Policy Briefing: Safeguarding Independent Software Distribution in the EU

Date: August 2025
Prepared for: European Commission, National Regulators, Digital Rights Stakeholders

---

Executive Summary

Google's intent to restrict app deployment exclusively to *registered and verified developers* raises profound questions for Europe's digital future. While framed as a security measure, this model risks undermining **competition law, the EU's Digital Markets Act (DMA)** objectives, and the Commission's agenda on **digital sovereignty**.

Independent and open-source ecosystems—such as **F-Droid**—provide essential benefits in transparency, security auditing, and diversity of innovation. Restricting such platforms erodes **user autonomy**, consolidates market power in the hands of non-European corporations, and weakens the EU's ability to govern its own digital sphere.

Regulators must act to ensure Europeans retain the right to install, distribute, and develop lawful software outside of corporate-controlled channels.

Key Concerns within the EU Context

1. **Digital Sovereignty at Risk**
   - The EU has committed, through policy strategies such as the **EU Digital Strategy (Shaping Europe's Digital Future)**, to reduce dependency on non-European gatekeepers.

   - A closed distribution model transfers control of Europe's digital economy further into the hands of a single US-based corporation.
2. **Conflict with the Digital Markets Act (DMA)**
   - The DMA directly prohibits practices by "gatekeepers" that restrict interoperability or limit fair access for competitors.

   - By blocking alternative app stores and distribution models, Google's restrictions may **fall foul of Articles 6 and 7 of the DMA**, which seek to prevent abusive self-preferencing and forced exclusivity.
3. **User Rights and Fundamental Freedom**
   - The **Charter of Fundamental Rights of the EU** guarantees freedom of expression and information (Article 11). Restricting

lawful apps to corporate-approved channels limits individuals' ability to access, produce, and share digital tools.

  - The emerging **Right to Repair movement**—supported within EU legislation—extends naturally to the right of users to control their digital devices, including the software they install.

4. **Security Claims Do Not Justify Monopoly**
   - True cybersecurity in the EU rests on **diversity and transparency**, not corporate secrecy.

   - Open-source auditing and decentralized distribution help the EU's **NIS2 Directive** objectives for a resilient, cyber-secure internal market.

Impacts for Europe

- **On Developers & SMEs**: Independent European developers face higher entry barriers and exclusion from distribution ecosystems dominated by US-based corporations.

- **On Competition**: Violates the spirit of the DMA by strengthening non-European monopolies, reducing opportunities for European SMEs and startups.

- **On Users & Citizens**: Diminished autonomy, reduced choice, and dependence on external actors for basic digital functions.

- **On EU Policy Goals**: Weakens commitments to **open innovation, sovereignty, and resilience** outlined in Europe's Digital Decade targets.

Policy Recommendations

1. **Enforce the Digital Markets Act (DMA) Robustly**
   - Treat restrictions on third-party app distribution and side-loading as violations of gatekeeper obligations.

   - Invest in enforcement capacity within the European Commission to monitor compliance.

2. **Guarantee User Sovereignty through EU Digital Legislation**
   - Extend the principles of the **Right to Repair** and **Digital Fairness Act proposals** to enshrine the right to install and control lawful applications.

    - Explicitly protect **software openness and interoperability** in forthcoming EU policy frameworks.

3. **Promote Open Verification Standards**
    - Develop **European-led, decentralized app verification mechanisms** (e.g., EU-recognized cryptographic signing frameworks) to ensure trust without relying on external gatekeepers.
4. **Protect and Promote Open-Source Ecosystems**
    - Recognize open-source distribution platforms (like F-Droid) as **European public interest digital infrastructure**.

    - Provide EU funding and legal protections for community-driven app repositories to enhance innovation and resilience.

Conclusion

Restricting app deployment to corporate-approved, “verified” developers undermines the **Digital Markets Act**, diminishes **digital sovereignty**, and weakens Europe’s **innovation environment**. Open and independent distribution channels are not a security threat—they are a cornerstone of resilience, competition, and democratic digital governance.

The EU must respond decisively, enforcing gatekeeper obligations under the DMA, protecting user rights, and supporting open-source ecosystems as strategic assets for Europe’s digital future.