An Analysis of iOS App Permissions

Mobile apps need data to function. That's why app developers ask for varying levels of access to the information on your mobile device. Usually, it's to improve functionality, but occasionally it lacks proper justification.

App developers may request excessive access to personal information for a variety of reasons, including: sloppy code development, tailoring your experience whether in-app or across apps, monetizing you, providing legitimate functionality or for nefarious purposes (e.g., to steal data and resell without your knowledge).

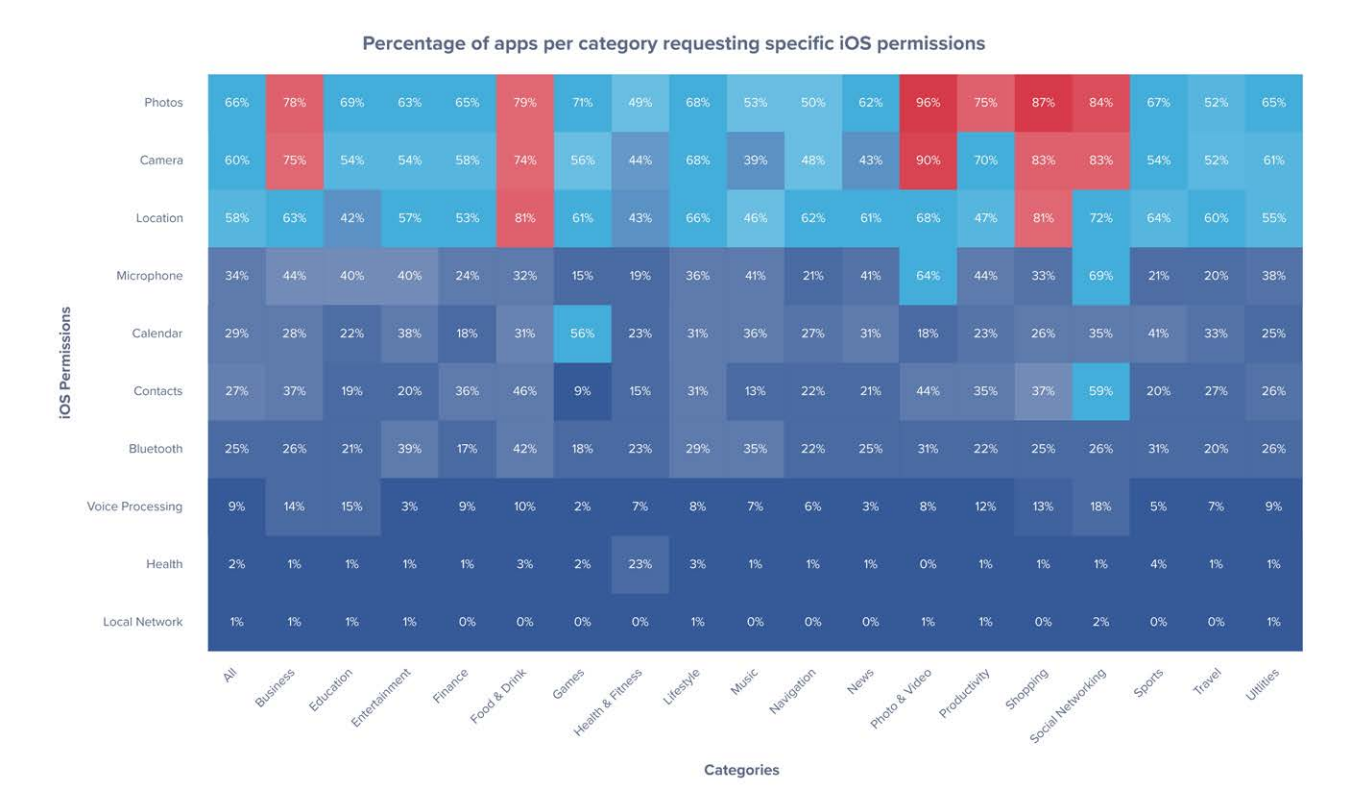
Apple and Google – who maintain the world's largest mobile app ecosystems for iOS and Android – have been cracking down on excess data collection. These two major platforms enforce standards that app developers must meet to gain a place on their respective app stores, and they continue to raise the bar when it comes to app permission transparency. Apple even made user privacy the theme of a recent **ad campaign.**

But the onus on proper data handling can't fall entirely on Apple and Google. Developers need to evaluate their data collection practices to minimize the potential privacy impact while maintaining functionality in their apps. On the other hand, consumers need to be aware of the privacy that they are giving up using the information available to them on their devices and the controls they provide to manage data collection.

Our analysis of iOS app permissions

To better understand the use of app permissions and the information that app developers are trying to collect, we looked at the metadata within a sample of almost 100,000 popular apps across the App Store catalogue. This sample was determined by looking at the apps that are installed within Wandera's customer base, which has 2.5 million devices under management. We did not include the millions of apps on the App Store that have not achieved widespread adoption. This analysis was carried out in Q2 of 2021. The metadata analyzed in this research comes from aggregated logs that do not contain personal or organization-identifying information.

For our analysis to be more actionable, we grouped apps by their App Store categories, allowing readers to look at how logical groups of apps are designed amongst their peer group.



Top four permissions

Our analysis shows the most requested data type is photos, with at least half the apps across every category requesting access to photos.

The top categories of apps requesting photo library access are:

1. Photo & Video (96%). This category includes apps such as YouTube, FaceApp and Splice.
2. Shopping (87%). This category includes apps such as Amazon, Shop and eBay.
3. Social Networking (84%). This category includes apps such as Facebook, Instagram and Twitter.

Photos

Historically, photo library access was all or nothing. For example, if a user wanted to upload a screenshot to Twitter, they'd have to give Twitter access to decades of photos in their library. There is nothing nefarious about a social media app needing photo library access, but this level of access is excessive and could put users at risk if paired with a poorly-built app. With iOS 14, Apple introduced **more consumer control** to photo permissions. Now, when an app needs the photo library, it must offer the user the choice of allowing access to selected photos or the entire library.

The camera is the second most popular permission requested.

The top categories of apps requesting access to the camera are:

1. Photo & Video (90%)
2. Shopping equal second with Social Networking (83%)
3. Business (75%). This category includes apps such as Zoom, Slack and WebEx.

Camera

While camera is a very common permission, it's a very risky one. With access to the camera, a bad actor can spy on users. This is the reason why top-secret organizations do not allow phones with cameras in their facilities and why some vendors disable camera access or remove it from the hardware to sell to these organizations.

In a **2020 lawsuit,** Instagram was accused of misusing the camera permission to spy on users when they had the app open but weren't interacting with the camera feature. Instagram claims it was a bug, and that no content was recorded.

Third on the list of most popular permissions requested is location.

The top categories of apps requesting location information are:

1. Shopping, equal first with Food & Drink (81%). The Food & Drink category includes apps such as DoorDash, UberEats and Yelp.
2. Social Networking (72%)
3. Photo & Video (68%).

Location

In 2019, both Apple and Google introduced an extra layer of consumer choice to location permissions. Prior to iOS 13, there were two location permissions: When In Use (foreground) and Always (background). With iOS 13, **Allow Once** was introduced, which is considered a temporary authorization.

Similarly, prior to Android 10, users were presented with two options: allow or deny. The former meant location was accessed at all times (foreground and background) and there was no in-between, but with Android 10, **tristate location permission** was introduced so users could then select 'allow only when app is in use.'

Learn more about location data misuse in **this investigation by The New York Times.**

The fourth most popular app request is microphone.

The top categories of apps requesting access to the microphone are:

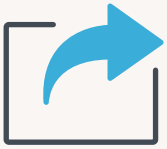
1. Social Networking (69%)
2. Photo & Video (64%)
3. Business, equal third with Productivity (41%). The Productivity category includes apps such as Asana, Google Calendar and TimeTree.

Microphone

Just like the camera, microphone app access in the wrong hands can have serious consequences. With the ability to activate the microphone, apps can record and transmit private conversations or **listen for what's going on around you** in order to sell this information to advertising organizations. And if the permission was abused, apps could do this without the users' knowledge.

However, in iOS 14, Apple introduced the orange dot that indicates when your microphone is in use by an app — making it easier for consumers to see if something fishy is going on.

Cross-app data sharing

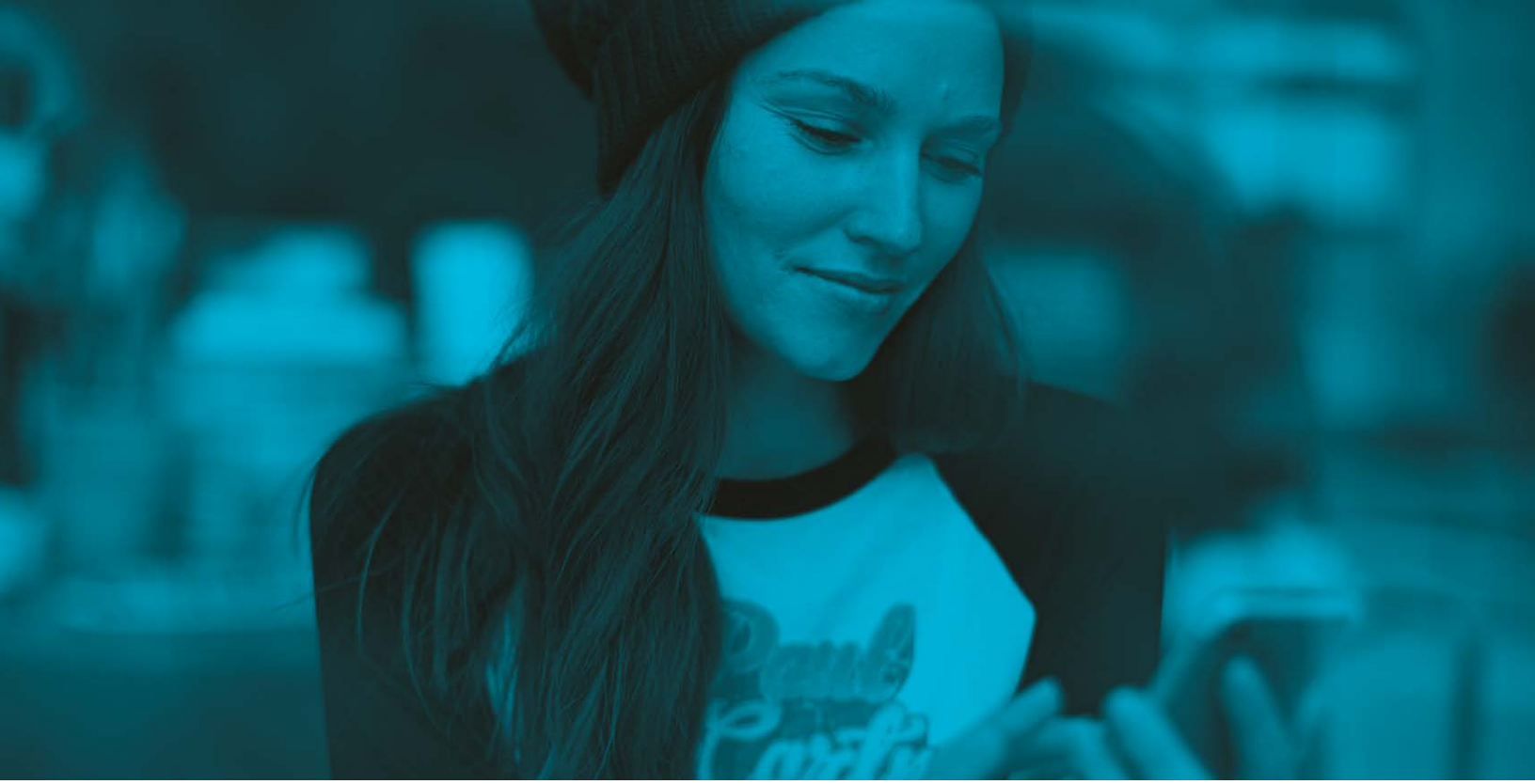


There is a great deal of information-sharing that goes on outside of the explicit permissions above. The app sandbox is intended to prevent apps from sharing data between them, but various tracking approaches circumvent that. Even though the apps aren't communicating directly with each other, by connecting various backend services and web interactions, an advertiser can piece together an accurate picture of a user based on their online behavior. Here are some examples of cross-app information sharing that fall outside of the permissions outlined above:

Information exchanges hands (or apps) via advertising identifiers that track and share information about user behavior for ad targeting purposes, which the average user probably never realizes. This cross-app information exchange for advertising is why after you searched for 'sourdough' on Google, your Instagram feed suddenly started including ads for bread-baking equipment. Recently, Apple device users were given more control over their privacy when Apple released its new App Tracking Transparency feature with iOS 14.5. Now app developers need to ask whether they can track your activity across other companies' apps and websites. Note: our permissions analysis does not yet include this permission due to its newness.

The next example concerns the photo library. Apps accessing the photo library might also be accessing GPS data embedded in the photos, making it possible for unwanted parties to decipher where a person has been and when — even where they live and work. Location data will only attach to photos if GPS is enabled for the camera. But if you disable GPS data for the camera, you will lose some of the benefits it provides within the photo library. **Here's some information on how to avoid sharing the location data of photos** when you send them.

A case of data mishandling came to light in 2020 when LinkedIn and TikTok were accused of **copying the clipboard** contents of iOS users. The issue was discovered in the beta version of iOS 14 when Apple added a new privacy feature that showed a quick pop-up that let users know when an app has read content from their clipboard. At first this may not seem consequential, but it's not uncommon for people to use a password manager and copy-paste credentials from the password manager into a website or app.



Key takeaways

Despite improvements by both Apple and Google in promoting personal privacy, consumers need to take steps of their own to secure their data. The purpose of this research is to encourage users to consider the data they are sharing before accepting any request that appears on their devices. There are some data points in this analysis that aren't surprising, and some that are.

For example, the majority (62%) of navigation apps request access to your location. It makes sense for placing you on a map, but why do almost half of them (48%) also request access to your camera? Same story for the 83% of shopping apps requesting access to your camera. It makes sense for scanning QR codes, but why do so many (87%) also request access to your photo library? It pays to think about what an app actually needs to function before hitting accept.

There are categories of apps asking for more access than others. According to our analysis, these are Photo & Video, Shopping and Social Networking. If you have a high number of apps in these categories, consider deleting any you don't use regularly to minimize the risk of data exposure.

Some permissions are more sensitive than others, and this will vary person to person. Maybe you work in an industry where you have sensitive files stored in your photo library, or maybe high-profile contacts in your contact library. If this is the case, consider reviewing each sensitive permission within your settings to audit the apps that have access to it so you can remove any that might pose a risk.

Recommendations

To minimize the risk of having your sensitive information exposed to unwanted parties, we recommend the following additional precautions:

- Read permissions carefully when they pop up. Ask yourself: does this app need access to the private data to function? For example, if a weather app is asking for access to your camera or contact library, think twice before accepting, and don't hesitate to deny access to requests that you don't understand or don't agree with.
- Regularly audit your app permission settings to see which apps are accessing what on your device. Things to look for: (1) apps you no longer use (consider deleting them but if you cannot, remove the permission to sensitive data); (2) apps that are in the news (has there been a burst of privacy activity?).
- When it comes to location data, always grant permission 'only while in use' — which is available on both iOS and Android.
- Delete apps you no longer use to minimize the risk of bugs appearing in old or abandoned apps. There are features available on both iOS and Android to offload/delete unused apps.

If you oversee apps for others in a business context, consider the following:

- Adopt a security solution that offers app vetting. An app vetting tool can regularly check applications for new and emerging app vulnerabilities within your mobile estate. App vetting tools can also deliver a comprehensive list of apps that are being used across the mobile device fleet, complete with popularity ratings, versioning details and additional metadata. This is exactly the kind of information that helps IT admins determine what actions need to be taken to address risky, out-of-date or non-compliant apps.
- Keep your mobile estate up to date. As Apple and Google add improvements to permissions settings, you want to ensure users are benefiting from them — so use a security tool that can flag out-of-date OS versions within your mobile estate.
- Ensure users aren't jailbreaking their devices to install third-party apps. Not only do the third-party apps pose a risk since they haven't been vetted by Apple or Google, but jailbreaking a device removes the protections built into the operating system, leaving the device in a very risky state.

Our intention with this analysis is not to invoke fear, but instead educate you and your users on the options available and how to best keep all aspects of device, user and organizational data secure. Contact us to learn how you can put safeguards in place and scale your security posture.

To learn more, contact Jamf.