United States Senate

WASHINGTON, DC 20510

November 18, 2026

Sundar Pichai
Chief Executive Officer
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

We write to follow up on our January 9, 2026, letter urging Google to enforce its Google Play 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 Google continues to distribute applications marketed and distributed for the purpose of generating nonconsensual intimate imagery via its app store. These findings demonstrate Google'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 presence of these apps on Google Play.

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, Google continues to distribute NCII-generating apps. In April 2026, the Tech Transparency Project (TTP) reported that Google Play search results, autocomplete suggestions, 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 Google is not merely failing to remove applications that facilitate intimate image abuse - it may also be profiting from their distribution on Google Play.

More troubling still, Google'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. Researchers identified 27 apps associated with the network on Google Play as of September 11, including 20 rated suitable for all ages. In accompanying reporting, WIRED documented links to Hong Kong-registered KeLing Technology Limited and described how remotely hosted content and referral information could determine which features an application displayed. WIRED reported that Google had removed most of the implicated apps before the publication contacted the company, but it remains unclear when Google detected the network, how it identified the apps, or whether its enforcement disrupted the developers responsible. 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.

Google prohibits applications that claim to undress people or see through clothing and has repeatedly emphasized the sophistication of its app review systems. In February 2026, Google reported preventing more than 1.75 million policy-violating applications from being published in 2025 and banning more than 80,000 developer accounts. In August 2026, Google warned developers about AI-facilitated NCII, directed particular attention to "nudify," "undress," and deepfake features, and stated that it enforces its policies against apps that advertise nudifying capabilities on any platform. Yet the following month, 27 apps belonging to a network promoted through explicit advertisements on Meta's platforms were available on Google Play. Clarifying policies and reporting large enforcement totals is not the same as effectively identifying applications designed to facilitate NCII. Preventing these abuses requires effective detection and enforcement, including monitoring applications after approval.

Moreover, Google 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, Google has 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 Google accessed or utilized that information, whether any applications identified by AI Forensics or WIRED were previously flagged, or whether Google incorporated those signals into its review and enforcement systems.

These findings raise questions not only about individual failures of app review, but also about Google'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 Google'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 Google rejected, removed, or suspended for enabling users to generate nonconsensual nude or sexually explicit imagery in violation of Google's policies? Please provide the applicable guidelines, annual totals, and the number of actions initiated proactively rather than in response to external reports.
- Google's 2025 safety report states that it prevented more than 1.75 million policy-violating applications from being published and banned more than 80,000 developer accounts. How many of those actions involved applications facilitating NCII or sexual deepfake abuse? How does Google classify these violations in its transparency reporting?
- How does Google test applications to determine whether they can generate nude or sexually explicit images from photographs of identifiable people, in violation of Google Play policies? Does Google test face-swapping capabilities, paid features, remotely hosted functionality, and other methods developers may use to conceal these capabilities during review?
- When did Google 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 Google's review process test these pathways, including links from Facebook and Instagram advertisements?
- How does Google 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?
- Google has stated that it enforces its policies against apps that advertise nudifying capabilities. How does Google monitor advertising on other platforms, including Meta's, for promotion of Google Play apps? How many enforcement actions has Google taken on this basis, and did any involve apps associated with the network identified by AI Forensics and WIRED?
- Has Google 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 Google Play, when did Google receive them, and what investigations or enforcement actions resulted?
- Were any applications or associated domains identified by AI Forensics or WIRED previously reported to Google through Lantern or other information-sharing resources? If so, when did Google first receive the relevant information and why were the applications still available?

- What has Google 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 Google Play following enforcement actions?

Google has repeatedly defended its app review and enforcement systems as essential to protecting users. Yet independent researchers continue to document apps on Google Play that generate nonconsensual intimate imagery, including apps purpose-built for abuse and engineered to conceal that purpose from Google's review. Google 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 Luján
United States Senator

Edward J. Markey
United States Senator