JS|HELD

PERSPECTIVES

Strategies for Mobile App Developers to Minimize Rising Risks from Privacy Laws

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

As mobile device applications continue to proliferate – magnified in no small part by the recent surge in artificial intelligence-related tools to facilitate creation of apps – they have become indispensable tools for communication, entertainment, and commerce.

Just like websites and other internet-connected platforms, mobile apps must also adhere to stringent data privacy regulations and require proper user consent before sharing personal data with third parties. These laws and regulations include the General Data Protection Regulation (GDPR) in the European Union and in the United States: the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and various US state laws including the California Consumer Privacy Act (CCPA).

However, privacy teams often face challenges in maintaining compliance due to limited visibility and reliance on manual processes, particularly when managing data flows to third-party software development kits (SDKs). These SDKs – complex software packages used to integrate features like advertising, analytics, and customer engagement – pose significant privacy risks as they automatically collect sensitive data such as device and advertising identities. They're also generally more challenging for compliance needs due to their proprietary code and underlying engineering attributes.

This article explores key strategies to minimize privacy risks involving mobile apps and SDKs, given the incrementally expanding US data privacy laws and international frameworks like GDPR that will increase the potential for privacy-related scrutiny of these technologies.

DATA MINIMIZATION AND PURPOSE LIMITATION: CORE PRINCIPLES IN MOBILE APPS

Data minimization and purpose limitation are foundational privacy tenets that dictate collecting only the data necessary for a specified purpose and using it solely for that purpose unless further consent is obtained. This may seem self-evident but gets increasingly complex given the tendency of third-party applications to 'daisy chain' together. When data is shared with one third-party application it can inadvertently share data with other third-party applications as well. These tendencies can be numerous and challenging to track for app and website owners. As such, data minimization and purpose limitation help simplify workflows and reduce costs. In a number of respects, they can be considered guardrails to help manage 'access.' Broken down a bit further, and perhaps more simply:

Data Minimization: This means an app should grab only the information it absolutely needs to do its job. Imagine a weather app: it needs your city to give you a forecast, but it doesn't need your exact street address or your contact list. If it's collecting more than the bare minimum – like a flashlight app asking for your location when all it needs to do is turn on your phone's light – that's a red flag.

Purpose Limitation: This prescribes an app to only use your data for the stated reason it disclosed upfront. For example, if a fitness app collects your step count to track your workouts, it shouldn't surreptitiously use that data to sell ads until it asks you first. It helps maximize transparency in the underlying code and processes.

These concepts matter because they protect users and organizations from apps that overreach. In the US, laws like California's CCPA push for this. Regardless of explicit reference in privacy laws, these measures are part of best practices that will help organizations if or when challenged. The GDPR, on the other hand, is much stricter and explicit – data has to be necessary for the app's purpose, without exceptions. For example, a game asking for your exact GPS location to "check local laws" could swap that for a simple "pick your country" dropdown, keeping things minimal and purpose driven.

PERMISSIONS AND PROCESSING: RUNTIME VS. INSTALL-TIME DILEMMAS

Mobile apps interface with users through permissions, which vary in timing and impact. Runtime permissions—

prompts appearing during app use (e.g., requesting camera access when snapping a photo)—are lauded for aligning with data minimization by seeking consent only when needed. Install-time permissions, requested upon app launch, often grant blanket access without immediate justification, potentially violating minimization principles. For example, an app requesting photo access at startup, absent clear context, may amass unnecessary data, contravening both GDPR and US state laws. Even with the best of intentions, collecting data for "wait and see" use cases is problematic and costly.

Runtime permissions keep data collection tied to the moment it's needed, matching up with data minimization. Install-time permissions can let an app collect data it doesn't yet (or ever) need, which could violate rules like the GDPR's and, increasingly US laws' necessity test if it's not clear why the data is being gathered. For attorneys, this is a key area to check: if an app is asking for too much too soon, it might be stepping over the line.

On-device processing further bolsters minimization. By handling sensitive data locally—say, analyzing biometric scans without server transmission—apps limit exposure. The Illinois Biometric Information Privacy Act (BIPA) exemplifies this. Case law suggests that purely on-device biometric processing may not trigger BIPA's stringent consent and retention rules, sparing developers from its hefty penalties. Automated deletion protocols, where stale data self-destructs after inactivity, also enhance compliance by reducing retention risks, a strategy resonant with both GDPR's storage limitation and US sensitive data laws.

SDKS AND THIRD-PARTY DISCLOSURES: HIDDEN RISKS

SDKs—prebuilt code libraries enabling features like analytics or ads—are ubiquitous in mobile apps but can raise potential red flags in a privacy risk profile. Often, developers integrate SDKs without fully mapping their data flows, risking unintended disclosures.

For example, an SDK leveraging a user's geolocation permission – based on the permission a user granted to the app – might share that data with the company that developed the SDK, which in turn may use it for targeted ads. Without contractual safeguards, such transfers may violate US cross-border restrictions, such as GDPR's third-party obligation or California's CCPA and its regulations which secure privacy rights for consumers including the right to opt out of the sale or sharing of consumers' personal information. For these reasons and others, it is critical for developers to understand the mechanisms of SDKs included in their mobile apps, and to initiate contract agreements when appropriate. Organizations developing mobile apps for business purposes should strongly consider inventorying SDKs, assessing their data handling, and negotiating agreements to ensure compliance with applicable laws.

TRANSPARENCY AND CONSENT: MOBILE-SPECIFIC CHALLENGES

Mobile screens constrain the ability to offer privacy notice presentations / pop-ups as commonly seen on websites, which in turn necessitates more layered disclosures and user navigation. Just-in-time notices—alerting users at the point of data use—enhance transparency, as do continuous signals (e.g., a persistent location tracking indicator). In-app settings with toggles for consent withdrawal, like "do-not-sell" links, are now standard, though state laws diverge on placement. Unfortunately, these features can fail and are often prone to bugs, so frequent user testing is essential.

Consent design also matters. Dark patterns—manipulative interfaces skewing user choices—invite regulatory scrutiny and attention. Symmetrical (equally accessible consent options) are a best practice. The EU's e-Privacy Directive adds rigor, requiring consent for any device data access – a standard that US laws rarely match. Mapping data flows to user choices is thus critical, and testing these after every release will save your legal team headaches down the road.

POTENTIAL PRIVACY VIOLATIONS AND ENFORCEMENT TRENDS

Violations abound when apps over-collect, misuse, or disclose data. A gaming app harvesting health data for ads without consent can violate multiple laws at once – GDPR's purpose limitation, CCPA's sale disclosure rules, and Protecting Americans' Data from Foreign Adversaries Act (PADFAA). While this use case is blatant, subtler cases have emerged in health and wellness sites being held to the HIPAA standard. Both Washington and New York now have state laws that extend HIPAA-like obligations to health-related businesses, including fitness, beauty, and dieting. Because these laws are both in the early stages, the legal actions have come mostly through private rights of action, which often settle before going to court (though that is starting to change).

In addition to new privacy laws, plaintiffs' firms now often bring cases based on new interpretations of older laws, like the California Invasion of Privacy Act (CIPA) and the federal Video Privacy Protection Act (VPPA). These cases now number in the thousands and counting. A couple of noteworthy cases include an allegation of violating CIPA in Aviles v. LiveRamp and Jancik v. WebMD, the latter in which the defendant violated VPPA by allegedly allowing Facebook (Meta) Pixel to monitor what videos users were watching on the WebMD site.

SDK-driven disclosures to unvetted third parties risk similar fates, especially under the US Department of Justice's bulk data restrictions. Enforcement is escalating. The Federal Trade Commission's 2024 actions against location data brokers and California's focus on children's privacy signal a crackdown on opaque practices. Biometric Information Privacy Act (BIPA) violations from on-device biometric processing gone awry – e.g., unintended server transfers – also carry private rights of action, amplifying exposure.

As demonstrated, there are multiple risk areas involved with SDK use, inadvertently or otherwise. SDKs have the potential to:

- Gather excessive information
- Perform unauthorized data collection by third parties
- Wrongly share / use sensitive information

CONCLUSION: STRATEGIC COMPLIANCE IN A COMPLICATED LANDSCAPE

For mobile app developers and organizations utilizing mobile apps for business, privacy compliance demands a proactive, multi-faceted approach. Embedding data minimization via runtime permissions, on-device processing, and automated deletion helps mitigate risk. Transparent, user-friendly notices and robust consent mechanisms—aligned with technical flows—build trust and legality. SDK vetting and contractual oversight are critical as well, given cross-border and third-party complexities.

Additionally, given the myriad risks involved there is increased incentive in retaining outside counsel and / or expert advisors to help guide organizations in their development and execution of mobile apps and related applications.

In addition to advisory services and related guidance, outside experts also have access to customized and proprietary tools designed to assess app privacy risks. These tools are capable of scanning codebases, identifying data flows, and flagging compliance gaps, which can offer proactive solutions to help pinpoint potential risk areas. Those risks can then be adequately remediated before they evolve into regulatory or legal issues.

By flagging compliance gaps—whether under GDPR, CCPA, or PADFAA— attorneys and expert advisors empower developers and corporate stakeholders to remediate issues pre-launch, reducing legal exposure. These services can also include recommendations for policies tailored to a given organization, with recurring audits and / or privacy spot checks, as appropriate. In an era of fragmented, yet stringent, privacy laws, this combination of technology and diligence maximizes safeguards for user data and corporate integrity.

ACKNOWLEDGEMENTS

We would like to thank our colleague, Antonio Rega, and Ian Cohen of LOKKER, for providing insight and expertise that greatly assisted this research.

MORE ABOUT THE AUTHORS

Antonio Rega is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, data privacy & information governance, emerging technology and discovery on behalf of global corporations and law firms. Based in New York, Antonio focuses on leading complex investigations and matters involving proactive and reactive discovery and analysis, often conducting in-depth forensic examinations of electronically stored information (ESI) across repositories (cloud-based, localized, or mobile). He regularly assists clients with advisory and strategy through all phases of investigations, regulatory compliance or litigation needs, such as regulatory requests, responses to government subpoenas, and related governance needs, among other areas of specialization.

Antonio is a Certified Fraud Examiner (CFE); EnCase Certified Examiner (EnCE); Computer Certified Examiner (CCE); Cryptocurrency Tracing Certified Examiner (CTCE), CipherTrace; Blockchain Council's Certified Cryptocurrency Auditor (CCA); TRM Labs Certified Investigator (TRM-CI); and Licensed Private Investigator (PI) for the State of Texas.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 345 8592.

Ian Cohen is the chief executive officer and founder of LOKKER(www.lokker.com), providing online data privacy and compliance solutions for enterprises, as well as technical support for legal teams both during and after litigation. A former CEO of Credit.com and Chief Product Officer at Experian, Cohen is an expert in online data privacy, data risk, and consumer-permissioned data. He founded LOKKER to address privacy risks inherent in web modern architecture.