Surveillance Is Not Safety

TypexAI Official Position Statement on User Privacy | *June 10, 2026*

On June 7, 2026, UK Prime Minister Keir Starmer issued a public ultimatum to Apple and Google: within three months, both companies must activate OS-level scanning to detect and block sexually explicit images involving minors across all applications on their platforms. If they fail to comply, the government has stated it will legislate — with potential criminal liability for executives. This is not a hypothetical. It is an active policy demand with a concrete deadline directed at the two operating systems that run the majority of the world's personal devices.

What OS-Level Scanning Actually Means

This proposal does not target specific applications. It targets the operating system itself. If implemented, Android and iOS would scan content at the system level — before it reaches any individual app. Every application distributed through Google Play or the App Store would operate on an infrastructure that analyses user content by default. Individual developers would have no mechanism to opt out on behalf of their users. The scanning would occur regardless of the privacy architecture of any given application.

The risks extend beyond the stated purpose. Surveillance infrastructure built for one defined task rarely remains limited to it. The technical capacity to detect one category of content can be reconfigured — by policy decision, not engineering — to monitor political speech, personal beliefs, or private correspondence. This is not speculation. It reflects the consistent historical pattern of how monitoring systems evolve once the foundational precedent has been accepted.

There is also a structural security risk: any system capable of scanning private content at scale is a high-value target for malicious actors. Its existence creates new attack surfaces affecting all users in all jurisdictions.

How This Affects Bardo

Bardo is a fully local, offline-first note-taking application distributed via Google Play. It has no backend infrastructure. User data never leaves the device. Notes are stored in encrypted form, and Bardo applies system-level protections — including Android's FLAG_SECURE — to prevent screen capture and on-screen analysis by third-party processes.

The current UK initiative is specifically targeted at image-based content. Bardo does not store or transmit user images, which places it outside the direct scope of the present proposal. However, the precedent being established is not narrow. Once OS-level content inspection becomes a legal norm, its extension to text, documents, and any other personal content requires only a policy decision, not new technical infrastructure.

If Google proceeds with OS-level scanning under UK government pressure, TypexAI will deploy all available technical measures to protect Bardo users — including screen visibility controls, process isolation, and steganographic techniques. In that context, TypexAI's technology Veil becomes directly relevant: Veil allows sensitive text to be concealed inside ordinary-looking text, optionally protected by a password, so that even content visible on screen carries no readable signal to an automated scanner. Veil exists today as a standalone tool at typexai.dev/veil. Its integration into Bardo is under active consideration as a response to precisely this type of regulatory risk.

TypexAI's Position

TypexAI fully supports the protection of children from harm. We do not believe, however, that converting personal devices into inspection infrastructure is an effective, proportionate, or safe method of achieving this. Effective child safety requires systemic investment: funding protection services, improving digital literacy for minors and parents, targeted law enforcement action against illegal actors, and meaningful accountability for platforms that knowingly distribute harmful material.

TypexAI is based in Tallinn, Estonia. In February 2026, Estonian Minister Kristina Kallas publicly stated that Estonia does not support mandatory monitoring of private communications. TypexAI's values are consistent with and reinforced by this national position.

We will continue building Bardo and future products on the principle that private digital space must remain private. We will not voluntarily introduce content scanning or background analysis of user data. And we will continue to develop technical safeguards that protect our users regardless of what platform-level decisions are made above us.

TypexAI — Tallinn, Estonia