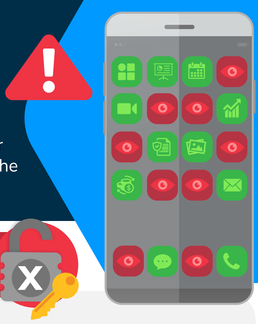
INFOGRAPHIC

The 5 Most Overlooked Mobile App Privacy Risks

Modern mobile apps leak more data than most teams realize. These overlooked privacy gaps threaten customer trust, regulatory compliance and brand reputation. Spot the biggest blind spots and the privacy risks they introduce.



Risk 1 Excessive or Dangerous Permissions

Mobile apps often request more permissions than necessary, exposing sensitive data.

Why It Matters

- Expands the privacy attack surface
- Enables fingerprinting, sensor access and device insights
- Increases the impact of any compromise
- Creates regulatory and compliance risk (GDPR, CCPA, HIPAA, etc.)

Where It Hides

- Legacy permissions left in code or templates
- SDKs silently adding or expanding permissions

How to Reduce the Risk

- Enforce least privilege and validate permission behavior during runtime
- Continuously test to detect permission changes in every update

Risk 2 Uncontrolled Sensitive Data Collection & Sharing

Many apps collect or retain more personal data than required for core functionality.

Why It Matters

- Creates regulatory exposure
- Unmonitored data flows bypass governance controls
- Erodes user trust and increases breach impact

Where It Hides

- Ad/analytics libraries with aggressive data defaults
- APIs that pass sensitive data in unexpected ways

How to Reduce the Risk

- Continuously test app behavior and analyze data flows, collection patterns and retention practices

Risk 3 Hidden Data Flows in Third-Party SDKs & APIs

Third-party components often transmit data to external domains without clear visibility or control.

Why It Matters

- Third-party leakage drives many privacy findings
- Dynamic SDK behavior can change after app release
- Violates compliance requirements for third-party governance

Where It Hides

- Ad/analytics libraries with aggressive data defaults
- APIs that pass sensitive data in unexpected ways

How to Reduce the Risk

- Validate SDK and API behavior through continuous testing

Risk 4 Unmonitored Network Connections & External Transmission

Apps frequently call external servers, content delivery networks and services users never see — sometimes insecurely.

Why It Matters

- Exposes sensitive data to interception and misuse
- Creates unapproved or unknown data flows
- Weakens privacy posture

Where It Hides

- Background network calls not covered in pre-release testing
- Legacy TLS, cleartext traffic or broken certificate pinning

How to Reduce the Risk

- Monitor outbound traffic for insecure or unauthorized connections

Risk 5 AI-Driven Data Exposure

AI-powered features capture rich user inputs, but their data pipelines often lack transparency.

Why It Matters

- Sensitive voice, image and behavioral data may feed external models
- Third-party AI services often retain or reuse uploaded data
- Creates unpredictable privacy and compliance consequences

Where It Hides

- AI inference APIs processing raw user content
- Model training repositories with unclear retention rules

How to Reduce the Risk

- Assess AI components as standalone processors with dedicated controls

Validate Mobile Privacy Across Every Build

Meet regulatory demands, accelerate audits and safeguard your brand by finding and fixing hidden privacy gaps. NowSecure Privacy provides continuous visibility into what your mobile apps collect, share and expose.

NowSecure