United States Senate

WASHINGTON, DC 20510

November 18, 2026

John Ternus
Chief Executive Officer
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Dear Mr. Ternus:

We write to follow up on our January 9, 2026, letter urging Apple to enforce its App Store policies against X and Grok for the mass generation of nonconsensual sexualized images of women and children. Nearly ten months later, independent investigations demonstrate that Apple continues to distribute applications marketed and distributed for the purpose of generating nonconsensual intimate imagery via its App Store. These findings demonstrate Apple's continued failure to enforce its own policies and raise serious questions about the effectiveness of the safeguards it has repeatedly cited to excuse the continued presence of these apps in the App Store.

The consequences of these failures are not hypothetical. A 2024 survey by the Center for Democracy & Technology found that 15% of U.S. public high school students knew of AI-generated nonconsensual intimate imagery (NCII) depicting someone at their school. A separate 2025 Thorn survey found that 6% of young people reported having been targeted by AI-generated NCII. Internationally, in February 2026, UNICEF reported that at least 1.2 million children in 11 countries disclosed being victims of nonconsensual nudification in the past year. Outside of schools, NCII is frequently weaponized against female journalists, human rights defenders, politicians, and other prominent women – not simply to humiliate them, but to discredit, intimidate, and silence their work and advocacy. Research by the American Sunlight Project revealed that one in six female Members of Congress were targeted by sexually explicit deepfakes and a 2025 New America investigation documented 100 cases involving public officials across 14 countries, 97 of them involving women. A 2026 UNESCO and UN Women report also found that 45% of surveyed women journalists had self-censored in response to online violence, underscoring the broader threat of image-based sexual abuse to women's free expression rights.

Despite the stakes and prevalence of these harms, and contrary to its own rules, Apple continues to distribute NCII-generating apps. In April 2026, the Tech Transparency Project (TTP) reported that Apple's App Store search results and advertisements directed users to applications capable of digitally undressing people in photographs or placing their likenesses into sexually explicit content without their consent. Across Apple's App Store and Google Play, applications identified in that investigation had accumulated an estimated 483 million downloads and more than $122 million in lifetime revenue. A further investigation by TTP published in October found that test

accounts for a 13-year-old boy could download dozens of applications capable of nonconsensual AI-generated intimate imagery. Across Apple's App Store and Google Play, 135 applications were available to TTP's test accounts with a combined 5.5 billion downloads and $3.9 billion in estimated lifetime revenue. These findings suggest that Apple is not merely failing to remove applications that facilitate intimate image abuse, it may also be profiting from their distribution in its App Store.

More troubling still, Apple's review processes allow developers to conceal prohibited functionality. In November 2026, AI Forensics documented a network of 444 connected applications, some of which concealed sexual deepfake functionality from app store reviewers but revealed it to users arriving via advertisements on Meta's platforms. In accompanying reporting, WIRED documented links to Hong Kong-registered KeLing Technology Limited, prompting Apple to remove 19 associated applications. Apple explained that developers had changed the websites supplying the applications' content after approval. Together, these findings expose a vulnerability that cannot be addressed through initial app review alone: developers can use remotely hosted content and referral-based techniques to deliver prohibited functionality to customers after clearing initial review.

In October 2026, Apple revised its App Review Guidelines to explicitly address AI-generated nonconsensual intimate imagery and clarify its longstanding prohibition on apps that conceal functionality during review or change their features after approval. But clarifying these prohibitions is not the same as effectively enforcing them. Developers who change remotely hosted content or reveal prohibited features only to users having arrived through particular advertisements may evade Apple's initial review. Preventing these abuses requires effective detection and enforcement - not just clearer platform rules.

Moreover, Apple has access to industry intelligence that could help it identify abusive applications and coordinated developer networks, both at initial review and in subsequent monitoring. Through the Tech Coalition's Lantern information-sharing program, Apple is reported to have access to signals shared by participating companies concerning detection of harmful activities across platforms. In June 2025, Meta announced that it had shared more than 3,800 unique URLs associated with nudify applications and websites through Lantern since late March 2025. It remains unclear whether Apple accessed or utilized that information, whether any applications identified by AI Forensics or WIRED were previously flagged, or whether Apple incorporated those signals into its review and enforcement systems.

These findings raise questions not only about individual failures of app review, but also about Apple's ability to identify repeat offenders, disrupt coordinated networks, and monitor apps after approval. The TAKE IT DOWN Act, enacted in May 2025, criminalizes certain nonconsensual disclosures of intimate imagery and imposes removal obligations for imagery published on covered platforms. However, its enactment has not resolved the proliferation of apps marketed or designed to facilitate this abuse. That gap warrants scrutiny of both Apple's enforcement practices and potential gaps in federal law. To help examine those gaps, please respond to the following questions:

- For each year from 2022 through 2026, how many applications has Apple rejected, removed, or suspended for enabling users to generate nonconsensual nude or sexually explicit imagery in violation of Apple's policies? Please provide the applicable guidelines, annual totals, and the number of actions initiated proactively rather than in response to external reports.
- Apple's 2025 transparency report lists 360 removals under Guideline 1.1.4 concerning sexual and pornographic content. How many of those removals involved applications facilitating NCII or sexual deepfake abuse? Under what other guidelines are such violations recorded, and will Apple begin reporting NCII-specific enforcement statistics?
- How does Apple test applications to determine whether they can generate nude or sexually explicit images from photographs of identifiable people, in violation of its App Review Guidelines? Does Apple test face-swapping capabilities, paid features, remotely hosted functionality, and other methods developers may use to conceal these capabilities during review?
- When did Apple first become aware that developers were concealing prohibited functionality by displaying different interfaces or features to users arriving through particular advertisements or referral sources? Does Apple's review process test these pathways, including links from Facebook and Instagram advertisements?
- In 2024, 404 Media reported that apps listed as "art generators" in Apple's App Store were advertised on Instagram and adult websites as tools to undress women. What, if any, changes did Apple make to its review and monitoring processes in response, and why did those changes not detect the network identified by AI Forensics and WIRED?
- What specific technical or procedural changes did Apple implement following its October 2026 App Review Guidelines Revisions? How does Apple detect changes to remotely hosted content or other functionality after an app has been approved, and how many additional apps have been identified or removed through these measures?
- Has Apple received or accessed Lantern signals relating to nudify apps, associated websites, or developer networks? If so, how many such signals corresponded to apps submitted to or distributed through the App Store, when did Apple receive them, and what investigations or enforcement actions resulted?
- Were any applications or associated domains identified by AI Forensics or WIRED previously reported to Apple through Lantern or other information-sharing resources? If so, when did Apple first receive the relevant information and why were the applications still available?
- What has Apple learned from its investigations into the developers and networks responsible for distributing apps intended to facilitate NCII, including those identified by AI Forensics and WIRED? Please describe the networks' apparent operators, geographic locations, common technical infrastructure, methods of evading app review and enforcement, and use of intermediary developers or companies. To what extent have these networks continued operating or returned to the App Store following enforcement actions?

Apple has repeatedly defended its control over app distribution as necessary to protect users. Yet independent researchers continue to document apps on Apple's App Store that generate

nonconsensual intimate imagery, including apps purpose-built for abuse and engineered to conceal that purpose from Apple's reviewers. Apple must explain why its review and enforcement systems have failed and what concrete measures it will take to more effectively enforce its own policies. We request responses to the above questions by December 9, 2026.

Sincerely,

Ron Wyden
United States Senator

Ben Ray Lujan
United States Senator

Edward J. Markey
United States Senator