UNDERSTANDING APPS AND WHAT THEY CAN DO

We have created this informational guide to help you with understanding the types of apps on a mobile device (smartphone) that may represent privacy or safety risks. The following are examples of various types of risky apps, how they may be advertised to consumers, and examples of the kinds of information that the app can obtain from a mobile device.

1. **CHILD TRACKING/PARENTAL CONTROL APPS**
   - **A.** These apps are advertised for parents to track their children.
   - **B.** These apps might be able to access location, call history and SMS (text) history, camera, microphone, and application usage.

2. **SPOUSE TRACKING APPS**
   - **A.** These apps are advertised for spouses or partners to track each other.
   - **B.** These apps might be able to access location, SMS (text) and call history, and Facebook/WhatsApp.

3. **PHONE COMPANY TRACKING APPS**
   - **A.** These apps are provided by your cell phone company and are often preloaded in many phones sold by those companies. These apps allow users with same phone plan to share their location.
   - **B.** These apps might be able to access your real-time location, and in some cases SMS and call logs.

4. **FIND MY PHONE/ANTI-THEFT APPS**
   - **A.** These apps are advertised for people who want to find their phone if they ever lose it.
   - **B.** These apps might be able to access your real-time location.

5. **FIND MY FRIENDS/FAMILY TRACKING APPS**
   - **A.** These apps are advertised to people who want to know the location of their friends and family.
   - **B.** These apps might be able to access your real-time location.

6. **DATA SYNCING APPS**
   - **A.** These apps are advertised for people who want to sync data between devices (other phones or computers).
   - **B.** These apps might be able to access location, call history, SMS (text) history, photos and videos.

7. **AUTOMATIC CALL RECORDING APPS (ANDROID PHONES)**
   - **A.** These apps are advertised for people who want to record phone calls on an Android phone.
   - **B.** These apps might be able to access call history and call recordings.

8. **OVERT SPYWARE**
   - **A.** These apps are advertised for people who want to remotely track and control another device.
   - **B.** These apps might be able to access location, call history, SMS (text) history, camera and microphone, keyboard, and social media communications (e.g., Facebook Messenger, WhatsApp, Snapchat, etc.).

EXAMPLES OF THE INFORMATION THE PERSON WHO INSTALLED THE APPLICATION MIGHT HAVE ACCESS TO:

- If the application is able to access your location, the person can track your real-time location at any given moment by searching for your mobile device on a map.
- If the application is able to access your SMS (text) history and call history, the person can forward all your text message conversations and a log of your call history.
- If the application is able to access your camera and microphone, the person can see through the camera on your mobile device and capture sound around you at any given time.
- If the application is able to access your camera, the person can access photos and videos saved on your mobile device.
- If the application is able to access your keyboard, the person can see anything you have typed into your mobile device's keyboard.
- If the application is able to access your Facebook account, the person can access what posts you liked and what you have commented under posts.
- If the application is able to access your Facebook messenger, the person can access message history exchanged between you and friends on Facebook.
- If the application is able to access your WhatsApp, the person can access your call log and message history.
- If the application is able to access your Snapchat, the person can access your memories and Snapchat stories as well as your Snapchat friends.

PLEASE NOTE THAT THESE ARE ONLY SOME EXAMPLES, AND ARE NOT A COMPREHENSIVE LIST OF ALL THE INFORMATION THAT THE PERSON WHO INSTALLED THE APPLICATION MIGHT HAVE ACCESS TO