The paper discusses two main methods that apps use to circumvent app permissions to gain access to sensitive and private information. The first method, a covert attack, relies on obtaining the sensitive information from another app that does have access to the information. The other method is a side attack which gains access to the information be circumventing the permissions for the data, such as the geolocation data in the EXIF metadata of photos. Even though there are laws and policies to try and protect users from this kind of abuse, it's clear that this preventative measure isn't enough to protect users. The method described in the paper, using a mix of static and dynamic analysis with automated and randomized UI Fuzzing, doesn't guarantee that it finds all the intrusions by apps. It seems like the first step would be designing a standard system that apps have to pass to gain the authentication from the app store. By designing a full proof method that is enforced by the provider of the app (Google Play Store, iTunes, Windows Store, Steam, etc) would provide the foundation for protection since it seems that system is currently in place besides the permissions settings built into Android's OS. The other fault that is allowed in the current system is that apps can request permission for services that they don't need. Since the policy gives the least permissions possible, it actually enforce this like intended, if the app doesn't use the permissions in the app, then they should not be allowed to ask for permission. This seems like something that could be done in a preanalysis of the app. It also seems like the other problem, though only briefly mentioned in the paper, is user understanding of what permission give the apps. The user may not understand what type of information they are giving up (such as the geolocation data locationed in photos' EXIF metadata). When the user is uninformed, they may grant permission that they didn't intend to. A possible solution to this is a contractual agreement that states what the app is using the data for on the screen where the permission is granted. This would make sure that users are informed about exactly what the app is using the permissions for. This would also hold developers responsible to stick to the guidelines specified. There is then a clear line that would say whether an app had unjustly used the permissions. As mentioned in the paper, the problem needs to be tended by the user, developer, and provider to have a long and lasting effect and stronger and enforced regulations might be the only way to make all parties conform.