Analyzing the Role of General App Creators in Protecting the Privacy of Vulnerable Populations

Tianshi Li
Human-Computer Interaction Institute, Carnegie Mellon University
5000 Forbes Ave, Pittsburgh PA
tianshil@cs.cmu.edu

Jason I. Hong
Human-Computer Interaction Institute, Carnegie Mellon University
5000 Forbes Ave, Pittsburgh PA
jasonh@cs.cmu.edu

Abstract
Privacy has become a growing concern in our society, especially for certain populations that are either less capable of protecting their privacy (e.g., children) or more vulnerable to privacy attacks (e.g., undocumented immigrants). Prior work often attempts to provide specific strategies for vulnerable populations to cope with those issues. In this position paper, we focus on how to help app creators (e.g., programmers, UX designers) better consider how their apps can be made inherently safer for vulnerable users. We analyze the opportunities and challenges of engaging app creators as a complementary force to other coping strategies, and call for more innovations in all stages of app development by proposing two high-level suggestions for research on this topic: 1) Integrating relevant requirements and nudges into their normal workflow; and 2) Designing a proper division of labor between app creators and the rest of the ecosystem.

Author Keywords
Privacy; vulnerable populations; usable privacy; software engineering; developer tools; privacy by design.

CCS Concepts
- Security and privacy → Usability in security and privacy;
Introduction
Nowadays, digital technologies have been deeply woven into our daily lives in various forms, such as mobile apps, web apps, desktop apps, and IoT apps. However, some users of these apps may be especially vulnerable to privacy risks. For example, some may be incapable of protecting their data, such as children [3, 24, 2] and elderly people [12]. Others may have more sensitive data, such as victims of domestic violence [9] and human-trafficking [4], undocumented immigrants [11], and LGBTQ people [19].

Prior research has provided in-depth characterization of privacy risks faced by different vulnerable populations and proposed corresponding solutions, including building protective tools [15, 9, 24], advocating for better regulations and policies [2, 3], and providing training and resources of best practices in privacy protection for these populations [3]. Although contributing important insights for each problem, prior work often focuses on highly specialized solutions.

Conversely, we argue that it is also important to study how to help general app creators build apps that are inherently safer for vulnerable users, because research suggests that off-the-shelf apps (e.g., websites, mobile apps, IoT apps) may constitute a major source of privacy attacks on vulnerable populations. For example, malicious users may abuse the location sharing feature to convert a benign app to a spying machine [9], harass the victims on social media and communication apps [15], and acquire sensitive information about a person via publicly downloadable data records [4].

The rest of the paper contains three parts. First, we try to draw some common characteristics of vulnerable populations that account for certain privacy problems. Then we explain the necessity and potential benefits of incorporating the power of app creators to address the identified problems. Finally, we call for more innovations in all stages of the app development life cycle, and propose two high-level suggestions for conducting research on this topic: 1) Integrating relevant requirements and nudges into app creators’ normal workflow; 2) Designing a proper division of labor between app creators and the rest of the ecosystem.

Characteristics that Account for Vulnerability
In this section, we highlight why protecting privacy is particularly challenging for certain populations.

Low technical literacy
A recurring problem about vulnerable populations is low technical literacy [3, 11, 9]. Being less technical-savvy means they may be less aware of data being shared when using digital services, especially when the app collects data in the background. Moreover, although these users care about privacy, they lack the ability to estimate risks and to protect themselves from potential risks [11].

Low socioeconomic status
Some people are in a low socioeconomic status, which potentially make them value other factors more than privacy and make decisions that sacrifice privacy in exchange for the benefits of technology (e.g., free services supported by targeted ads based on users’ location data). Therefore, it may also hinder their ability of managing privacy risks.

Under extreme conditions
Data that may be innocuous under normal circumstances for the vast majority of the population, may become highly risky in extreme circumstances. For example, mobile apps that collect location data, and smart speakers that collect audio logs (e.g. Alexa logs [20, 13]) which can be used to infer whether the user is at home and what are their activities, can be extremely sensitive to people such as undocumented immigrants and survivors of human-trafficking.
How to Build Safer Apps for Vulnerable Users

In the following, we introduce several ways in which general app creators (e.g., programmers, UX designers) may improve the safety of their apps for vulnerable populations.

Apply inclusive design for privacy in app design

Recent research has started looking at novel design methodologies that can help designers to reflect on privacy-related values early in product development [25]. We argue that designers should also actively reflect on privacy for marginalized populations, following the same spirit as inclusive design methods [5]. As suggested by prior research, inclusive design may not only help app creators foresee problematic privacy practices for edge users, but also improve privacy for general users. We hope there could be formal guidelines and better tools to remind and help designers apply inclusive design to protect privacy for vulnerable populations.

Comply with privacy laws and best practices

Current privacy regulations and policies already require general app creators to take some actions to protect certain vulnerable populations. For example, the Children’s Online Privacy Protection Act (COPPA) is a US federal law that requires apps to obtain parental consent before collecting personal information of users under the age of 13. Additionally, many takeaways from research on vulnerable populations are in line with the best practices of privacy and security for general populations [9], such as minimum data collection and proper authentication [7, 6].

However, due to developers’ low awareness of the regulations and best practices [14], and the difficulty in converting the high-level principles into concrete engineering requirements, we need to provide them with more support. For example, tools that provide just-in-time suggestions when programmers write relevant code or read relevant posts could help raise their awareness of these principles and allow for timely reflection on their design decisions.

Identify risks of abusive use

A benign app can be used for malicious purposes [9], which requires prompt detection and handling of abusive use. Instead of solely identifying these problematic apps in an ad-hoc way, we envision that app stores can require app creators to provide detailed data practice descriptions to automatically identify more apps with similar risks. For example (Figure 1), when researchers have learned that the “Find My” app can be abused, they can look up for other apps that have the same data use “accurate location being shared constantly with another user” (e.g. Google Maps).

Provide personalized privacy notices

To make the privacy risks and protective methods more clear to vulnerable users, apps should provide privacy notices in various forms [18] that are more comprehensive, upfront, and proactive than the coarse-grained permission requests [23] and lengthy privacy policies [16]. Ideally, privacy notices should be personalized to tailor to different populations’ needs. For example, for users with lower technical literacy, the use of jargon should be avoided; for users under extreme conditions, the app should provide warnings about features susceptible to abusive use (e.g. the real-time location sharing feature in Figure 1), and even proactively remind them to turn off the features.

How to Better Leverage App Creators’ Power

Despite the potential benefits, there are still challenges in how to make app creators act in the ways suggested above. Based on prior work that help app creators improve privacy [21, 22, 10, 1] and our experience in building developer tools for privacy [14], we propose the following two suggestions in designing practical and systematic solutions to this problem.
Integrating requirements and nudges into the normal workflow

Privacy laws and app store policies have a big impact on app creators. Some of them have already taken certain vulnerable populations into account (e.g., COPPA). However, these policies tend to be high level, abstract, and hard to interpret, and app creators are largely unaware of them [14].

We argue that there are many exciting research opportunities in designing tools that embed contextual suggestions in the normal workflow. The suggestions may consist of hard requirements for complying with laws, as well as soft nudges to increase app creators’ awareness of best practices. For example, when the programming environment detects the collection of age information, it can immediately remind developers that they need to comply with COPPA and obtain parental consent before collecting data of users under 13 (requirements); they may also want to design privacy features that facilitate teenagers [24] and elderly people [12] to manage their privacy (nudges). The nudges need to be carefully designed to avoid fatigue issues.

Using a hybrid of distributed and centralized approaches

Despite the benefits of keeping app creators in the loop, it is not realistic or ideal to fully rely on them. Although “identifying abusive use” and “providing personalized privacy notices” can offer considerable benefits to the affected users, they are edge cases to app creators, who may not consider the extra design and implementation work to be worthwhile.

Therefore, we argue that a promising solution could be to design a proper division of labor between app creators and the rest of the ecosystem, which can potentially allow app creators to do less work when improving privacy. For example, developers may only need to disclose privacy practices that are hard to analyze (e.g., data sharing on the server end, purposes for collecting data) in a certain format (e.g., via privacy annotations [14]; see Figure 2), and let the operating system generate personalized warnings (e.g., “Your real-time location has been shared with other registered users of the app since ...”) based on user-configured alarm levels. This idea may also benefit other entities. For example, policymakers could require app creators to provide an enhanced version of “privacy policy” that is linked to the actual implementation. This may help with privacy auditing and law enforcement.

With the above analysis, we hope to demonstrate the research opportunities in helping app creators improve privacy. Existing work has touched upon methods to help designers [25] and developers [14, 8, 17]. We also hope to see work on other roles (e.g., lawyers), and how different roles collaborate. In addition, we hope more privacy research for vulnerable populations can offer concrete design recommendations for app creators, which could be important resources for studying interventions on app creators.

Conclusion

In this position paper, we discuss the important role app creators play in building safer apps for vulnerable users. With the two suggestions proposed at the end, we hope to open up the discussion on how privacy researchers specialized in different areas can collaborate to better support app creators to fulfill their responsibilities.
ACM Copyrights & Permission Policy
Accepted extended abstracts and papers will be distributed in the Conference Publications. They will also be placed in the ACM Digital Library, where they will remain accessible to thousands of researchers and practitioners worldwide. To view the ACM's copyright and permissions policy, see: http://www.acm.org/publications/policies/copyright_policy.

REFERENCES


