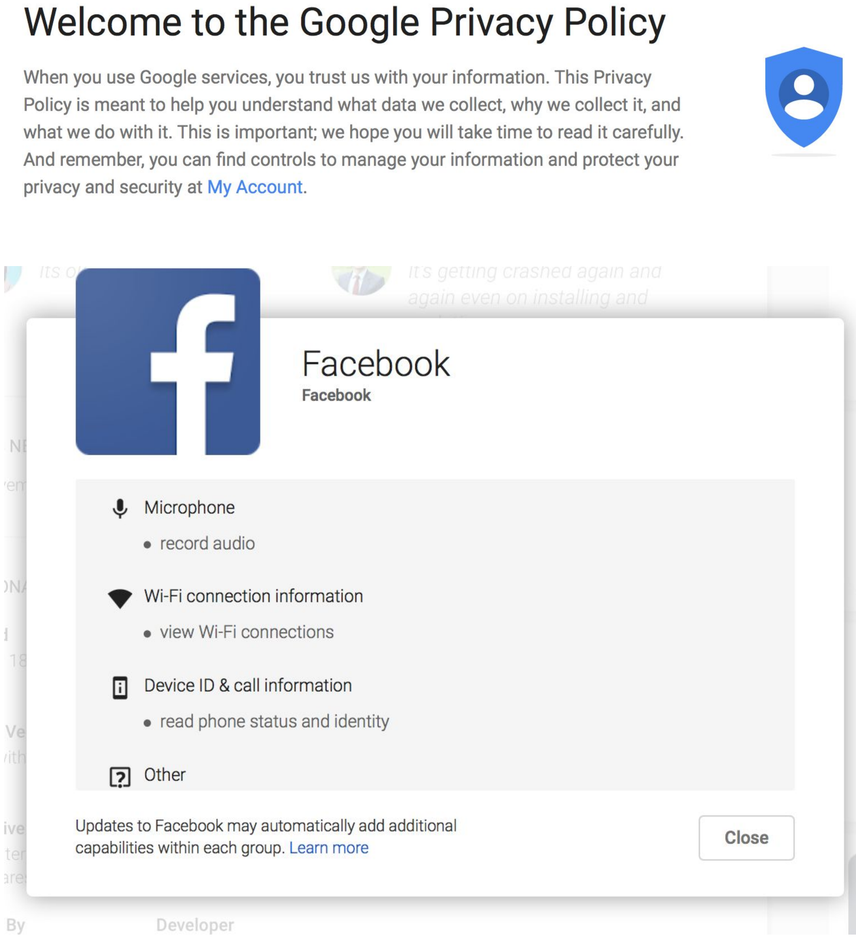
Helping Android Developers Write Privacy-preserving Apps

Tianshi Li, Matt Fredrikson, Yuvraj Agarwal, Jason Hong

Making privacy-preserving apps is nontrivial

- The legitimacy of personal data collection is highly dependent on the context and purpose. There could be a trade-off between privacy and usability.
- The data practices are mostly opaque to users.



- Privacy policy - lengthy, legal language, and separate from the app
- Android permission - too general (Does Facebook eavesdrop on me to customize their ads?)

What challenges do developers face?

- We interviewed 10 Android developers (including student and professional developers) to understand the challenges that hinder them from making privacy-preserving apps. We identified four types of challenges from the interview results:

1. Developers may not be aware of the recommended practices
2. Developers may need external reminders to conform to good privacy practices
3. Developers may be unwilling to follow some privacy guidelines they don't agree with or contradict other goals
4. Developers may not have clear understanding of their apps' data practices due to app iterations and collaborating with other developers without enough documentation

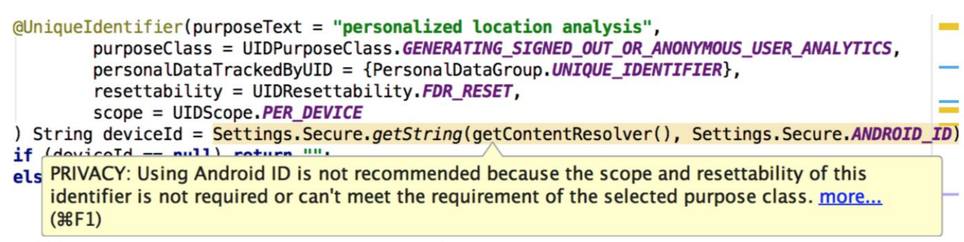
Limited developer support for privacy are available

- Documentation and tutorials for privacy
- Privacy policy generators
- IDE plugins for secure programming
- Taint analysis

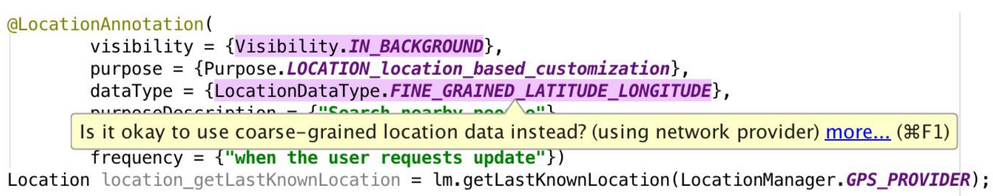
Our approach: An IDE plugin that helps developers write privacy-preserving code

```
@LocationAnnotation(
        visibility = {Visibility.IN_BACKGROUND},
        purpose = {Purpose.LOCATION_location_based_customization},
        dataType = {LocationDataType.FINE_GRAINED_LATITUDE_LONGITUDE},
        purposeDescription = {"Search nearby people"},
        retentionTime = {"during the session"},
        frequency = {"when the user requests update"})
Location location_getLastKnownLocation = lm.getLastKnownLocation(LocationManager.GPS_PROVIDER);
```

- The IDE plugin can detect an API call that accesses personal data. Then it requires the developer to complete an annotation (@LocationAnnotation), including the purposes of using the data and other important properties



- Given the purpose provided by the developer, the plugin suggests a better option of unique identifier to use based on the best practices guidelines from Google



- The plugin will also remind developers of potential sensitive data practices and suggest alternative options.