The 'privacy by design' approach for mobile apps: Why it's not enough

27 July 2021, by Dusty-Lee Donnelly

Credit: CC0 Public Domain

The mobile apps installed on our smartphones are one of the biggest threats to our digital privacy. They are capable of collecting vast amounts of personal data, often highly sensitive.

The consent model on which privacy laws are based doesn't work. App users remain concerned about privacy, as a recent survey shows, but they still aren't very good at protecting it. They may lack the technical know-how or the time to review privacy terms, or they may lack the willpower to resist the lure of trending apps and personalized in-app offers.

As a result privacy laws have become more detailed, imposing additional requirements about notice, data minimisation, and user rights. Penalties have become harsher. And the laws are often global in reach, such as the US Children's Online Privacy Protection Rule and the EU's General Data Protection Regulation. For instance, a South African developer of an app downloaded by children in the US and the EU must comply with both and with South Africa's Protection of Personal Information Act. This complexity can create a significant compliance burden.

But the real problem, according to a report by the EU Agency for Cybersecurity, is that lawyers and app developers don't speak the same language. An app developer may have no idea how to translate abstract legal principles into concrete engineering steps.

As a result regulators have looked to the concept of "privacy by design" as a way to bridge this divide. The concept was coined in the late 1990s by Ann Cavoukian when she was the Information and Privacy Commissioner for Ontario, Canada. Privacy by design goes beyond privacy policies and in-app permission settings. It requires developers to think about privacy from the first moment of the design process.

Cavoukian set out seven foundational principles for a privacy by design approach. But it is the second principle, "privacy as a default setting," that really sets the bar for a privacy-friendly app.

"Build in the maximum degree of privacy into the default settings for any system or business practice. Doing so will keep a user's privacy intact, even if they choose to do nothing."

This places the responsibility on the app developer to think about the user's privacy upfront, and design the app in such a way that privacy is protected automatically, while still offering a fully functional app experience.

But my research showed that design decisions made by app developers are constrained by existing technologies and platform rules designed by others. These include the device hardware and operating system, the software development kit, ad libraries and app store review policies.

The answer is privacy by (re)design, where all roleplayers in the ecosystem take privacy seriously

and redesign existing platforms and technologies. But enforcing that approach will require tighter legal regulation of third party data sharing.

Change of mindset

Applying a privacy by design approach requires a change of mindset by developers. They must be proactive, rather than responding after the fact to a data breach that could have been prevented. The days of collecting as much personal data as possible in the hope that it might prove valuable later are gone. Developers must align data collection to a specific purpose for which the data is needed and communicate that to app users. They should also anonymise or delete the data as soon as possible.

Privacy should become a key component of design methodology, selection of technical tools, and organizational value statements.

These are important changes, endorsed in guidelines for mobile app developers published by the Global System for Mobile Communications and by regulators in the US, the UK, Australia and Canada, among others. In the EU "data protection by design and by default" is now a legal obligation of the General Data Protection Regulation.

But, as my research shows, this might not be enough without the redesign of the app ecosystem to address data sharing, a view supported by other research. According to one study most apps transmit data directly to third parties, like Google, Facebook and ad exchanges, via trackers embedded in the app code. But I found that privacy laws do not comprehensively or consistently address this third party sharing.

The term "third party" is not defined in the Protection of Personal Information Act, but would include ad networks, content-sharing sites and social networking platforms. Third parties are thus distinguished from downstream processors who may perform specified data processing on your behalf under a contract.

It is difficult to enforce legal liability against these third parties, who are often outside the country where the app was developed. Their terms and conditions typically place full responsibility for privacy compliance by the app on the app developer. This may leave app users unprotected. But it could also expose the app developer to unforeseen legal liability.

Liability for the app developer arises because under both the Protection of Personal Information Act and General Data Protection Regulation if you played a role in determining "the purpose or means" of data processing you are a "joint" responsible party (data controller) for the data processed by the third party.

The European Court of Justice has twice held small businesses liable as "joint controllers" for Facebook's collection of data, via a fan page and a like button. Although the judgments stress that joint control is not necessarily "equal liability," this should still be a concern for app developers.

For example, app developers using the Facebook Software Development Kit are sharing personal data with Facebook. Event logs such as "app installed," "SDK initialized" and "app deactivated" give detailed demographic and behavioral insights about an app user. In 2018 Privacy International reported that the setting to delay transmission of logged events until after the user has consented was only added by Facebook 35 days after General Data Protection Regulation came into force, and then only if enabled by the developer for SDK version 4.34 or higher. This change appears to have followed repeated bug reports filed on the developer's platform.

Takeaways

The takeaway here for developers following a privacy by design approach is to "trust but verify":

- Check contract terms and third party code carefully;
- Monitor developer platforms for security and privacy updates;
- Only work with organizations that offer adequate privacy guarantees;
- Notify your users about data transfers to third parties and provide easy to use privacy

controls.

- Keep logs so that you can respond promptly if an app user requests details of the personal data you hold and the recipients (or categories of recipients) of that data.

Prosecuting app developers who breach data laws is important but not enough. Ultimately the parties who design the technologies and platforms on which mobile apps are built and marketed must be brought within the legal accountability framework to close the privacy loop.

Provided by The Conversation
APA citation: The 'privacy by design' approach for mobile apps: Why it's not enough (2021, July 27) retrieved 23 October 2021 from https://techxplore.com/news/2021-07-privacy-approach-mobile-apps.html