We introduce a system to analyze Android apps’ compliance with privacy requirements:

- We define privacy requirement compliance to mean that apps need a privacy policy and must behave according to it.
- In addition, the policy by itself is required to follow requirements (e.g., on notifying a user on access, edit, and deletion rights).
- In detail, apps that process Personally Identifiable Information (PII) are generally required to:
  1. Have a privacy policy (either on its Google Play page or inside the app).
  2. Include notices about policy changes and access, edit, and deletion rights.
  3. Notify users of data collection practices.
  4. Disclose how data is shared with third parties.

Classification results for a policy test set (n=40) and the occurrence of positive classifications (Pos) in a set of n=9,050 policies

- 2,455 apps have one potential privacy requirement non-compliance, 2,460 have two, and only 1,461 adhere completely to their policy (out of n = 9,050 apps).
- Each app exhibits a mean of 1.83 instances of potential privacy requirement non-compliance.
- Non-compliance does not necessarily mean that a law is violated.