSAM detection tool called PhotoDNA in collaboration with Microsoft.

109. At all relevant times, PhotoDNA is considered the industry standard in detecting digitized CSAM.

110. PhotoDNA includes an image comparison technology that detects matches between modified versions of the same image or images. The PhotoDNA algorithm converts the image to grayscale, resizes the image, divides it into squares, and then assigns hash values based on the shading in each square. To combat the spread of CSAM, Microsoft has publicly released information about how its image matching algorithm works.

111. PhotoDNA and/or similar CSAM detection tools can determine the similarity between two images, even if they are not identical. 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 altered CSAM images to known and identified CSAM.

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

113. This remains the case despite that its peers and competitors, such as Microsoft, Google, Meta, and DropBox, utilize proactive CSAM detection technologies like PhotoDNA to detect, report, and remove knownhashed child pornography.[24]

B. APPLE'S PROPOSED CSAM DETECTION AND REPORTING TOOLS

114. In August of 2021, Apple announced a new feature for its iPhone iOS15 operating system designed to combat the spread of CSAM (Apple's "CSAM Detection").[25] CSAM Detection consisted of several tools, including a proprietary hashing technology dubbed "NeuralHash," a Matching-Database Setup and On-Device Private Set Interaction Protocol ("MDSP"), and Threshold Secret Sharing ("TSS").[26] The tools like NeuralHash and MDSP, which would have been performed directly on users' devices, were originally planned as software updates.

115. According to Apple, these tools enable it "to accurately identify and report iCloud users who store known Child Sexual Abuse Material (CSAM) in their iCloud Photos accounts . . . This process is secure, and is expressly designed to preserve user privacy."[27]

116. Broadly speaking, and as explained further below, the CSAM Detection tools operate in the following manner: (1) NeuralHash assigns hash values to images; (2) these hash values are compared to known CSAM hash values on a user's device; (3) suspected CSAM hash matches are encoded in a "safety voucher" before upload to iCloud; (4) once the upload of

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

[25] *See* Frank Bajack & Barbara Ortutay, *Apple **to scan** U.S. iPhones for Images of Child Sexual Abuse,* AP NEWS (Aug. 6, 2021), available at: https://apnews.com/article/technologybusiness-child-abuse-apple-inc-7fe2a09427d663cda8addfeeffc40196 [https://perma.cc/44M4-HJ55]; *see also* APPLE, *CSAM Detection Technical Summary*, August 2021.

[26] APPLE, *CSAM Detection Technical Summary*, August 2021.

[27] *Id.* at Introduction.

suspected CSAM reaches a certain numerical threshold, Apple is able to review the images and report relevant information to the National Center for Missing and Exploited Children. (NCMEC, as defined above).[28]

1. NeuralHash

117. NeuralHash works by creating unique identifiers (hash values) for users' photos that are stored on iPhone devices and uploaded to an iCloud Photo library.[29] Hashing is the process of assigning a hash value, which is a unique, fixed-length string of characters, akin to a digital fingerprint.

118. Hash values are unique and irreversible. With respect to cyber security, these digital fingerprints are used to verify the authenticity and integrity of data.[30]

119. Because hash values are distinctive and without duplicates, each piece of CSAM ever produced will have a unique hash value when hashed. Given this, it is possible to compare the hash value of one file to known CSAM hash values to determine whether that file contains CSAM.

120. While altering an image changes that image's hash value, technology is readily available to match altered CSAM images to their originals. Microsoft's PhotoDNA, for instance, matches similar images even if the files are not identical.

[28] Matthew Panzarino, *Interview: Apple's Head of Privacy Details Child Abuse Detection and Messages Safety Features,* TECHCRUNCH (Aug. 10, 2021, 9:00 AM), available at: https://techcrunch.com/2021/08/10/interview-apples-hea d-of-privacy-details-childabuse-detection-and-messages-safety-features/ [https://perma.cc/BGZ3-XTT3]; APPLE, *CSAM Detection Technical Summary*, August 2021.

[29] *See* APPLE*, Security Threat Model Review of Apple's Child Safety Features,* 5-11(Aug. 2021), available at: https://www.apple.com/child-safety/pdf/SecurityThreatModelReview-ofAppleChildSafetyFeatures.pdf [https://perma.cc/N6CF-BRXV].

[30] *See id*.

121. Similar to PhotoDNA, NeuralHash is capable of detecting similar and altered CSAM images, including those that differ in size or transcription quality. This is because NeuralHash is a perceptual hashing function that bases hash value on features of the image instead of the precise values of the pixels.[31]

2. Matching-Database Setup and Private Set Interaction Protocol ("MDSP")

122. The hash values of known CSAM are kept in a centralized repository controlled by the NCMEC for CSAM detection purposes.[32]

123. Through the MDSP part of the anticipated CSAM Detection software update, Apple would have installed hash values from NCMEC onto users' iPhones and compared the hashes from a user's image before uploading that image to iCloud.

124. To be clear, all that would have been loaded onto users' devices would be the alpha-numerical hash values of known CSAM assigned by NCMEC, not the CSAM itself. As discussed above, hash values are akin to a digital fingerprint—not the actual CSAM images.[33]

125. While other technology companies have used hashing technology for years to locate and report CSAM on their platforms by scanning emails and cloud data, Apple would have been the first to install anti-CSAM hashing and detection technology directly on users' devices.[34]

[31] APPLE, *CSAM Detection Technical Summary*, August 2021 at pp. 4-5.

[32] Rudin, *Walling off Privacy: Apple's NeuralHash Controversy, the ECPA, the Fourth Amendment, and Encryption*, 21 COL. TECH. L. J. 2 (May 8 ,2023).

[33] APPLE, *CSAM Detection Technical Summary*, August 2021, at p. 6; *see also* Rudin, *Walling off Privacy: Apple's NeuralHash Controversy, the ECPA, the Fourth Amendment, and Encryption*, 21 Col. Tech. L. J. 2 (May 8, 2023).

[34] Timothy Gernand, *Scanning iPhones to Save Children: Apple's On-Device Hashing Algorithm Should Survive a Fourth Amendment Challenge*, 127 DICKENSON L. REV. 1 (Fall 2022).

126. The Private-Set-Interaction ("PSI") Protocol, which powers Apple's CSAM Detection, has both an on-device and server component.[35]

127. With respect to the on-device PSI Protocol, before an image is stored onto iCloud Photos, the device compares an image's NeuralHash against NCMEC hash database. [36]

128. Based on this hash matching process, user images are assigned a safety voucher before upload to iCloud. A safety voucher is a data record associated with each image in the iCloud Photos account. It is generated on-device by the CSAM Detection process. The vouchers cryptographically encode whether an image has a match within the database of known CSAM values.[37]

129. The output of the PSI protocol reveals to Apple's server whether there is a match.[38] When the safety vouchers are uploaded to Apple's servers, only vouchers associated known CSAM hashes can be decrypted.

3. Threshold Secret Sharing ("TSS")

130. Apple had originally planned only to flag and review iCloud accounts when the number of safety vouchers exceeded a pre-defined numerical threshold—i.e., TSS.

131. Once a user's account was flagged, only then would Apple use its encryption keys to interpret the contents of safety vouchers associated with the matching CSAM images.[39]

[35] APPLE, *CSAM Detection Technical Summary*, August 2021, at p. 6; Rudin, *Walling off Privacy: Apple's NeuralHash Controversy, the ECPA, the Fourth Amendment, and Encryption*, 21 Col. Tech. L. J. 2, 7 (May 8, 2023).

[36] *Id.*

[37] APPLE, *CSAM Detection Technical Summary*, August 2021, at p. 9.

[38] *Id.*

[39] *Id.*

132. According to Apple, through the use of its protocol, "[n]othing is ever revealed about non-matching images during any step of the CSAM Detection process . . . . with a combination of Private Set Intersection and Threshold Secret Sharing, Apple is able to learn the relevant image information only once the account has more than a threshold number of CSAM matches, and even then, only for the matching images."[40]

133. Once Apple would have flagged an account, Apple had planned to disable the iCloud user's account, review each report manually to confirm matches, and then send a report to NCMEC.

134. When the NCMEC receives a report of suspected CSAM, the organization's analysts review the information to determine if it meets the criteria for a referral to criminal authorities. If it does, the NCMEC will send a detailed referral to the appropriate state or local law enforcement agency.

135. On information and belief, this same process would have been applied to Apple's referrals had CSAM Detection been implemented.

4. Apple's CSAM Detection Tools Fall Short of the Standard of Care

136. Apple imposed several constraints on its CSAM Detection tools before scrapping the project entirely.

137. These constraints were arbitrary from a technical standpoint; they are not required for any technology-based reason but rather were designed to support Apple's narrative that it protects user privacy.

138. First, Apple deliberately designed and failed to engineer NeuralHash to adequately generate distinct hash values for non-similar images with the same accuracy as PhotoDNA.

[40] *Id.*, at p. 8.

139. Second, Apple ensured CSAM Detection would not trigger a report to Apple unless 30 images or more were detected as CSAM. 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.

140. Lastly, the 30-image threshold was too conservative, even under its own design. According to Apple, there was less than **a one in one trillion** chance per year of incorrectly flagging a given account. To put this in perspective, the chances of winning a billion-dollar Powerball jackpot are about 1 in 292 million. That means winning the Powerball for any individual is about 3,425 times more likely than having their iCloud account incorrectly flagged by Apple for CSAM.

V. APPLE ANNOUNCES AND THEN QUIETLY CANCELS CSAM DETECTION

A. APPLE LAUNCHES PRESS TOUR AROUND CSAM DETECTION

141. Apple touted its decision to implement CSAM Detection, speaking to several media sources and launching a new section of its website. Apple's move engendered goodwill, solicited positive responses, and was applauded by experts and child safety professionals.

142. Apple worked with NCMEC while developing NeuralHash. Marita Rodriguez, executive director of strategic partnerships, sent the following email to the Apple privacy team upon the announcement of NeuralHash:[41]

[41] Chance Miller, *In internal memo, Apple addresses concerns around new Photo scanning features, doubles down on the need to protect children*, 9TO5MAC (Aug. 6, 2021, 7:02 AM PDT), available at: https://9to5mac.com/2021/08/06/apple-internal-memo-icloud-photo-scanning-concerns/.

> Team Apple,
>
> I wanted to share a note of encouragement to say that everyone at NCMEC is SO PROUD of each of you and the incredible decisions you have made in the name of prioritizing child protection. It's been invigorating for our entire team to see (and play a small role in) what you unveiled today.
>
> I know it's been a long day and that many of you probably haven't slept in 24 hours. We know that the days to come will be filled with the screeching voices of the minority.
>
> Our voices will be louder.
>
> Our commitment to lift up kids who have lived through the most unimaginable abuse and victimizations will be stronger.
>
> During these long days and sleepless nights, I hope you take solace in knowing that because of you many thousands of sexually exploited victimized children will be rescued, and will get a chance at healing and the childhood they deserve.
>
> Thank you for finding a path forward for child protection while preserving privacy.

143. John Clark, President & CEO, National Center for Missing & Exploited Children, proclaimed, "Apple's expanded protection for children is a game changer. With so many people using Apple products, these new safety measures have lifesaving potential for children who are being enticed online and whose horrific images are being circulated in child sexual abuse material. At the National Center for Missing & Exploited Children we know this crime can only be combated if we are steadfast in our dedication to protecting children. We can only do this because technology partners, like Apple, step up and make their dedication known. The reality is that privacy and child protection can co-exist. We applaud Apple and look forward to working together to make this world a safer place for children."

144. Former Attorney General Eric Holder pronounced, "The historic rise in the proliferation of child sexual abuse material online is a challenge that must be met by innovation from technologists. Apple's new efforts to detect CSAM represent a major milestone, demonstrating that child safety doesn't have to come at the cost of privacy, and is another example

of Apple's longstanding commitment to make the world a better place while consistently protecting consumer privacy."

145. David Forsyth, Chair in Computer Science at the University of Illinois at Urbana-Champaign College of Engineering, emphasized, "Apple's approach preserves privacy better than any other I am aware of […] In my judgment, this system will likely significantly increase the likelihood that people who own or traffic in [CSAM] are found; this should help protect children. Harmless users should experience minimal to no loss of privacy, because visual derivatives are revealed only if there are enough matches to CSAM pictures, and only for the images that match known CSAM pictures. The accuracy of the matching system, combined with the threshold, makes it very unlikely that pictures that are not known CSAM pictures will be revealed."

146. Apple's Head of Privacy gave an interview with TechCrunch to discuss the new technology.[42] When asked why now and not sooner, Apple emphasized that it had a focus on user privacy, and the technology did not exist until now:

> **TC:** Most other cloud providers have been scanning for CSAM for some time now. Apple has not. Obviously there are no current regulations that say that you must seek it out on your servers, but there is some roiling regulation in the EU and other countries. Is that the impetus for this? Basically, why now?
>
> **Erik Neuenschwander:** Why now comes down to the fact that we've now got the technology that can balance strong child safety and user privacy. This is an area we've been looking at for some time, including current state of the art techniques which mostly involves scanning through entire contents of users' libraries on cloud services that — as you point out — isn't something that we've ever done; to look through users' iCloud Photos. This system doesn't change that either, it neither looks through data on the device, nor does it look through all photos in iCloud Photos. Instead

[42] Matthew Panzarino, Interview: *Apple's head of Privacy details child abuse detection and Messages safety features*, TECHCRUNCH (Aug 10, 2021, 8:00 AM PDT), available at: https://techcrunch.com/2021/08/10/interview-apples-head-of-privacy-details-child-abusedetection-and-messages-safety-features/.

> what it does is gives us a new ability to identify accounts which are starting collections of known CSAM.
>
> **TC:** So the development of this new CSAM detection technology is the watershed that makes now the time to launch this. And Apple feels that it can do it in a way that it feels comfortable with and that is 'good' for your users?
>
> **Erik Neuenschwander:** That's exactly right. We have two co-equal goals here. One is to improve child safety on the platform and the second is to preserve user privacy. And what we've been able to do across all three of the features is bring together technologies that let us deliver on both of those goals.

147. To coincide with the announcement and press tour promoting NeuralHash, Apple created a new section of its website, "Expanded Protections for Children."[43] Therein, Apple declared, "We want to help protect children from predators who use communication tools to recruit and exploit them, and limit the spread of Child Sexual Abuse Material (CSAM)."

148. Apple touted that it would "use new applications of cryptography to help limit the spread of CSAM online, while designing for user privacy. CSAM detection will help Apple provide valuable information to law enforcement on collections of CSAM in iCloud Photos." Apple assured its users and the world of its ambitions and acknowledged "protecting children is an important responsibility. These efforts will evolve and expand over time."[44]

[43] https://www.apple.com/child-safety/, original version available at: https://web.archive.org/web/20210805191220/https://www.apple.com/child-safety/.

[44] *Id.*

B. Apple Abandons CSAM Detection Under Privacy Advocates' Pressure

1. Public Response

149. Initially, Apple defended its CSAM-detecting methods "as designed with user privacy in mind."[45]

150. But even with this caveat, Apple was not prepared for the backlash that followed, not from the general public but from a vocal minority of purported privacy advocates.

151. Echoing the fear-based speculations of Apple's San Bernardino Letter, the Cato Institute remarked on Apple's CSAM Detection tools,

> [H]ere's what Apple is implementing: A surveillance program running on the user's personal device, outside the user's control, will scan the user's data for files on a list of prohibited content, and then report to the authorities when it finds a certain amount of content on the list. Once the architecture is in place, it is utterly inevitable that governments around the world will demand its use to search for other kinds of content—and to exert pressure on other device manufacturers to install similar surveillance systems.

152. WhatsApp, a primary competitor to Apple for end-to-end encryption services, asserted that Apple's changes amounted to an "Apple-built and operated surveillance system that could very easily be used to scan private content for anything they or a government decides it wants to control."

153. The Electronic Frontier Foundation ("EFF") decried Apple's plans as a "backdoor to increased surveillance and censorship around the world" and "ammunition" to authoritarian governments. To induce readers to sign a petition against Apple's plans, the EFF further added that "governments have been asking for years for a way around Apple's encryption, and now Apple has caved to the pressure."

[45] APPLE, *CSAM Detection Technical Summary*, August 2021.

154. Privacy advocates made these criticisms in spite of the fact that Apple initially defended its CSAM Detection tools as a balance between its privacy commitment and the need to fight CSAM, assuring the public its detection tools were narrowly tailored to this purpose. Apple's representations included that:

i. CSAM detection would not provide Apple any information about photos other than those that match the hash values of known CSAM;[46]

ii. Apple's CSAM detection system "only works with CSAM hash images" and cannot detect other types of data on users' devices;

iii. Apple would "refuse" government demands to add non-CSAM images to the hash list;

iv. CSAM detection would not incorrectly flag innocent images of child nudity, such as those of one's own children in a bathtub;

v. CSAM detection does not work for users who have iCloud Photos disabled and does not work on private iPhoto library on the device.[47]

155. Given Apple's representations and promises to its customers, the privacy-related criticisms leveled by a vocal minority were alarmist and unfounded. However, Apple recognized the threat to its brand posed by this opposition.

2. Apple's Broken CSAM Promise

156. Even amidst backlash, from September 2021 to December 2022, Apple allowed the public to believe that a rollout of its CSAM Detection tools would occur.

157. But Apple had a brand to protect. On or about December 7, 2022, Apple announced that it was back-tracking and that it would not implement NeuralHash or any other CSAM Detection tools on its products.

[46] APPLE, *Expanded Protections for Children: Frequently Asked Questions*, August 2021, v1.1 (August 2021).

[47] *Id.*

158. By December 16, 2022, Apple had quietly removed several references to NeuralHash from its website.[43]

159. Shortly after Apple abandoned its CSAM Detection tools or other child safety technologies to detect known CSAM, Apple's director of investigations and child safety, Melissa Marrus Polinsky, and its trust and safety director, Margaret Richardson, left the company.[48]

160. 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.[49]

161. Defending Apple's decision, Erik Neuenschwander, Apple's director of user privacy and child safety, penned a publicly available letter to the Heat Initiative, a child safety advocacy organization, explaining Apple's reasoning. According to Neuenschwander, "[s]canning every user's privately stored iCloud data would create new threat vectors for data thieves to find and exploit . . . It would also inject the potential for a slippery slope of unintended consequences. Scanning 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."

162. These representations were false and/or misleading as they related to Apple's previously announced CSAM Detection tools. Not only are they rebutted by Apple's own representations at the time (and cited herein), including Apple's representation that CSAM Detection only worked with existing hashed CSAM images, but they are challenged by Apple's subsequent actions.

[48] *Id.*

[49] *Id.*

163. Portions of Erik Neuenschwander's letter, including the quoted material above, are publicly available to and accessible by residents of West Virginia.

164. In a separate letter to the Securities Exchange Commission authored by Apple's Counsel at the law firm Gibson Dunn, Erik Neuenschwander's letter is attached in full as an exhibit. Thus, the letter in full is also publicly available to and accessible by residents of West Virginia.

165. In September 2024, Apple released iOS 18 for iPhones that included a feature called Enhanced Visual Search ("EVS"). This feature allows users to search their photo library for landmarks or points of interest, even if the photos lack geolocation data. It utilizes privacy-preserving techniques, including on-device processing, homomorphic encryption, and Oblivious HTTP relays, to protect user data.

166. EVS uses the same or similar technology as NeuralHash and the proposed CSAM Detection tools; instead of identifying CSAM, it helps users identify and learn more about objects, landmarks, plants, animals, and other visual elements within their photos.

167. Similar to Apple's CSAM Detection process, EVS matches a user's photos to a global index Apple maintains on its servers.

C. APPLE CONTINUES TO MISREPRESENT ITS ROLE IN FIGHTING CSAM

168. Despite discarding its plans to employ CSAM Detection, Apple misrepresents to consumers and third parties that it actually takes proactive measures against CSAM.

169. Available on Apple's website is its Privacy Policy, which "describes how Apple collects, uses, and shares your personal data."

170. In relevant part, Apple's Privacy Policy states, "Apple uses personal data to power our services, to process your transactions, to communicate with you, for security and fraud

prevention, and to comply with law. We may also use personal data for other purposes with your consent" (emphasis omitted). In relevant part, the Privacy Policy further states,

> **Security and Fraud Prevention.** To protect individuals, employees, and Apple and for loss prevention and to prevent fraud, including to protect individuals, employees, and Apple for the benefit of all our users, and prescreening or scanning uploaded content for potentially illegal content, including child sexual exploitation material.

Id. (emphasis in original).

171. Apple materially mispresents that it "conducts prescreening or scanning uploaded content for … child sexual exploitation material." This misrepresentation provides illusory comfort to users, including CSAM victims and their families, that Apple implements appropriate measures to prevent the storage and hosting of CSAM, among other things.

172. At all times, this Privacy Policy would have been accessible to residents in West Virginia.

173. In addition to the misstatement in its privacy policy, Apple does not disclose to West Virginia residents the material fact (in its terms of service or elsewhere) that its products facilitate the possession, collection, safeguarding, and spread of CSAM. Nor does Apple disclose that it declines use tools for its products that could reduce the possession, collection, safeguarding, and spread of CSAM.

174. Due to this omissions, West Virginians purchasing Apple's products, including paid-for storage of iCloud, would not have been aware that Apple's products facilitate the possession, collection, safeguarding, and spread of CSAM.

VI. APPLE'S CONDUCT FACILITATES PREVENTABLE CRIMES

175. The possession and distribution of CSAM is illegal under state and federal law. *See, e.g.,* W. Va. Code § 61-8C, *et seq.*

176. In designing its products, including iCloud, Apple made specific design choices that recklessly and foreseeably enabled illegal conduct related to CSAM, even though the standard of care, as established by Apple's peers, is to design a cloud storage platform with robust CSAM detection and reporting features. Apple's design choices additionally include the decision to operate iCloud as a large-scale cloud storage and synchronization service with enhanced privacy protections, while declining to implement any system-wide mechanism to detect known CSAM or to permit users to directly and efficiently report suspected CSAM stored in iCloud to Apple.

177. These enhanced privacy protections include encryption, and particularly, end-to-end encryption. Apple has chosen to offer end-to-end encryption for stored iCloud data without implementing compensating safeguards, such as system-wide CSAM detection or user-accessible reporting mechanisms for iCloud content. As a result, Apple's encrypted environment provides increased secrecy and reduced oversight for users who store and safeguard CSAM, making detection more difficult and allowing such material to persist and be accessed across devices, all the while Apple recognizes that its ecosystem is the "greatest" platform for distributing CSAM.

178. The risks associated with iCloud's present design do not outweigh the utility of designing products without CSAM detection features, and in particular, the now shelved CSAM Detection tools previously designed by Apple.

179. The persistent consumption, possession, and safeguarding of CSAM creates long-lasting and permanent harm to victims it depicts, their families, and, in light of the strong public interest in preventing CSAM, the public at large.

180. Not only do CSAM victims suffer emotional harm knowing that CSAM depicting them may never cease to exist, but predators that possess and consume CSAM are more likely to contact children for the purposes of exploitation and sexual abuse.

181. Given both the ongoing emotional harm to victims and the propensity for perpetrators to harm children through direct contact, “the creation, use, and distribution of CSAM is an urgent public health and human rights crisis.”

182. After Apple failed to implement its CSAM Detection tools or any other features to detect known CSAM on Apple’s products, including iCloud, West Virginia continued to experience harms to its quasi-sovereign interests brought about from Apple’s conduct. These include impact to the public health and general welfare of the State, the facilitation and continuation of unlawful conduct, including the possession and safeguarding of CSAM, and the physical and mental health, safety, and welfare of its residents, including especially but not limited to children and CSAM victims.

VII. APPLE’S CONDUCT IMPACTS WEST VIRGINIA

183. The NCMEC maintains a CyberTipline, which is the nation’s centralized reporting system for the online exploitation of children. In 2024, West Virginians made 5,000 total reports to the CyberTipline.

184. Most tips reported to NCMEC involve the possession, manufacture, and/or distribution of suspected CSAM.

185. West Virginia Child Advocacy Centers (“WVCACs”) have experienced increases in children requiring their services, with a nearly 8% increase from 2020 through 2025. WVCACs provide safe, child-friendly facilities where child protection, criminal justice, and child treatment professionals work together to investigate abuse, hold offenders accountable, and help children heal. Child victims include West Virginians who have been depicted in or exposed to pornography. Statistics involving WVCACs are tracked by the West Virginia Child Advocacy Network. (“WVCAN”).

186. In 2025, almost half of children serviced by WVCACs reportedly experienced sexual abuse.

187. Children serviced by WVCACs often undergo forensic interviews where they recount their abuse and trauma. Children may also require medical and/or counseling services.

188. Similar to other states, law enforcement personnel in West Virginia often begin investigating a case involving CSAM with a tip from NCMEC, which relays facts gathered by technology companies like Dropbox, Snapchat, Facebook, or Google.

189. These tips have, in fact, led to the discovery, prosecution, and conviction of individuals in West Virginia who possessed CSAM.

190. In one such example, 2:23-cr-00046 (S.D.W. Va.), Facebook submitted a tip to NCMEC, which relayed that information to the appropriate law enforcement personnel. This tip eventually led to a guilty plea from a Defendant in West Virginia who possessed CSAM on his cellular telephone. The tip resulted after the Defendant uploaded a video containing CSAM through Facebook Messenger.

191. Given the interconnectedness and ease of communication in the modern world, out-of-state residents are also capable of causing harm to West Virginia minors. In one example, 3:22-cr-87 (S.D.W.Va.), an out-of-state resident coerced minor female residing within the Southern District of West Virginia to record and send him sexually explicit images of herself via the Snapchat multimedia instant messaging app.

192. As discussed above, Apple lacks CSAM detection mechanisms and otherwise provides services like encryption that help perpetrators involved in the possession or distribution of CSAM evade detection. Consequently, reports of CSAM by Apple to NCMEC are, according to Michael Stuart, former U.S. Attorney for the Southern District of West Virginia, "laughably

(and tragically) low." On information and belief, this statement applies with equal force to both the nation and West Virginia specifically.

193. Apple's products, including the iPhone, have been involved in CSAM-related crimes in West Virginia. However, reporting often involves individuals who happen to discover evidence of wrongdoing, not because of Apple's detection or reporting mechanisms.

194. In one example, 2:25-cr-00069 (S.D.W. Va.), staff for a charity found a convicted sex offender in possession of an unauthorized iPhone. In response to this discovery, the suspect replied, "There's enough on that cell phone to put me away for life of [sic] this time." To his probation officer, the suspect stated his iPhone contained CSAM and that he had intentionally used the cell phone to engage in behavior that would return him to prison for life and that he was "going out in a blaze of glory."

VIII. LEGAL CLAIMS

COUNT I

STRICT LIABILITY – DESIGN DEFECT

195. West Virginia repeats and reallege all prior paragraphs as if fully incorporated herein.

196. At all relevant times, Defendant designed, developed, managed, operated, tested, produced, labeled, marketed, advertised, promoted, controlled, sold, supplied, and/or distributed its products. Apple has also benefited from the use of its products by child pornographers to collect, possess, store, host, and/or safeguard CSAM.

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

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

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

200. Apple defectively designed its products, particularly iCloud, to permit the ongoing collection, possession, storage, hosting, and/or safeguarding of CSAM.

201. Further, Apple has not enabled its users to easily report CSAM when information is transmitted over applications like iMessage.

202. The defects in the design of Apple's products existed before the release of these products to 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.

203. Apple defectively and knowingly designed its products to permit, promote, facilitate, and acquiesce to the ongoing collection, possession, storage, hosting, and safeguarding of CSAM.

204. Apple defectively and knowingly designed its products to lack integrated, easily accessible mechanisms for reporting CSAM.

205. Apple failed to test the safety of its products. While Apple performed some product testing and knew of ongoing harm to West Virginia and its citizens, it failed to adequately remedy its product's defects or warn consumers about their known hazards.

206. Apple's products are defective in design and pose a substantial likelihood of harm for the reasons outlined in this complaint 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.

207. Apple's products are likewise defectively designed because they create an inherent risk of danger; specifically, by failing to prevent or prohibit the collection, possession, storage,

hosting, and safeguarding of CSAM the products facilitate criminal activity and undermine the public's trust in the marketplace.

208. Such risks and harms can also include but are not limited to exposure to predators, sexual exploitation, social isolation, and profound mental health issues, including but not limited to depression, anxiety, and other harmful effects, particularly in children and CSAM victims.

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

210. Apple could have utilized cost-effective, feasible alternative designs, which were the industry standard, including technology development and product changes, to minimize the harms to victims of CSAM, including, but not limited to:

a. Implementing its proprietary CSAM Detection tools;

b. Implementing industry-standard systems on iCloud to prevent its use for the purpose of collection, possession, storage, hosting, and safeguarding of known hashed CSAM;

c. Implementing freely available and industry-proven child protection API tools such as PhotoDNA and Project Arachnid Shield to prevent the collection, possession, storage, hosting, and safeguarding of known hashed CSAM through their products;

d. Utilizing the legal definition of child pornography and related case law when reviewing detected CSAM to prevent underreporting of known hashed CSAM;

e. Utilizing the NCMEC Child Sexual Abuse Material Hash List on its products including iCloud and Apple devices;

f. Implementing available proactive detection measures to detect and report known CSAM on iCloud, iMessage, and/or Apple devices.

g. Implementing integrated, easily accessible reporting mechanisms for users to report CSAM sent through iMessages or iCloud.

211. Alternative designs were readily and inexpensively available to reduce the presence of known hashed CSAM on Apple products and would not limit Defendant's products while reducing the gravity and severity of the danger posed by those products' known defects.

212. Predators and child pornographers used Defendant's products in reasonably foreseeable ways for, inter alia, the collection, possession, storage, hosting, and safeguarding of known hashed CSAM.

213. The physical, emotional, and economic harms suffered by the West Virginia public were reasonably foreseeable to Apple during product development, design, advertising, marketing, promotion, and distribution.

214. 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 who used the products without any substantial change in the product's condition.

215. As a direct and proximate result of Apple's products' design, CSAM collection, possession, storage, hosting, and safeguarding via Apple systems has persisted in West Virginia. West Virginia has also suffered and continues to suffer pecuniary losses and harms. Although, as of the time of this complaint, West Virginia has not yet quantified expenditures on health benefits, treatment services, and physical or mental healthcare relating or arising out of Apple's conduct, it reasonably believes it has incurred and will continue to incur such additional pecuniary losses and harms.

COUNT II

NEGLIGENCE

216. West Virginia repeats and realleges all prior paragraphs as if fully incorporated herein.

217. Apple had a duty to exercise reasonable care in the design, manufacture, testing, marketing, and distribution into the stream of commerce of Apple's technology products, including iCloud. Apple's duty to exercise reasonable care included ensuring that Apple's products, including iCloud and iMessage, did not pose a significantly increased risk of injury to the public, including victims of CSAM.

218. Apple failed to exercise reasonable care in the design, manufacture, testing, marketing, and distribution into the stream of commerce of its technology products, including iCloud and iMessage. 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 and industry-standard child protection features could present a danger if pedophiles, predators, or child pornographers used their products, and therefore were not safe for use.

219. Even though Apple knew or should have known that its design of its technology products would facilitate the use of such products for the purpose of collection, possession, storage, hosting, and safeguarding of known hashed CSAM, and therefore inflict additional injuries to victims of known hashed CSAM, Apple continued to market its products as safe.

220. Not only did Apple fail to utilize longstanding freely available industry-standard technology like the NCMEC Child Sexual Abuse Material Hash List, it negligently designed its own CSAM Detection solution, then failed to implement it.

221. Furthermore, Apple owed a duty to exercise reasonable care in the design, configuration, and rollout of iCloud and related account- and link-sharing features so as not to create or dramatically increase foreseeable risks of injury to members of the public, including victims whose images are contained in NCMEC's CSAM hash list, whose images Apple knew were being hosted and safeguarded using Apple products.

222. Apple breached that duty by, among other things, deploying and promoting iCloud features or configurations, without compensating safety measures, that

a. Promoted frictionless synchronization and propagation of documents across user devices and cloud storage;

b. Enabled mass redistribution of images or videos across devices and among users;

c. Lacked abuse-prevention guardrails for iCloud links (e.g., link-rate throttling);

d. Lacked account-level friction and verification for bulk sharing/storage behavior consistent with CSAM tracking patterns;

e. Used encryption and/or other privacy-guaranteeing mechanisms to shield users' possession and distribution activities from apple, law enforcement, and other third parties.

223. Separate and apart from the allegations above, Apple additionally breached that duty further by failing to implement its promised CSAM Detection tools and, among other things, failing to design its CSAM Detection tools with:

a. The ability to adequately generate distinct hash values for non-similar images with the same accuracy as PhotoDNA; and,

b. An adequate image threshold, which would trigger a CSAM report to Apple.

224. These design choices created and magnified a risk that did not previously exist (or materially increased the risk); they were affirmative product design decisions that made iCloud a more efficient vector for the repeated redistribution of CSAM images by criminal actors.

225. Separately and additionally, Apple voluntarily undertook to design, test, and roll out CSAM countermeasures for iCloud (including the NeuralHash initiative it publicly announced in August 2021 after collaborating with child-safety stakeholders), representing that the company had found a path that would materially curb CSAM dissemination from iCloud while protecting privacy.

226. Having undertaken that safety program and induced reliance from victims, advocates, counterparties, and the public at large, Apple owed a duty to exercise reasonable care in performing (or in terminating) that undertaking. Apple breached that duty by:

a. architecting the safety program with artificial thresholds and synthetic vouchers that delayed escalation and concealed match volumes from Apple's own reviewers;

b. withdrawing the safety program after public commitment, while concurrently expanding encryption configurations and propagation features that foreseeably increased dissemination risks; and,

c. failing to implement alternative, non-content-review safeguards when it abandoned the announced measures.

227. Apple's negligent performance and termination of its CSAM Detection undertaking increased the risk of harm by removing promised and relied-upon safeguards while making iCloud's dissemination pathways more efficient.

228. Separate and apart, Apple breached its duty to exercise reasonable care in the design, configuration, and rollout of iMessage by failing to include an integrated, easily accessible CSAM reporting mechanism.

229. But for Apple's negligent design and negligent undertaking (including its withdrawal of promised safeguards without deploying compensating, non-content-moderation safety measures), the volume of CSAM collection, possession, storage, hosting, and/or safeguarding via Apple systems would have been materially reduced. As a direct and proximate result of Apple's negligence, the State has suffered and continues to suffer pecuniary losses and harms. Although, as of the time of this complaint, West Virginia has not yet quantified expenditures on health benefits, treatment services, and/or physical or mental healthcare relating or arising out of Apple's conduct, it reasonably believes it has incurred and will continue to incur such additional pecuniary losses and harms.

COUNT III

PUBLIC NUISANCE

230. The State repeats and realleges all prior paragraphs as if fully incorporated herein.

231. A public nuisance is an act or condition that operates to unreasonably interfere with any right common to the general public.

232. Apple intentionally, negligently, and/or recklessly caused, created, and/or contributed to a public nuisance which proximately caused injury to the State and interfered with public rights.

233. Through its conduct—detailed throughout this Complaint—Apple knowingly and significantly contributed to the collection, possession, storage, hosting, and safeguarding of CSAM, including in the State.

234. The collection, possession, storage, hosting, and safeguarding of CSAM harms public health, social welfare, and common public resources, as alleged throughout this Complaint.

235. As a consequence of Apple's creation or maintenance of a public nuisance, the State has or will bear additional burdens pertaining to the long-term protection of public health and safety, including mental, behavioral, and physical health needs of children and CSAM victims.

236. This public nuisance can be abated by Apple's implementation of a comprehensive CSAM detection tools across its ecosystem, including but not limited to, the deployment of such tools to scan for CSAM in user uploads to iCloud and the inclusion of integrated, easily accessible mechanisms for reporting CSAM in its products.

COUNT IV

VIOLATIONS OF THE WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT

237. The State repeats and realleges all prior paragraphs as if fully incorporated herein.

238. The West Virginia Consumer Credit and Protection Act ("WVCCPA") prohibits an entity from using "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

239. Apple's conduct, as alleged herein, involves "trade or commerce" within the meaning of the WVCCPA.

240. Apple's actions and statements, as detailed above, constitute unfair or deceptive acts or practices prohibited by WVCCPA. These include, but are not limited to, statements falsely, unfairly, and/or deceptively representing the nature of Apple's purported efforts to protect children, including its misrepresentation in its Privacy Policy that Apple conducts "prescreening or scanning [of] uploaded content for … child sexual exploitation material" and its promotional statements concerning NeuralHash and other subsequently abandoned CSAM Detection initiatives; and statements falsely, unfairly, and/or deceptively representing the reasons for Apple's abandonment of its CSAM Detection initiatives (including NeuralHash), predicated on purported technical infeasibility and/or privacy threats purportedly created by such initiative. These also include, but are not limited to, its failure to disclose to West Virginia residents the material fact that its products facilitate the possession, collection, safeguarding, and/or spread of CSAM and lack industry-standard tools to detect and report CSAM.

241. The facts detailed in this Complaint constitute multiple unfair or deceptive acts and practices broadly prohibited by W. Va. § 46A-6-104.

242. Apple is prohibited from claiming its products have benefits and protections that it that those products did not have, which is prohibited by W. Va. Code § 46A-6-102(7)(G).

243. Apple is prohibited from omitting material facts in its terms of service, including the fact that is products shield CSAM traffickers from law enforcement scrutiny, where those facts pose a known danger to the public. W. Va. Code § 46A-6-102(7)(M).

244. Apple is also broadly prohibited from practices in the sale of its good that creates a likelihood of confusion in violation of W. Va. Code § 46A-6-102(7)(L).

245. The conduct of Apple described throughout this Complaint establishes multiple statutory violations of the WVCCPA and constitutes unfair and deceptive acts and practices pursuant to W. Va. Code § 46A-6-104.

246. Each occurrence of a failure to abide by laws and rules enacted to protect the consuming public or to promote a public interest constitutes an unfair or deceptive act or practice in violation of the WVCCPA.

247. Apple's unfair, deceptive, and unconscionable acts or practices, or the effects thereof, are continuing, will continue, and are likely to recur unless permanently restrained and enjoined.

248. Consequently, the State seeks all available relief under the WVCCPA, including, but not limited to, disgorgement, restitution, civil penalties, equitable relief, injunctive relief, and attorneys' fees and costs.

IX. PRAYER FOR RELIEF

The State respectfully seeks the following relief:

A. An order providing for all appropriate injunctive relief requiring Apple to take reasonable measures to abate the public nuisance its conduct has caused, created, and/or contributed to;

B. An order declaring that Apple's conduct as set forth herein violates West Virginia law;

C. An order requiring other appropriate injunctive relief to bring Apple's conduct in conformity with law.

D. Restitution, disgorgement, civil penalties, and all other pecuniary and monetary relief available under law;

E. Attorneys’ fees and costs of litigation as permitted by law;

F. Pre-judgment and post-judgment interest as permitted by law;

G. Punitive damages as permitted by law; and

H. All other and further relief as this Court deems just and proper.

Dated: February 19, 2026

Respectfully Submitted,

JOHN B. MCCUSKEY,
ATTORNEY GENERAL OF WEST VIRGINIA

/s/ John B. McCuskey
John B. McCuskey (WVSB #11137)
Attorney General of West Virginia
Office of the West Virginia Attorney General
P. O. Box 1789
Charleston, West Virginia 25326
Telephone: (304) 558-8986
Jace.H.Goins@wvago.gov
Abby.G.Cunningham@wvago.gov
Counsel for the State of West Virginia

/s/ Matthew Stonestreet
Troy N. Giatras (WVSB #5602)
Matthew Stonestreet (WVSB #11398)
The Giatras Law Firm, PLLC
118 Capitol Street, Suite 400
Charleston, West Virginia 25301
Telephone: (304) 343-2900
troy@thewvlawfirm.com
matt@thewvlawfirm.com
Special Assistant Attorneys General
For the State of West Virginia