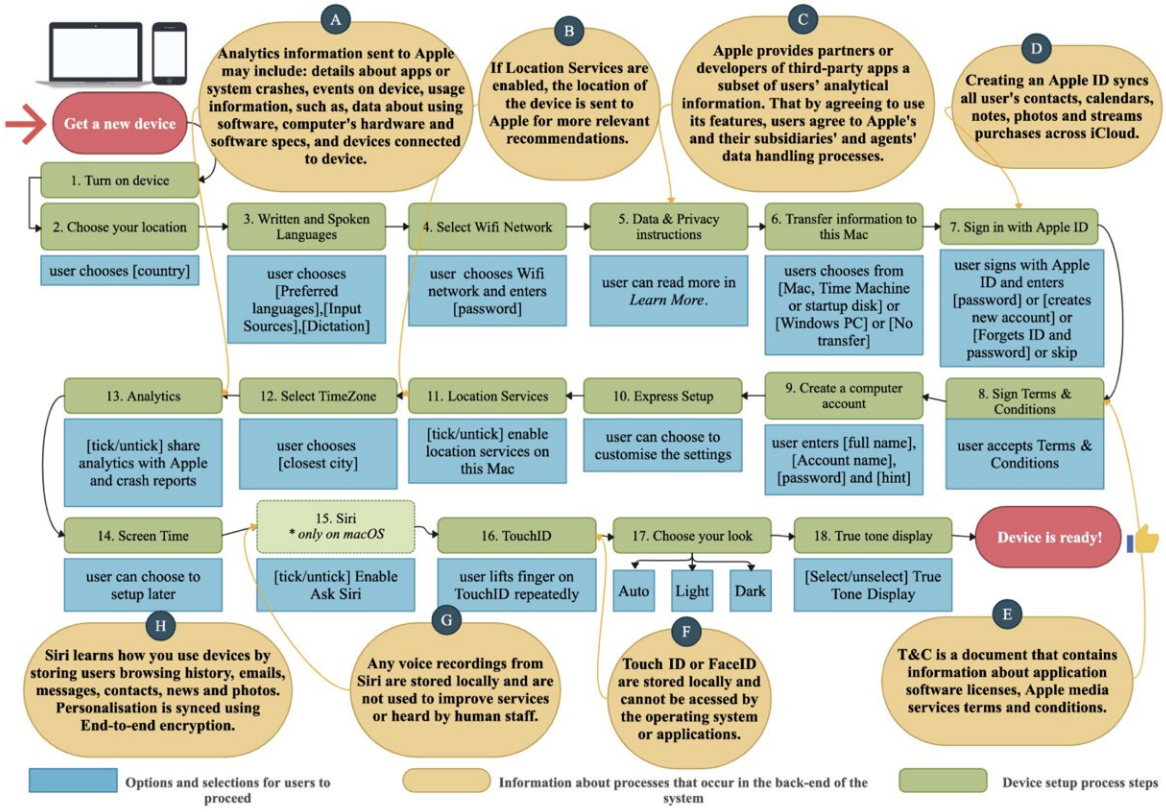
Keeping your data from Apple is harder than expected, finds study

April 3 2024



The contrast between the steps users experience and the data handling processes involved at various stages of the device setup process. The user begins the process of setting up their device by purchasing a new device. Steps 1 - 18 explain the steps required for a complete setup of a user's device, for instance, a MacBook (macOS 10.15+). Yellow bubbles denoted by letters A - H are summaries of Apple's official privacy policy statement [3]. Bubbles A - H highlight examples of personal information collection occurring at various stages of the setup process. In addition to other data handling procedures, such as the

location of the information stored (e.g., in F), users' fingerprints are stored locally on the device. We note that there may be slight variations between the order of the presentations of these settings in iOS and macOS. Additionally, Siri (step 15) is not prompted during device setup in iPhone (iOS 14.0) The order of the diagram is based on the order of presentation of the settings on macOS. Credit: *Privacy of Default Apps in Apple's Mobile Ecosystem* (2024)

"Privacy. That's iPhone," the slogan proclaims. New research from Aalto University begs to differ.

Study after study has shown how voluntary third-party apps erode people's privacy. Now, for the first time, researchers at Aalto University have investigated the privacy settings of Apple's default apps, the ones that are pretty much unavoidable on a new device, be it a computer, tablet, or mobile phone.

The researchers will present their findings in mid-May at the CHI conference, and the peer-reviewed research paper is already available online.

"We focused on apps that are an integral part of the platform and ecosystem. These apps are glued to the platform, and getting rid of them is virtually impossible," says Associate Professor Janne Lindqvist, head of the computer science department at Aalto.

The researchers studied eight apps: Safari, Siri, Family Sharing, iMessage, FaceTime, Location Services, Find My and Touch ID. They collected all publicly available privacy-related information on these apps, from technical documentation to privacy policies and user manuals.

The fragility of the privacy protections surprised even the researchers.

"Due to the way the user interface is designed, users don't know what is going on. For example, the user is given the option to enable or not enable Siri, Apple's virtual assistant. But enabling only refers to whether you use Siri's voice control. Siri collects data in the background from other apps you use, regardless of your choice, unless you understand how to go into the settings and specifically change that," says Lindqvist.

Participants weren't able to stop data sharing in any of the apps

In practice, protecting privacy on an Apple device requires persistent and expert clicking on each app individually. Apple's help falls short.

"The online instructions for restricting data access are very complex and confusing, and the steps required are scattered in different places. There's no clear direction on whether to go to the app settings, the central settings—or even both," says Amel Bourdoucen, a doctoral researcher at Aalto.

In addition, the instructions didn't list all the necessary steps or explain how collected data is processed.

The researchers also demonstrated these problems experimentally. They interviewed users and asked them to try changing the settings.

"It turned out that the participants weren't able to prevent any of the apps from sharing their data with other applications or the service provider," Bourdoucen says.

Finding and adjusting privacy settings also took a lot of time. "When making adjustments, users don't get feedback on whether they've succeeded. They then get lost along the way, go backwards in the process

and scroll randomly, not knowing if they've done enough," Bourdoucen says.

In the end, Bourdoucen explains, the participants were able to take one or two steps in the right direction, but none succeeded in following the whole procedure to protect their privacy.

Running out of options

If preventing data sharing is difficult, what does Apple do with all that data?

It's not possible to be sure based on public documents, but Lindqvist says it's possible to conclude that the data will be used to train the artificial intelligence system behind Siri and to provide personalized user experiences, among other things.

Many users are used to seamless multi-device interaction, which makes it difficult to move back to a time of more limited data sharing. However, Apple could inform users much more clearly than it does today, says Lindqvist. The study lists a number of detailed suggestions to clarify privacy settings and improve guidelines.

For individual apps, Lindqvist says that the problem can be solved to some extent by opting for a third-party service. For example, some participants in the study had switched from Safari to Firefox.

Lindqvist can't comment directly on how Google's Android works in similar respects, as no one has yet done a similar mapping of its apps. But past research on third-party apps does not suggest that Google is any more privacy-conscious than Apple.

So what can be learned from all this—are users ultimately facing an

almost impossible task?

"Unfortunately, that's one lesson," says Lindqvist.

More information: Paper: Privacy of Default Apps in Apple's Mobile Ecosystem

Provided by Aalto University