Supplementary Material for "Assessing Privacy Compliance Awareness and Practices Among Mobile Third-party Library Developers"

Fares F. Alharbi*
Indiana University-Bloomington
Bloomington, Indiana, USA and
Taibah University
Medina, Saudi Arabia
fafaalha@iu.edu

Ece Gumusel*
Rutgers University
New Brunswick, New Jersey, USA
ece.g@rutgers.edu

Luyi Xing
University of Illinois Urbana-Champaign
Champaign, Illinois, USA
lxing@illinois.edu

Xiaojing Liao
University of Illinois Urbana-Champaign
Champaign, Illinois, USA
xliao@illinois.edu

ACM Reference Format:
Fares F. Alharbi*, Ece Gumusel*, Luyi Xing, and Xiaojing Liao. 2026. Supplementary Material for "Assessing Privacy Compliance Awareness and Practices Among Mobile Third-party Library Developers". In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3830454.3832742

A Appendix

Open Science

Our research team has prepared the following artifacts available to the scientific community: (1) Recruitment Materials (§A.1), (2) Survey Questionnaire (§A.2), and (3) Interview Questionnaire (§A.3), and (4) Codebook (§A.4).

A.1 Recruitment Materials

A.1.1 Interview Invitation Email. Two recruitment emails were used to invite participants to the interview study. The emails shared identical study information, eligibility criteria, compensation details, and consent-related language, and differed only in the opening paragraph and subject line to reflect the recruitment source. One version was sent to survey respondents who indicated willingness to participate in a follow-up interview, and the other was sent to contributors of popular open-source SDK projects on GitHub.

Email Subject.

- *Follow-Up on Your Survey Participation: Scheduling an Interview*
- *Invitation: Short Interview About Your Open-Source Contribution*

Email Content. Greetings,
[Opening paragraph varied by recruitment source:]

- **Survey respondents:** Thank you for completing the survey and for indicating your willingness to participate in a follow-up interview.
- **Open-source contributors:** Thank you for your contributions to open-source Mobile SDK projects. As part of an academic research study, we are examining how SDK developers work and make design decisions.

The interview included approximately 22 questions and required approximately 20–30 minutes to complete. Participants were informed that the study had received ethics approval from the Institutional Review Boards of both Indiana University and the University of Illinois Urbana-Champaign.

Eligibility Criteria.

(1) Participants were 18 years of age or older.
(2) Participants were literate in English.
(3) Participants were Mobile SDK developers.

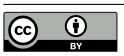
Compensation. Participants received a $25 Amazon gift card upon completion of the interview.

Privacy and Confidentiality. Information collected in this study was used solely for research purposes and was handled in accordance with institutional research ethics guidelines of the Institutional Review Boards of both Indiana University and the University of Illinois Urbana-Champaign.

How to Participate. Participants were invited to reply to the email to indicate their availability for scheduling the interview.
Fares F. Alharbi, Indiana University Bloomington (fafaalha@iu.edu)

A.1.2 Public Recruitment Post (Survey Invitation via Reddit). In addition to direct email recruitment, a public recruitment post was used to invite SDK developers to participate in the survey. The post was shared on Reddit in public, developer-focused communities and directed interested individuals to an anonymous online questionnaire.

*The work was completed with equal contribution, and the first two authors are listed in alphabetical order.



This work is licensed under a Creative Commons Attribution 4.0 International License.
CCS '26, The Hague, Netherlands.
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3832742

Post Content. Hi everyone,
We are researchers conducting a research project to understand Mobile SDK developers' practices. If you have built or maintained a mobile SDK, your insights would be incredibly valuable. The survey is anonymous and takes only a few minutes to complete.
https://iu.co1.qualtrics.com/jfe/form/SV_6Dr5tzIDdnL8vqK
Thank you for your time.

A.1.3 Public Recruitment Post (Interview Invitation via LinkedIn). In addition to email-based recruitment, a public recruitment post was shared on LinkedIn to invite SDK developers to participate in a follow-up interview. The post targeted developers with experience building or maintaining SDKs and provided contact information for scheduling interviews.

Post Content. Are you a Mobile SDK Developer? I'd Love Your Input!
Hi everyone! I am conducting research on mobile SDK development practices and am seeking developers with hands-on experience building or maintaining SDKs.
If you are open to participating in a short interview (approximately 25 minutes), your insights would be greatly appreciated. As a token of appreciation, participants received a $25 Amazon gift card upon completion of the interview.
Interested participants were invited to contact the researcher directly to schedule an interview.

A.2 Survey Questionnaire

This appendix presents the survey questionnaire administered to participants. The questions are shown in the same wording and order as presented in the online survey. The survey was anonymous, and no personally identifiable information was collected.

Background
In this section, please provide information about your professional experience.

(1) **Which of the following best describes your current role?** *Multiple choice; select all that apply*
- Mobile app developer
- Web developer
- Mobile SDK developer
- Open-source contributor/maintainer
- Privacy/cybersecurity engineer
- Other: specify

(2) **How familiar are you with integrating third-party SDKs or libraries?** *Single choice – Likert scale*
- Not familiar at all
- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

(3) **What platforms does your SDK primarily target? Select all that apply:** *Multiple choice; select all that apply*
- Android
- iOS
- Web
- Cross-platform (e.g., React Native, Flutter)
- Other: specify

(4) **What type of SDK(s) do you primarily work on?** *Multiple choice; select all that apply*
- Analytics/tracking
- Advertising/monetization
- Social/sharing features
- Payments/finance
- Authentication/security
- Developer utilities (e.g., UI kits, debugging tools)
- Other: specify

(5) **What is your primary role in SDK development?** *Single choice*
- Software Engineer
- Product Manager
- Compliance/Legal Specialist
- Security Engineer
- Other: specify

(6) **How many years of professional software development experience do you have?** *Single choice – Likert scale*
- <1 year
- 1–3 years
- 3–5 years
- 5–10 years
- 10+ years

(7) **Do you work in a team? If yes, how large is your SDK team?** *Single choice – Likert scale*
- 1-5
- 6-10
- 11-20
- 20+
- Not applicable

Attention Check

(8) **To confirm you are paying attention, please select "Car" below.** *Single choice*
- Airplane
- Car
- Train
- Boat
- Bicycle

Privacy Responsibility & Perception
In this section, we'd like to understand your awareness of privacy regulations and your responsibilities related to privacy compliance in SDK development.

(9) **How familiar are you with privacy regulations (e.g., GDPR, CCPA, COPPA, etc.)?** *Single choice – Likert scale*
- Extremely familiar
- Very familiar
- Somewhat familiar
- Slightly familiar
- Not familiar at all

(10) **Which privacy regulations are most relevant to your SDK? (Select all that apply)** *Multiple choice; select all that apply*
- GDPR (EU)
- CCPA/CPRA (California, USA)
- COPPA (Children's Privacy, USA)

- LGPD (Brazil)
- Other: specify

(11) **How confident are you that you understand what is required of you regarding privacy compliance (e.g., GDPR, CCPA/CPRA)?** *Single choice – Likert scale*
- Not confident
- Slightly confident
- Moderately confident
- Very confident
- Extremely confident

(12) **Who should be responsible for privacy compliance when your SDK is used in a mobile app? Select all that apply.** *Multiple choice; select all that apply*
- SDK developers
- App developers
- Platform providers (e.g., Apple, Google)
- Legal professionals
- Governance, risk, and compliance teams
- Privacy teams
- Other: specify

(13) **To what extent do you agree with the following statement?: "I feel responsible for ensuring privacy compliance of the SDK."** *Single choice – Likert scale*
- Not at all
- Slightly
- Moderately
- Very
- Fully

Privacy Compliance Practices

In this section, we'd like to learn about the practices and processes you/your team use to ensure privacy compliance in SDK development.

(14) **At what stage in SDK development do you consider privacy compliance?** *Multiple choice; select all that apply*
- Design phase
- Development phase
- Testing/QA phase
- Post-release/maintenance
- Not currently considered
- Other: specify

(15) **Which practices do you follow to ensure privacy compliance? Select all that apply:** *Multiple choice; select all that apply*
- Internal privacy reviews
- Automated tool analysis
- Manual privacy disclosures
- Use of compliance frameworks (e.g., GDPR, CCPA checklists)
- Data minimization/encryption
- Managing user consent flows
- None
- Other: specify

(16) **How do you assess privacy risks from third-party libraries (TDLs) included in SDK? Select all that apply:** *Multiple choice; select all that apply*
- Manual code review
- Automated privacy/security scanning
- Vendor documentation
- No formal process
- Other: specify

(17) **Which tools or frameworks do you currently use to manage privacy compliance? Select all that apply:** *Multiple choice; select all that apply*
- Custom internal tools
- Platform tools (e.g., Apple Privacy Manifest, Play Console)
- Third-party compliance tools
- None
- Other: specify

(18) **What kind of privacy disclosure does your SDK provide? Select all that apply:** *Multiple choice; select all that apply*
- iOS Privacy Manifest
- iOS Privacy Label Disclosure Guidelines
- Android Data Safety Section Disclosure Guidelines
- Software Bill of Materials (SBOM)
- Privacy Policy
- Terms of Service
- None
- Other: specify

(19) **How effective do you think your current privacy compliance processes are?** *Single choice – Likert scale*
- Not applicable
- Not effective
- Slightly effective
- Moderately effective
- Very effective
- Extremely effective

Challenges

In this section, we want to understand the difficulties and obstacles you face in achieving privacy compliance while developing SDKs.

(20) **What challenges have you encountered with these privacy disclosure requirements? Select all that apply:** *Multiple choice; select all that apply*
- Lack of clarity or examples
- Too much manual work and poor tooling
- Hard to keep up with regulatory compliance updates (e.g., GDPR)
- Difficult to assess third-party behavior
- None
- Other: specify

(21) **How challenging is it to implement privacy compliance features (e.g., consent, data minimization)?** *Single choice – Likert scale*
- Not applicable
- Not challenging
- Slightly challenging
- Moderately challenging
- Very challenging
- Extremely challenging

(22) **How challenging is it to balance compliance with product delivery timelines?** *Single choice – Likert scale*

- Not applicable
- Not challenging
- Slightly challenging
- Moderately challenging
- Very challenging
- Extremely challenging

(23) **How difficult is it to monitor or control third-party data collection in SDK?** *Single choice – Likert scale*
- Not applicable
- Extremely difficult
- Somewhat difficult
- Neither easy nor difficult
- Somewhat easy
- Extremely easy

Needs & Support

In this section, we'd like to learn what resources, tools, or support would help you address privacy compliance challenges more effectively.

(24) **What would help you improve privacy compliance in SDK development? Select all that apply:** *Multiple choice; select all that apply*
- Better documentation and examples
- More automated tools
- SDK-specific policy templates
- Educational resources or training
- Community support
- Other: specify

(25) **How valuable would additional resources (e.g., checklists, automation tools, best practices) be for improving compliance?** *Multiple choice; select all that apply*
- Not applicable
- Not valuable
- Slightly valuable
- Moderately valuable
- Very valuable
- Extremely valuable

(26) **(Optional) What tools or resources would make privacy compliance easier for you as an SDK developer? Please explain in one or two sentences.** *The response is a text entry.*

A.3 Interview Questionnaire

This appendix presents the semi-structured interview guide used in the study. The questions were used to guide the interviews; follow-up questions were asked as needed to clarify or expand upon participants' responses.

(1) **Can you describe your current role and the kind of development work you do?**
(2) **How often do you work with third-party SDKs or open-source libraries in your projects (iOS, Android)?**
(3) **What kind of user data do your applications/SDK typically handle?**
(4) **What does "privacy compliance" mean to you in the context of your development work?**
(5) **How confident do you feel about your understanding of data privacy regulations like GDPR or CCPA?**
- *Probe:* Can you map each legal requirement to its corresponding technical implementation in your code?

(6) **Have you ever been responsible for ensuring that your mobile app complies with privacy laws and regulations? If so, what did that process involve?**
- *In case the answer is "It is other people/team job", Probe:* Do they do a check before or after your SDK development?

(7) **What steps do you typically take to evaluate a third-party SDK before integrating it?**
(8) **Have you ever discovered an SDK collecting data in ways that weren't expected or clearly documented? Can you describe your experience?**
(9) **How often do you encounter SDK documentation that uses vague terms like "may collect or store data"? How do you deal with that uncertainty?**
(10) **Have you ever had to remove or reject an SDK due to privacy or compliance concerns? What led to that decision?**
- *Probe:* How do you choose an SDK for your work? Are there organizational guidelines or an approved whitelist you follow? Do factors such as an SDK's popularity influence your decision?

(11) **How transparent are SDK vendors in your experience when it comes to explaining their data collection practices?**
(12) **Are there any SDK vendors or open-source projects you have worked with that stood out as particularly problematic from a privacy compliance standpoint?**
(13) **What kinds of violations or misleading practices have you seen from SDKs you have used? If there were any violations, how did you deal with them (e.g., documentation, reporting incidents)?**
(14) **What support, tools, or information would help you more effectively manage privacy compliance when integrating SDKs?**
(15) **If you could make one recommendation to SDK vendors to improve privacy compliance specifically for transparency what would it be?**
(16) **What role do you think app stores or platforms like Google Play or Apple should play in enforcing or guiding privacy compliance? In other words, are app privacy labels enough?**
(17) **Have you used any tools, audits, or compliance checkers to assess SDKs or your app's privacy posture? Were they helpful to comply with app stores or platforms or any privacy practices you follow?**
(18) **What would you recommend to other developers trying to navigate SDK privacy compliance challenges?**
(19) **What do you think would be most helpful in minimizing privacy risks from SDKs and improving overall privacy compliance?**
(20) **Are there any other questions or issues that you want to discuss further that we have not touched during the interview?**

A.4 Codebook

Table 1: Codebook

Main Theme	Subtheme	Description	Example	Frequency (n)
Awareness	Privacy Regulation Awareness	Knowledge of GDPR, CCPA/CPRA, COPPA, LGPD, HIPAA and other relevant regulations.	"Even [device IP] can be abused…I don't want to store this kind of data." (P6)	6
	Confidence in Compliance Understanding	Self-assessed ability to interpret and apply privacy regulations.	"I feel reasonably well equipped to meet compliance expectations." (P8)	4
	Data Privacy Risk Awareness	Recognition of privacy risks including data collection from third-party SDKs.	"I always check new SDKs for potential data leaks or over-collection." (P2)	3
Responsibility	Perceived Responsibility	Who is ultimately responsible for privacy compliance in SDK usage.	"Another person within the company…there's a department that's gonna check…I just mainly collect and process the data." (P6)	5
	Shared Responsibility	Cooperation between SDK developers, app developers, legal, and platform teams.	"We follow security rules, but the legal team handles overall compliance." (P5)	4
Practices	Organizational Processes	Company-level frameworks, internal guidelines, and review processes.	"I utilize third-party SDKs following normal company procedures…backend team sets permission levels." (P10)	6
	Technical Safeguards	Implementation of encryption, data minimization, consent flows, and secure coding practices.	"We use encryption in transit…data is collected minimally on the backend." (P1)	5
	Risk Assessment	Manual review, automated scanning, and vendor documentation checks.	"I investigate network calls, review documentation, and contact the SDK provider if necessary." (P2)	7
	Tool Usage	Use of platform tools, internal and third-party compliance tools.	"We use CodeQL to scan every SDK, and GitGuardian to check that no secrets are pushed." (P5)	4
	Transparency & Disclosure	Providing privacy information via manifests, privacy policies, SBOMs, and platform labels.	"Most big, reputable SDK providers are very clear…licensing, documentation, and data collection practices are accurate." (P4)	3
	Lifecycle Integration	Incorporating privacy considerations during design, development, testing, and post-release maintenance.	"Privacy is considered from the design phase through QA and post-release updates." (P9)	3
Challenges	Regulatory Complexity	Difficulty staying up-to-date with evolving laws and regional variations.	"It can be difficult because there are so many things to check…regulations are also becoming more detailed." (P3)	6
	Third-Party Opacity	Limited visibility into data collection and behavior of SDKs/libraries.	"Some use vague language…I feel these practices are somewhat deceptive." (P9)	4
	Product Timelines	Conflicts between compliance work and delivery deadlines.	"Compatibility issues between iOS and Android…weak encryption at times." (P1)	3
	Implementation Difficulty	Technical or procedural challenges implementing privacy features.	"Just sticking with what Apple and Google require is more than sufficient." (P8)	2
	Documentation	Lack of clear guidelines, examples, and templates for SDK-specific compliance.	"I wish there were ready-to-use policy templates for SDKs." (P7)	3
Support & Recommendations	Standardized Frameworks & Clear Documentation	Participants suggested creating ready-to-use compliance frameworks, clear SDK integration guides, and templates for privacy disclosures to save time and reduce errors.	"A standardized compliance framework with built-in checks and clear documentation would save time and reduce risk." (P7)	4
	Automated Compliance Tools	Use of technical tools such as static/dynamic analysis, CI/CD checks, and scanners to detect privacy or licensing issues automatically.	"CodeQL can scan every SDK for licensing issues, and GitGuardian ensures no secrets are pushed to GitHub." (P2)	3
	Real-Time SDK Guidance	Providing real-time guidance and SDK-specific privacy recommendations during development to adhere to evolving regulations.	"Comprehensive readme documentation should have a dedicated privacy section…switches in the SDK APIs to disable data collection." (P7)	3
	Stay Updated with Platform	Emphasis on keeping up with evolving app store rules, OS permissions, and security requirements to prevent non-compliance or data leaks.	"Just stay updated with the current set of security rules…Platforms like Apple and Google App Store can be involved in this process." (P1)	2
	Minimize Data Collection	Collect only essential data, use reputable SDKs, and carefully configure third-party services to prevent unnecessary exposure of sensitive information.	"Collect only what is absolutely needed, and start with minimal data…Use SDKs from reputable companies because they maintain privacy standards." (P7)	3