

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

AMY, et al.,
Plaintiffs,
v.
APPLE INC.,
Defendant.

Case No. [24-cv-08832-NW](#)

**ORDER GRANTING MOTION TO
DISMISS THE THIRD AMENDED
COMPLAINT WITH PREJUDICE;
GRANTING MOTION TO SEAL**

Re: ECF Nos. 81, 98, 99

The Court advises readers that this Order contains graphic descriptions of child sexual abuse.

* * *

This is a putative class action brought against Apple, Inc. by individuals depicted in Child Sexual Abuse Material (“CSAM”) shared using Apple’s technology and hosted on Apple’s servers. Named Plaintiffs Amy and Jessica (using pseudonyms) allege product liability, various negligence violations, and intentional infliction of emotional distress under state laws.¹ Currently pending before the Court is Apple’s motion to dismiss the third amended complaint (“TAC”).² ECF No. 98.

¹ The Court concurrently grants the pending application to seal the portions of Apple’s motion to dismiss the third amended complaint that identify Plaintiffs’ states of residence. *See* ECF No. 99.

² After the Court dismissed Plaintiffs’ federal claims with prejudice, *see* ECF No. 74, Plaintiffs filed a second amended complaint (“SAC”) asserting federal jurisdiction based on diversity. The parties subsequently briefed Apple’s motion to dismiss the SAC. *See* ECF Nos. 81, 83, 84. On April 27, 2026, the Court vacated the hearing on the motion to dismiss the SAC, finding the motion suitable for decision without oral argument pursuant to Civil Local Rule 7-1(b). ECF No. 92. Because the SAC did not include allegations related to the amount in controversy, the Court issued an Order to Show Cause why the case should not be dismissed for lack of jurisdiction. ECF No. 95. At the same time, the Court granted Plaintiffs leave to amend to cure the defect. *Id.*

This Court is obligated to follow both the letter of the law and the binding precedent that interprets it. As it stands, nothing in the law prevents any company, including Apple, from utilizing available technology or creating new technology to identify and report child pornography stored and distributed on their traditional servers or through their cloud services. Conversely, there is no law that obligates companies to proactively do so. Undoubtedly any such legislation would come at a cost of at least some loss of privacy for millions of people. But if lawmakers expected that companies would take steps to prevent their products from being used for storing and distributing child pornography based on something short of a legal imperative, this case, like many others before it, demonstrates the inadequacy of that approach. If lawmakers want to ensure that Apple and other companies address their role in the dissemination of CSAM, they must require it under the law. In other words, lawmakers can fix this problem that is contributing to the exploitation of children. This Court cannot.

The Court GRANTS Apple's motion to dismiss with prejudice because the current state of the law necessitates that outcome.

I. BACKGROUND

A. Apple Devices and iCloud Products

The Court provided a thorough review of Plaintiffs' allegations in its previous Order granting Apple's motion to dismiss Plaintiffs' initial complaint, almost all of which remain unchanged. *See* Order, ECF No. 74. The Court assumes the reader's familiarity with that Order and does not repeat the substance here, except where noted. Also, unless otherwise noted, the factual background below is drawn from Plaintiffs' allegations in the TAC. *See* ECF No. 97. The Court, as it must, deems all Plaintiffs' allegations true for the purpose of resolving Apple's motion to dismiss.

Plaintiffs' claims are aimed specifically at Apple's iCloud service, a data storage solution that is built into each Apple device that automatically updates, syncs, and backs up user data every

Plaintiffs timely filed a TAC that included allegations that confirmed the amount in controversy surpassed the necessary threshold but otherwise remained unchanged. ECF No. 97. Apple refiled its motion to dismiss the SAC, ECF No. 81, with updated paragraph citations to the TAC for the Court's ease of review. *See* ECF No. 98.

1 day. TAC ¶¶ 45-46. Plaintiffs allege that Apple has actual knowledge that its products and
 2 services are defectively designed when it comes to CSAM. *Id.* ¶ 82. In support of this contention,
 3 Plaintiffs quote a text message sent in 2020 by Apple’s then anti-fraud chief Eric Friedman. *Id.*
 4 ¶¶ 83-85. In the 2020 text thread, Friedman states that other tech companies focus on “trust and
 5 safety” but “suck” when it comes to privacy, and the priorities at Apple “are the inverse [w]hich is
 6 why [Apple] [is] the greatest platform for distributing child porn, etc.” *Id.* ¶ 84. When asked in
 7 the text thread if there is “a lot of [CSAM] in our ecosystem,” Friedman responds, “Yes,” and
 8 admits that Apple has “chosen to not know [about CSAM] in enough places where we really
 9 cannot say.” *Id.*

10 Plaintiffs allege that virtually all of Apple’s peer competitors, including Microsoft and
 11 Google, employ a program called PhotoDNA on their products to affirmatively identify and report
 12 CSAM to law enforcement. *Id.* ¶¶ 88-95. But, “Apple fails to use these standardly accepted
 13 industry-wide child protection tools.” *Id.* ¶ 95. Instead, in August 2021, after years of criticism,
 14 Apple announced that it would be launching a similar, proprietary program called NeuralHash. *Id.*
 15 ¶¶ 98-99.

16 Apple heavily promoted NeuralHash in the weeks after it was announced, insisting it
 17 would maintain user privacy better than PhotoDNA. *See id.* ¶¶ 125-140. Concurrent with the
 18 announcement of NeuralHash, Apple’s website added a new section, “Expanded Protections for
 19 Children.” *Id.* ¶ 138. “Therein, Apple declared, ‘We want to help protect children from predators
 20 who use communication tools to recruit and exploit them, and limit the spread of Child Sexual
 21 Abuse Material (CSAM).’” *Id.*

22 According to Plaintiffs, “Apple’s decision to finally implement CSAM detection
 23 engendered goodwill, solicited positive responses, and was applauded by experts and child safety
 24 professionals.” *Id.* ¶ 125. The President and Chief Executive Officer of the National Center for
 25 Missing & Exploited Children, John Clark, announced, “Apple’s expanded protection for children
 26 is a game changer. With so many people using Apple products, these new safety measures have
 27 lifesaving potential for children who are being enticed online and whose horrific images are being
 28 circulated in child sexual abuse material.” *Id.* ¶ 127. Clark continued: “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.” *Id.* Similarly, former United States Attorney General, Eric Holder, stated that the rise in online child sexual abuse material is a challenge that “must be met by innovation from technologists” and “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.” *Id.* ¶ 130.

But Apple’s announcement was quickly met with vigorous criticism from privacy advocates, and it soon became clear that NeuralHash was significantly less precise than PhotoDNA. *Id.* ¶¶ 149-151. On September 2, 2021, only a month after Apple announced NeuralHash, the company revealed that it was going to delay rollout without providing any additional timeline. *Id.* ¶ 152. The following year on “December 7, 2022, Apple announced it would not implement NeuralHash or any other CSAM detection tools on its products.” *Id.* ¶ 157.

In mid-2023, child safety advocates pressed Apple about why it abandoned NeuralHash. The TAC provides a portion of Apple’s response from Erik Neuenschwander, Director of User Privacy and Child Safety at Apple, to Sarah Gardner at the Heat Initiative, and Plaintiffs provide via footnote the source for the full quotation.³ *Id.* ¶ 158. The Court provides the fuller context of the quotation with the portions not directly quoted in the TAC italicized in brackets:

[As you note, we decided to not proceed with the proposal for a hybrid client-server approach to CSAM detection for iCloud Photos from a few years ago, for a number of good reasons. After having consulted extensively with child safety advocates, human rights organizations, privacy and security technologists, and academics, and having considered scanning technology from virtually every angle, we concluded it was not practically possible to implement without ultimately imperiling the security and privacy of our users.

Scanning of personal data in the cloud is regularly used by companies to monetize the information of their users. While some companies have justified those practices,] we’ve chosen a very different path — one that prioritizes the security and privacy of our users. Scanning

³ TAC ¶ 158 n.42. (“Emails between Erik Neuenschwander, Director of User Privacy and Child Safety at Apple, and Sarah Gardner at the Heat Initiative (Aug. 30–31, 2023) <https://s3.documentcloud.org/documents/23933180/apple-letter-to-heat-initiative.pdf>.”)

every user’s privately stored iCloud content would in our estimation pose serious unintended consequences for our users.

[Threats to user data are undeniably growing — globally the total number of data breaches more than tripled between 2013 and 2021, exposing 1.1 billion personal records in 2021 alone. As threats become increasingly sophisticated, we are committed to providing our users with the best data security in the world, and we constantly identify and mitigate emerging threats to users’ personal data, on device and in the cloud.] Scanning 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 (such as images, videos, text, or audio) and content categories.

Id. ¶ 158.

That same month, Apple launched the option for end-to-end encryption for iCloud data, making it “nearly impossible for either Apple or law enforcement to detect known CSAM stored on iCloud.” *Id.* ¶ 162.

B. Plaintiffs

Plaintiffs Amy and Jessica are victims of child sexual abuse. As young children in the early 2000s, Amy and Jessica were repeatedly raped and exploited by male relatives for the express purpose of producing CSAM to share on the internet. *Id.* ¶¶ 166-179. CSAM depicting Amy and Jessica continues to be possessed, traded, and distributed by child predators. Amy and Jessica are victims in nearly ninety CSAM criminal prosecutions. *Id.* ¶ 185. “[H]undreds of individuals charged and/or convicted for possessing known detectable CSAM depicting [Amy and Jessica] and the class members,” involved the use of Apple’s products. *Id.* The TAC identifies dozens of these other putative class members, who as children were similarly victimized by perpetrators who photographed and filmed their sexual abuse and then shared the resulting CSAM with other consumers and distributors of child pornography.⁴ *Id.* ¶¶ 185-195. As alleged in the

⁴ See, e.g., TAC ¶ 186 (“Victims discovered in the above cases include Alice (depicted in the At_Dawnchild pornography series), Andy (depicted in the SpongeB child pornography series), Angela (depicted in the Angela child pornography series), Anna (depicted in the MiddleModelSister child pornography series), April (depicted in the AprilBlonde child pornography series), Carrie (depicted in the FaceBaby child pornography series), Casseaopeia

TAC, even the briefest summaries of the abuse endured by these children, now members of the putative class, describe profound cruelty.⁵

Plaintiffs allege that Apple’s failure to implement any known CSAM detection is a design defect because Apple can safely implement readily available features to prevent the spread of known CSAM but has continuously failed to do so.

C. Procedural Posture

On October 15, 2025, the Court dismissed Plaintiffs’ first amended complaint (“FAC”) with partial leave to amend. ECF No. 74. In particular, the Court dismissed Plaintiffs’ first cause of action brought under 18 U.S.C. §§ 2252, 2252A, and 2255 with prejudice. The Court set forth the history of those statutes in its Order:

Congress enacted 18 U.S.C. § 2255, known as “Masha’s Law,” in 2005 to address the “lack [of] effective remedies under Federal law” for victims of child pornography. *Stephens v. Clash*, 796 F.3d 281, 285 (3d Cir. 2015) (internal quotation omitted). Masha’s Law provides a civil remedy for “[a]ny person who, while a minor, was a victim of a violation of” various sections of Title 18 prohibiting sexual exploitation of children, including §§ 2252 and 2252A. *M.H. On behalf of C.H. v. Omegle.com LLC*, 122 F.4th 1266, 1271 (11th

(depicted in the Lighthouse 3 child pornography series), Chelsea (depicted in the 2crazygurls child pornography series), Dipper (depicted in the Jester child pornography series), Emily (depicted in the Tightsngold child pornography series), Erika (depicted in the PinkHeartSisters1 child pornography series), Fiona (depicted in the BluesPink1 child pornography series), Ivy (depicted in the JBN Flowers2 child pornography series), Jack (depicted in the Rap72 child pornography series), Jane (depicted in the CinderBlockBlue child pornography series), Jenny (depicted in the Jenny child pornography series), Jordan (depicted in the BluesPlaid4 child pornography series), Julie (depicted in the JBN Flowers1 child pornography series), Kiera (depicted in the BluesPink3 child pornography series), Lana (depicted in the Youngest Model Sister child pornography series), Matthew (depicted in the BlueButterfly and Honeycomb child pornography series), Raven (depicted in the Teal&PinkPrincess2 child pornography series), Sarah (depicted in the MarineLand1 child pornography series), Sloane (depicted in the Tara child pornography series), Taylor (depicted in the RedGlassesCry child pornography series), Tori (depicted in the PinkHeartSisters2 child pornography series), and Wyatt (depicted in the HarleyDude1 child pornography series), are all members of the Class and were similarly victimized by the easily identified criminal offenders listed in the chart who were charged and/or convicted for possessing the same known detectible CSAM depicting them.”).

⁵ See, e.g., *id.* ¶ 189 (“‘Maureen’ (depicted in the Lighthouse1 child pornography series) was a toddler when her abuse began, and the abuse continued for several years until she was approximately eight years old. An unrelated adult male, known as ‘Uncle Charlie,’ would wake Maureen and sexually abuse her during the night. Her abuse was filmed, and the images created show Maureen being vaginally and anally penetrated, being forced to perform oral sex on an adult male, and being dressed up in costumes, then undressed and sexually assaulted for viewers. Maureen is a member of the proposed class.”).

Cir. 2024). It is a violation of Masha’s Law to: “knowingly receive[], or distribute[], any visual depiction using any means . . . including by computer . . . if— . . . [the] visual depiction involves the use of a minor engaging in sexually explicit conduct; and . . . such visual depiction is of such conduct”; it is also a violation to “knowingly possess[] . . . any . . . material that contains an image of child pornography that has been . . . transported using any means or facility of interstate or foreign commerce . . . including by computer.” 18 U.S.C. § 2252(a)(2), (4); 18 U.S.C. § 2252A(a)(2), (5).

Id. at 7 (ellipses in the original). As the Court noted, “to succeed on this claim, Plaintiffs [needed to] allege that Apple knowingly received or distributed CSAM.” *Id.* Plaintiffs failed to make the required showing; they alleged only that Apple was willfully ignorant of the existence of CSAM on its servers. *Id.* at 8. In *Does 1-6 v. Reddit, Inc.*, 51 F.4th 1137, 1145-46 (9th Cir. 2022), the Ninth Circuit found that willful ignorance of a publisher, without more, could not sustain a violation of a sex trafficking statute such as §§ 2252 or 2252A. *Id.*

Plaintiffs timely filed their SAC, which renewed certain claims and added others; Apple timely moved to dismiss. ECF Nos. 77-2, 81. Plaintiffs subsequently filed a TAC. *See* ECF No. 97; *infra* n.2. In their TAC, Plaintiffs now bring seven claims: products liability (Count I); claims alleging some form of negligence (Counts II-V, VII) and intentional infliction of emotional distress (Count VI).

II. LEGAL STANDARD

Under Fed. R. Civ. P. 12(b)(6), a complaint or cause of action can be dismissed where the pleading fails to state a claim upon which relief can be granted. To survive a motion to dismiss on those grounds, the “complaint must contain sufficient factual matter, accepted as true, ‘to state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is plausible on its face “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*

III. DISCUSSION

As it did in its previous motion to dismiss, Apple argues that § 230 of the Communications Decency Act (“CDA”) bars Plaintiffs’ suit in its entirety. *See* Mot. at 6-14, ECF No. 98. Section 230(c)(1) states that “[n]o provider or user of an interactive computer service shall be treated as

the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1). Controlling Ninth Circuit precedent holds that § 230 immunizes from liability “(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.” *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009). When considering whether § 230 applies, “[t]he proper analysis is to examine closely the duty underlying each cause of action and decide if it ‘derives from the defendant’s status or conduct as a publisher or speaker.’” *Estate of Bride by & through Bride v. Yolo Techs., Inc.*, 112 F.4th 1168, 1179 (9th Cir. 2024) (quoting *Barnes*, 570 F.3d at 1107). As the Ninth Circuit in *Estate of Bride* explained:

First, we examine the “right from which the duty springs.” Does it stem from the platform’s status as a publisher (in which case it is barred by § 230)? Or does it spring from some other obligation, such as a promise or contract (which, under *Barnes*, is distinct from publication and not barred by § 230)? Second, we ask what “this duty requir[es] the defendant to do.” If it *requires* that [defendant] moderate content to fulfill its duty, then § 230 immunity attaches.

Id. at 1177 (internal citations omitted). Put simply, “[a] claim that obliges the defendant to monitor third-party content to avoid liability also treats the defendant as a publisher.” *Doe I v. Twitter, Inc.*, 148 F.4th 635, 640 (9th Cir. 2025).

Here, Plaintiffs allege three categories of claims—products liability, negligence, and emotional distress. Though not explicitly alleged, at least one of two duties underlies each of the claims against Apple: (1) the 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” those depicted within CSAM shared on the platform; and (2) the duty “to exercise reasonable care in performing and terminating its voluntary safety undertaking,” namely the development and deployment of NeuralHash. TAC ¶¶ 303, 320. Apple supposedly breached both duties when it failed to deploy NeuralHash or otherwise take steps to stem the proliferation of CSAM in iCloud. *See, e.g.*, TAC ¶¶ 258 (Apple “fail[ed] to stop the spread and circulation of CSAM depicting [the] Plaintiffs”), 261 (alleging that design alternatives

1 include “CSAM detection measures”), 307(b) (faulting Apple for “withdrawing” a CSAM-
2 monitoring “program”).

3 Section 230 immunity is an affirmative defense—the Court noted as much in its previous
4 Order—so Apple bears the burden in establishing the validity of the immunity. *See Calise v. Meta*
5 *Platforms, Inc.*, 103 F.4th 732, 738 (9th Cir. 2024); Order at 6. The Court’s prior Order did not
6 make any findings on the issue of immunity under the CDA because it dismissed Plaintiffs’ claims
7 on other grounds. But now the Court must confront this issue squarely: if Apple can show that
8 Plaintiffs’ claims do not “allege enough facts to overcome Section 230 immunity, [those] claims
9 should be dismissed.” *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019)
10 (quoting *Barnes*, 570 F.3d at 1100–01).

11 Apple has made the requisite showing on both *Estate of Bride* steps. First, Plaintiffs’
12 claims treat Apple as a publisher or speaker of the CSAM content that animates Plaintiffs’
13 injuries. Fundamentally, Plaintiffs contend that Apple has elected to permit users to disseminate
14 and share third-party CSAM content when it could have—and, in their view, should have—used
15 readily available technology to prevent the distribution of child pornography depicting the
16 Plaintiffs in this putative class. The duties Plaintiffs seek to invoke “spring[] from the defendant’s
17 status as publisher,” and consequently, “immunity applies.” *Twitter*, 148 F.4th at 642. Second,
18 immunity also applies because “the means to avoid liability requires [Apple] to act as a publisher.”
19 *Id.* As a result, Apple is entitled to complete immunity under § 230.⁶

20 * * *

21 A survey of the Ninth Circuit’s recent, binding decisions addressing § 230 immunity
22 illustrates why Apple has immunity.

23
24 ⁶ In their opposition, Plaintiffs also insist that Apple is not a publisher, but a creator—and
25 therefore is not entitled to § 230 immunity—because Apple materially contributed to the behavior
26 that caused Plaintiffs’ harm. Opp’n at 8-11, ECF No. 83. Plaintiffs misconstrue the meaning of
27 material contribution. “A ‘material contribution’ does not refer to ‘merely . . . augmenting the
28 content generally, but to materially contributing to its alleged unlawfulness.’” *Gonzalez v.*
Google, 2 F.4th 871, 892 (9th Cir. 2021) (quoting *Fair Hous. Council of San Fernando Valley v.*
Roommates.com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008)). Because Plaintiffs do not allege
that Apple modified or augmented the CSAM on its servers in any way, this argument is without
merit.

1 The most recent opinion to discuss § 230 is *Doe I v. Meta Platforms, Inc.*, 174 F.4th 1159
 2 (9th Cir. 2026). That case was a putative class action brought by members of the Rohingya
 3 community, “a largely Muslim ethnic minority population indigenous to Western Myanmar—who
 4 were displaced from their homes following attacks by military and civilian forces.” *Id.* at 1163.
 5 The plaintiffs alleged that “Meta [wa]s to blame for fomenting the increased, pervasive violence
 6 against the Rohingya.” *Id.* Among other allegations, plaintiffs claimed that “Facebook’s core
 7 design and function exacerbated these harms, encouraging the creation of violent posts.” *Id.*

8 The Ninth Circuit rejected plaintiffs’ claims. As the court explained:

9 Plaintiffs’ theory is about the sharing of messages and what happens
 10 when some users interact with bad content, allegedly because of how
 11 the Facebook algorithm promoted some content whether specifically
 12 requested or not. *Cf. Est. of Bride*, 112 F.4th at 1180; *accord Grindr*
 13 *Inc.*, 128 F.4th at 1152–53. It thus necessarily relies on information
 14 provided by third parties. *See Lemmon*, 995 F.3d at 1087, 1093–94;
 15 *accord Barnes*, 570 F.3d at 1101. Calling Facebook a “product”
 16 rather than a publication platform only obscures the point that Meta
 17 “published user-generated speech that was harmful” to Plaintiffs.
 18 *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016)]. This case
 19 is more like *Estate of Bride*, where we concluded that a products
 20 liability claim was barred by Section 230: “What is th[e] harm” at the
 21 root of Plaintiffs’ claims but the violent and inciting “posts of others”
 22 posted on Facebook? 112 F.4th at 1180.

23 *Id.*

24 The reasoning above applies with equal force to the facts in the instant action. Though the
 25 content here relates to CSAM rather than calls for ethnic violence, the resultant injury comes from
 26 the same source: the third-party who generated the content. As alleged, Plaintiffs’ injuries are the
 27 direct result of the actions of third parties who used iCloud to share CSAM, a use Apple neither
 28 explicitly condones nor prevents (even assuming—as alleged in the TAC—that Apple was aware
 of the use of iCloud for this purpose). As the Court found previously, the TAC does not allege
 that Apple had actual knowledge that a specific user was disseminating CSAM using iCloud. *See*
 Order at 8. And though Plaintiffs allege that Apple knew that its tools were likely to be used to
 distribute child pornography (as confirmed by the internal Apple text messages at the center of this
 case), *see* TAC ¶¶ 82-87, under the current state of the law, Apple is still entitled to immunity
 under § 230—irrespective of that general knowledge.

Doe v. Grindr, Inc. is similarly dispositive—Apple references *Grindr* several times in its motion. *Doe v. Grindr Inc.*, 128 F.4th 1148, 1152–53 (9th Cir. 2025); Mot. at 2-3. There, plaintiff, a minor, was assaulted by men that he met through defendant’s app. When creating his account, plaintiff represented that he was over 18 years old, and the app did not require him to verify his age. Plaintiff’s “theory of liability [was] that [defendant] breached its duty not to design . . . defective products by failing to prevent a minor from being matched with predators, by matching users based on geographic data it extracted from them, and by allowing [the plaintiff] to communicate with abusive adults,” even when safer alternative designs were feasible. *Grindr*, 128 F.4th at 1153. The Ninth Circuit concluded that the claim was barred by § 230 because the “challenged features of the App”—which “were meant to facilitate the communication and content of others”—were “not independent of Grindr’s role as a facilitator and publisher of third-party content.” *Id.* (internal quotations omitted).

Plaintiffs do not address or attempt to distinguish *Grindr*, even though their claims are nearly identical to those asserted and rejected in that case. Like the plaintiff in *Grindr*, Plaintiffs take issue with Apple’s failure to deploy a product or tool that prevents bad actors from misusing its product. According to Plaintiffs, “Apple’s failure to implement any known CSAM detection is a design defect.” TAC ¶ 220. But Plaintiffs cannot avoid the fact that a tool that *detects* CSAM must *review* CSAM to make such a determination. And while Apple *could* have taken steps to do so—as its competitors have done by using PhotoDNA—*Grindr* confirms that § 230 bars claims arising from the design decisions Apple *could* have taken where those claims relate to Apple’s role facilitating the communication and content of others.

Plaintiffs do confront *Doe I v. Twitter*, another case from 2025. 148 F.4th 635 (9th Cir. 2025). According to Plaintiffs, the *Twitter* decision supports their suit because it (1) “clarifies that claims aimed at a platform’s reporting systems and safety tooling do not treat the defendant ‘as a publisher’”; and (2) “emphasizes that Section 230 does not preclude claims based on a platform’s independent statutory duties.” Opp’n at 4-5. Plaintiffs are incorrect on both counts.

On the first issue, Apple points out that Plaintiffs are attempting to “shoehorn” their claims into *Twitter*’s “separate discussion of user reporting mechanisms and statutory reporting

violations.” Reply at 4, ECF No. 84. This case does not concern or even discuss Apple’s content reporting systems; it concerns Apple’s “failure to implement industry-standard safeguards” against the dissemination of CSAM. Opp’n at 8. Though reporting systems and CSAM safeguards may both be described as “defects,” the latter requires the Court to treat Apple as a publisher. Twitter “could fulfill its purported duty to cure reporting infrastructure deficiencies without monitoring, removing, or in any way engaging with third-party content,” *Twitter*, 148 F.4th at 645; Apple cannot fulfill a duty to institute CSAM safeguards without deploying a tool like NeuralHash or PhotoDNA. Both NeuralHash and PhotoDNA were built to monitor and report violative images uploaded to company servers. Yet just the decision regarding whether to *deploy* either tool is a choice related to content moderation. And “any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under [§] 230.” *Roommates.com*, 521 F.3d at 1170–71.

As to the second reason, Plaintiffs misconstrue *Twitter*’s actual ruling: it was only when “Twitter ha[d] obtained *actual knowledge* of [CSAM] . . . [that] it had a legal duty to promptly report that content to NCMEC.” *Twitter*, 148 F.4th at 647-48 (emphasis added). The Ninth Circuit was careful to distinguish that duty, which arose out of a statute, from a duty that would require Twitter to “scour its platform for content triggering its NCMEC-reporting duty.” *Id.* As the law stands, Apple likewise does not have a duty to go looking for CSAM on its servers via NeuralHash or any other means, no matter how easy it may be for them to do so.

Additionally, Plaintiffs ignore the portions of *Twitter* they find unfavorable, even though those portions bear directly on the issues here. The Ninth Circuit explicitly held that, when an interactive computer service provider is facilitating the dissemination of “content created by others, it is functioning as a publisher and is immune from liability related to that content” under § 230. *Id.* at 640. This is exactly what iCloud does: it grants users the ability to share their own content. In so doing, iCloud is “functioning as a publisher and is immune from liability related to” the underlying content, whether that be CSAM or something else.

Finally, and despite Plaintiffs arguments to the contrary, the Ninth Circuit’s decision in *Lemmon* does not require a different outcome. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1093 (9th

1 Cir. 2021); Opp’n at 7. The plaintiffs in *Lemmon* challenged a Snapchat filter that showed the
 2 speed a user was traveling, which the plaintiffs alleged encouraged reckless driving. *Id.* at 1088–
 3 89. When a young driver used the speed filter shortly before a fatal crash, his parents sued for
 4 negligent design. *Id.* at 1088, 1091-92. The Ninth Circuit allowed the claims to proceed because
 5 *Snap* had designed the filter that incited the crash and because “Snap could have satisfied its
 6 ‘alleged obligation’ . . . without altering the content that Snapchat’s users generate.” *Id.* at 1092.
 7 In short, the claim stood “independently of the content,” be it photo or video, “created with the
 8 Speed Filter.” *Id.* at 1093. In contrast, all of Plaintiffs’ claims here are inexorably linked to third-
 9 party content; Plaintiffs do not allege that Apple created content like a Snapchat filter that caused
 10 them harm.

11 Considering the case law discussed above, Apple cannot be held liable for any of
 12 Plaintiffs’ claims because they all treat Apple as a publisher. Apple’s motion to dismiss the TAC
 13 is therefore GRANTED.

14 * * *

15 This Order does not turn on whether Apple’s decisions contributed to Plaintiffs’ injuries.
 16 All Plaintiffs’ claims are founded on Apple serving as a publisher of third-party content. It is that
 17 role as “publisher” that is dispositive on the issue of immunity. This does not mean that the
 18 existence of images and videos of the putative class members being sexually abused—content that
 19 they allege is regularly stored and disseminated on iCloud—has not caused Plaintiffs real and
 20 lasting harm. The current state of the law mandates that if Apple’s role in this harm “springs from
 21 [its] status as publisher,” Plaintiffs cannot hold the company accountable for those injuries.
 22 *Twitter*, 148 F.4th at 642.

23 Protecting children from sexual abuse and exploitation is neither partisan nor new. In
 24 recent years Senators Grassley and Durbin have collaboratively worked on bi-partisan legislation
 25 to address CSAM and online child exploitation.⁷ In 1984, President Reagan signed the Child

26 _____
 27 ⁷ See, e.g., Sentencing Accountability for Exploitation Act (SAFE) Act, S. 3394, 119th Cong.
 28 (2026); Ending Coercion of Children and Harm Online (ECCHO) Act, S. 3397, 119th Cong.
 (2026). Senators Graham and Blumenthal have also made attempts to address these same issues in

Protection Act, which was crafted to address and toughen the laws on the growing production and distribution of child pornography. When he signed the law, he expressed deep concern about our collective obligation to prevent the sexual abuse of children caused by the creation and dissemination of child pornography.⁸ And here we find ourselves more than forty years later, with the volume of child exploitation cases expanding year over year, and child pornography distributed at a speed and volume that was inconceivable when President Reagan made his remarks.⁹

The outcome of this case is bound by precedent. But the outcome also adds credence to claims that the Ninth Circuit “has expanded § 230(c)’s scope to provide functional immunity to internet companies, even when they are aware (or should be aware) of unlawful content on their websites.” *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 747 (9th Cir. 2024) (Nelson, J. concurring). The practical outcome is that the current state of the law prioritizes privacy—a laudable and critically important value given that in our modern world nearly all our most personal and intimate data (including financial and health records) are stored and transmitted online. But the law should not ignore how those who create, view, and distribute child pornography leverage

a series of bills introduced in the early 2020s; all stalled in committee. *See* Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020, S. 3398, 116th Cong. (2020); EARN IT Act of 2022, S. 3538 117th Cong. (2022); EARN IT Act of 2023, S. 1207, 118th Cong. (2023).

⁸ President Regan stated:

I feel very strongly about these measures. There’s no one lower or more vicious than a person who would profit from the abuse of children, whether by using them in pornographic material or by encouraging their sexual abuse by distributing this material . . . This pornography is ugly and dangerous. If we do not move against it and protect our children, then we, as a society, just aren’t worth much.

Ronald Reagan, Remarks on Signing the Child Protection Act of 1984 (May 21, 1984) (available at <https://www.reaganlibrary.gov/archives/speech/remarks-signing-child-protection-act-1984>).

⁹ “Because child pornography is now traded with ease on the Internet, ‘the number of still images and videos memorializing the sexual assault and other sexual exploitation of children, many very young in age, has grown exponentially.’” *Paroline v. United States*, 572 U.S. 434, 440 (2014) (quoting U.S Sentencing Comm’n, P. Saris et al., Federal Child Pornography Offenses 3 (2012)).

1 privacy protections to avoid detection by law enforcement. In the current legal framework, there
2 is no protection for members of the putative class—individuals who as children were
3 photographed and filmed while being abused in the vilest ways imaginable, and who now are
4 repeatedly victimized each time the intimate and tortured images of their trauma are distributed to
5 others. Those children are the collateral damage of our ineffective legal landscape. They deserve
6 better.

7 But lawmakers have not yet amended § 230 or enacted other legislation to address this
8 issue, and the Ninth Circuit broadly reads the scope of immunity in § 230. *Gonzalez v. Google*
9 *LLC*, 2 F.4th 871, 913 (9th Cir. 2021) (Berzon, J., concurring) (noting the “growing chorus of
10 voices calling for a more limited reading of the scope of [§] 230 immunity”), *vacated*, 598 U.S.
11 617 (2023).

12 Accordingly, Apple is immune from the claims raised by Plaintiffs in this suit.

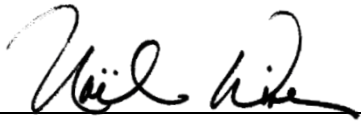
13 **IV. CONCLUSION**

14 For the reasons stated, the Court GRANTS Apple’s motion to dismiss the TAC. Because
15 all Plaintiffs’ claims seek to treat Apple as a publisher of third-party content, the Court finds that
16 amendment would be futile. Plaintiffs’ suit is DISMISSED WITH PREJUDICE.

17 The Clerk of the Court is directed to close the case.

18 **IT IS SO ORDERED.**

19 Dated: July 13, 2026



Noël Wise
United States District Judge