**Product Satisfaction**

# Participant Information Sheet

# PriBOM - Privacy Bills of Material

## Project overview

This project proposes an approach to pull developers from different roles to the same page to coordinate privacy-related information, addressing the emerging privacy challenges faced by development teams. This project introduces PriBOM, a Privacy BOM that can provide detailed information about data practices, enabling more tailored privacy documentation and more customized and specific privacy notices creation. Our approach supports collaboration between different development roles and ensures all development teams are aligned in the privacy practices for crafting authentic privacy notices.

## What does participation involve?

Participation in this project will involve completing **an online survey that will take approximately 12 minutes**. The survey aims to access the usefulness of PriBOM. We will also collect some basic and un-identifiable demographic information.

## Risks and benefits

**We will not collect any identifiable personal information.** Aside from giving up your time, there are no foreseeable risks associated with participating in this project. **Participating in the survey will receive monetary rewards.** Your participation will also significantly help us on evaluating the proposed approach.

## Withdrawal from the research project

If you wish to withdraw, simply leave the survey page. You may withdraw from this project at any time up until publication of the final outputs.

## Confidentiality

**All information provided by you will be treated confidentially.** All data collected in this project will be reported in such a way that responses will not be able to be linked to any individuals. Any data collected as part of this project will be securely stored.

## How will my information be used?

It is anticipated that the data obtained through the survey will be published and presented in a variety of forums. This includes the production of scientific publication. De-identified data collected through the survey may also be used in future research.

**Thank you for taking the time to help with this research project. Please continue if you would like to participate.**

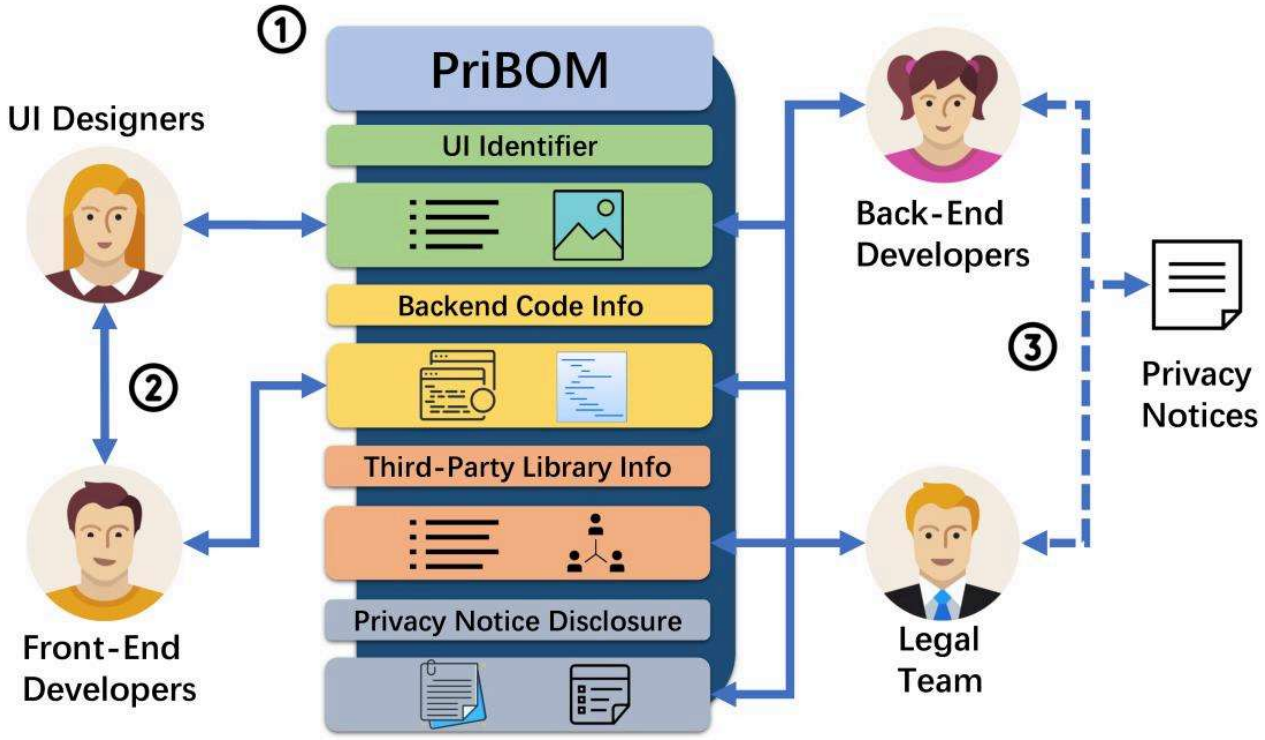
Welcome to our survey on PriBOM (Privacy Bills of Material)!

Why do we need PriBOM?

Application developers are facing severe privacy challenges to ensure that their software products comply with privacy standards and can provide comprehensive privacy notices to describe their privacy-related data practices, especially when such privacy concerns relate to user interface (UI) components of mobile applications.

What is PriBOM?

In response to the privacy challenges, we propose PriBOM to align developers from different roles on the same page for managing privacy-related information. PriBOM is inspired by the concept of the Software Bills of Material (SBOM) from the software engineering field. **It aims to bring together roles like UI designers, backend developers, and legal teams to coordinate privacy information at the widget level, addressing the emerging privacy challenges faced by developers today**.




● Privacy Information Inventory: PriBOM acts as a comprehensive inventory for UI widgets, encapsulating a detailed record of data handling practices including API usage, data types, permissions, and information in the privacy notices. This enhances the traceability in the "privacy chain," connecting front-end UI, backend privacy behavior, and the product's privacy policy.

● Privacy-Related Communication between Developers: PriBOM facilitates communication across different developer roles, helping to bridge knowledge gaps and promote a unified understanding of privacy implications, leading to more informed decision-making and cohesive development strategies.

● Collaboration with the Legal Team: PriBOM can help legal team conduct effective privacy compliance checks and facilitate developers in quickly responding to new requirements when a potential risk is raised by the legal experts.

**Data Field of PriBOM (Page 2/10)**

We present the design of PriBOM here, which includes four sections: UI Widget Identifier, Codebase and Permission, Third-Party Library and Privacy Notice Disclosure.

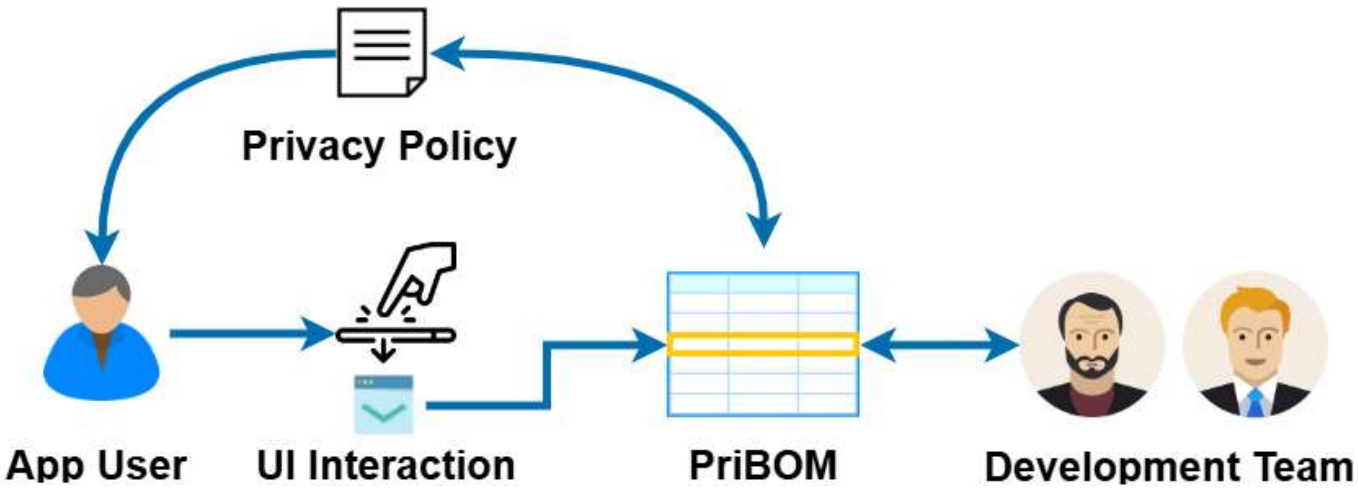
| UI Widget Identifier | |
|---|---|
| Data Field | Description |
| | |

| | |
|---|---|
| Widget Type | Component type of the widget. |
| Widget ID | A unique identifier for each UI widget component in the app. |
| Widget Name | Names given manually for widgets to better recognize them. |
| Widget Src | Reference to source files, e.g. JPG or PNG images. |
| **Codebase and Permission** | |
| **Data Field** | **Description** |
| Event | Specific events that the widget reacts to. |
| Handler | The function or method that handles the event. |
| Android API Level | The minimum Android API level required by the widget. |
| Permission | The Android permissions required by the widget. |
| Data Type | The types of data the widget collects or processes. |
| Method (permissions) Path/Location | The path that accesses to the file requesting the permissions. |
| **Third-Party Library** | |
| **Data Field** | **Description** |
| TPL Name | The package name of third-party libraries involved in the widget. |
| TPL Version | The version of third-party libraries involved in the widget. |
| Latest TPL Version | The most recent version of third-party libraries available. |
| TPL Publish Date (current version) | The release date of the current TPL version. |
| TPL Publish Date (latest version) | The release date of the latest TPL version. |
| **Privacy Notice Disclosure** | |
| **Data Field** | **Description** |
| Privacy Policy Description | Corresponding sections in the privacy policy related to widget's data practices. |
| Privacy Label Declaration | Disclosure of privacy practices on related data type in privacy label section. |

### An overview of PriBOM

The interaction between app users and UI components triggers data practices. These practices are disclosed to users through privacy notices such as the privacy policy.

PriBOM helps the development team create more accurate privacy notices by documenting privacy information related to this UI component.




**Demographics (Page 3/10)**

**We'd like to know more about your experiences with the software development:**

Q1. What is your role in development team/company?

- ○ Junior developer
- ○ Senior developer
- ○ Project manager
- ○ UI designer
- ○ Legal team
- ○ [ ] Other

Q2. What is your Year of experience in software development?

- ○ <1 year
- ○ 1-3 years
- ○ 3-5 years
- ○ 5-10 years
- ○ >10 years

Q3. What is the size of your project team?

- ○ <10 people
- ○ 10-20 people
- ○ 20-50 people
- ○ >50 people

## General Design of the PriBOM (Page 4/10)

PriBOM includes data fields in four sections: UI Widget Identifier, Codebase and Permission, Third-Party Library and Privacy Notice Disclosure.

### Q4. General Design of the PriBOM

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Intuitiveness]** The PriBOM's data fields are logical and promotes ease of understanding. | ○ | ○ | ○ | ○ | ○ |
| **[Format]** The layout and format of the PriBOM are intuitive for developers with varying levels of experience. | ○ | ○ | ○ | ○ | ○ |
| **[Relevance]** Information in the PriBOM is essential and contributes to privacy management. | ○ | ○ | ○ | ○ | ○ |

## Design of the Widget Identifier Section of the PriBOM (Page 5/10)

PriBOM includes UI identifier information to achieve sufficient identification of the UI

widgets.

| UI Widget Identifier | |
|---|---|
| **Data Field** | **Description** |
| Widget Type | Component type of the widget. |
| Widget ID | A unique identifier for each UI widget component in the app. |
| Widget Name | Names given manually for widgets to better recognize them. |
| Widget Src | Reference to source files, e.g. JPG or PNG images. |

**Q5. Design of the Widget Identifier Section of the PriBOM**

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Identification Precision]** PriBOM's design for widget identification is precise enough to pinpoint privacy issues to a specific UI component. | ○ | ○ | ○ | ○ | ○ |
| **[Clarity]** The widget name and type in the PriBOM is helpful in providing clear and common terminology for team members. | ○ | ○ | ○ | ○ | ○ |

**Design of the Codebase and Permission Section of the PriBOM (Page 6/10)**

This section of PriBOM focuses on the intricate relationship between the UI widgets and the codebase specifics.

| Codebase and Permission | |
|---|---|
| **Data Field** | **Description** |
| Event | Specific events that the widget reacts to. |
| Handler | The function or method that handles the event. |
| Android API Level | The minimum Android API level required by the widget. |

| | |
|---|---|
| Permission | The Android permissions required by the widget. |
| Data Type | The types of data the widget collects or processes. |
| Method (permissions) Path/Location | The path that accesses to the file requesting the permissions. |

### Q6. Design of the Codebase and Permission Section of the PriBOM

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Codebase Accessibility]** The path/location fields in PriBOM intended for codebase access promote better manageability. | ○ | ○ | ○ | ○ | ○ |
| **[Event & Handler]** The 'Event' and 'Handler' data field in PriBOM aid in tracing data flows in response to user events. | ○ | ○ | ○ | ○ | ○ |
| **[Permission]** Listing 'Permission' in PriBOM is crucial for transparent disclosure of data access needs and permission requests. | ○ | ○ | ○ | ○ | ○ |
| **[Data Type]** Including data types and associated permissions in PriBOM is instrumental for providing privacy information. | ○ | ○ | ○ | ○ | ○ |
| **[API-Level Awareness]** The inclusion of specific Android API levels in PriBOM is relevant and necessary for privacy documentation. | ○ | ○ | ○ | ○ | ○ |

How would implementing PriBOM in your projects impact the management and documentation of permission request and data collection? Please briefly describe any potential advantages or challenges.

### Design of the Third-Party Library Section of the PriBOM (Page 8/10)

This section in PriBOM is dedicated to managing and documenting the use of Third-Party Libraries (TPLs).

| **Third-Party Library** | |
|---|---|
| **Data Field** | **Description** |
| TPL Name | The package name of third-party libraries involved in the widget. |
| TPL Version | The version of third-party libraries involved in the widget. |
| Latest TPL Version | The most recent version of third-party libraries available. |
| TPL Publish Date (current version) | The release date of the current TPL version. |
| TPL Publish Date (latest version) | The release date of the latest TPL version. |

### Q7. Design of the TPL Section of the PriBOM

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Management]** PriBOM's inclusion of third-party library information is crucial for a comprehensive privacy review. | ○ | ○ | ○ | ○ | ○ |
| **[Discrepancy]** Documenting TPL versions may help identify discrepancies of privacy practices | ○ | ○ | ○ | ○ | ○ |

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| between different versions. | | | | | |
| **[Record]** The date fields of version date in PriBOM would help in maintaining a record of privacy-related updates. | ○ | ○ | ○ | ○ | ○ |
| **[Update Awareness]** The data fields of version date in PriBOM would help developers aware of the TPL updates about privacy practices. | ○ | ○ | ○ | ○ | ○ |

Reflecting on your previous projects, how would detailed tracking of Third-Party Libraries (TPLs) as proposed by PriBOM facilitate to manage privacy compliance?

**Design of the Privacy Notice Disclosure Section of the PriBOM (Page 7/10)**

For the two common forms of privacy notices, e.g., privacy policies and privacy labels, PriBOM links widget components directly to their respective disclosures in the privacy notices.

| **Privacy Notice Disclosure** | |
|---|---|
| **Data Field** | **Description** |
| Privacy Policy Description | Corresponding sections in the privacy policy related to the widget's data practices. |
| Privacy Label Declaration | Disclosure of privacy practices on related data type in privacy label section. |

**Q8. Design of the Privacy Notice Disclosure Section of the PriBOM**

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Alignment]** The Privacy notice fields in PriBOM adequately guides the incremental development of accurate privacy notices. | ○ | ○ | ○ | ○ | ○ |
| **[Traceability]** This section in PriBOM can help trace data practices to relevant descriptions in privacy policy. | ○ | ○ | ○ | ○ | ○ |
| **[Trackability]** This section in PriBOM can facilitate tracking from disclosures in privacy policy to related data practices in code. | ○ | ○ | ○ | ○ | ○ |

What potential benefits do you see in the PriBOM method of documenting data practices and their associated disclosures in the privacy notice?

## Usability and Practicality of the PriBOM (Page 9/10)

### Q9. Usability and Practicality of the PriBOM

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Communication]** The PriBOM is a practical solution for efficient privacy-related communication between different roles in development team. | ○ | ○ | ○ | ○ | ○ |
| **[Privacy Notice Generation]** The PriBOM can streamline | ○ | ○ | ○ | ○ | ○ |

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| privacy notice generation and management for development teams. | | | | | |
| **[Disclosure-Behaviour Alignment]** The PriBOM would make it easier to align privacy notice pieces with app's actual software behaviours. | ○ | ○ | ○ | ○ | ○ |
| **[Transparency Promotion]** The PriBOM can enhance the transparency about data handling within development teams. | ○ | ○ | ○ | ○ | ○ |
| **[Privacy Awareness]** Implementing the PriBOM could lead to improved privacy awareness among the development team members. | ○ | ○ | ○ | ○ | ○ |
| **[Risks Mitigation]** The PriBOM could systematically reduce the risks of overlooking privacy concerns during the development process. | ○ | ○ | ○ | ○ | ○ |
| **[Scalability]** The PriBOM is a scalable solution that could be adapted for different project sizes and complexities. | ○ | ○ | ○ | ○ | ○ |
| **[Consent Identification]** The PriBOM effectively aids in identifying user-consent-required data collection practices. | ○ | ○ | ○ | ○ | ○ |

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **[Inquiry Response]** PriBOM could reduce the effort needed to respond to privacy-related inquiries from users. | ○ | ○ | ○ | ○ | ○ |

Reflecting on your own experiences, how do you think implementing PriBOM in the development team might influence the collaboration between different roles toward privacy notice (e.g., privacy policy) management and generation?

**You have completed all questions!**

**Please continue to submit your response and finish the survey.**