Appendix 1: Methodology

This document describes the methodology BCP staff employed to identify and review 364 kids' mobile applications to examine the apps' disclosures about their privacy practices and interactive features and the apps' data collection and sharing practices. Our methodology was substantially similar to the methodology used in our December 2012 kids' app survey.

Following the steps described below, BCP staff first identified 498 kids' mobile applications (250 from Apple's App Store and 248 from Google Play). Staff limited the sample size to include only the first 200 results from each store. Staff subsequently excluded 36 apps (17 from Apple's App Store and 19 from Google Play) that fell within one of three categories: apps that reviewers categorized as intended only for adults, apps that required a specific device or pre-created account, and apps that reviewers could not interact with on first launch. Thus, the total sample size was 364 apps.

To identify the apps, in late 2014, staff searched on the term "kids" in the desktop version of Apple's iTunes App Store, which returned 250 results. As with the previous surveys, each app had its own nine-digit unique identifier number and its own app store promotion page describing the app. The app store promotion page for each app was viewable by typing in the specific web address within the itunes.apple.com website, which contained the unique app identifier number, into the Chrome browser on the desktop computer. Thus, staff located the unique web address for each app store promotion page using the following convention: http://itunes.apple.com/us/app/id[9-digit-unique-app-id]?mt=8. Staff then visited and saved copies of the browser-viewable app promotion pages for the apps identified through the search.

Immediately thereafter, staff searched on the term "kids" in the desktop version of Google Play, available at https://play.google.com. The search returned 248 results, each with its own unique identifier and its own app store promotion page describing the app. Like Apple, the Google Play app promotion page for each app was viewable by typing in the specific web address within the play.google.com website, which contained the unique app identifier, into the browser. Staff located the unique web address for each app store promotion page using the following convention: https://play.google.com/detials?id=[unique-app-id]&feature=search_result." Staff visited and saved copies of the app promotion pages for the apps identified through the search.

Staff saved each app store promotion page as a .txt file and as an .html file. Relevant fields found within the app promotion page, such as price, developer name, and number of ratings, were determined and extracted to an electronic database. As discussed above, staff then limited its sample size to the first 200 app results from each app store.

Staff downloaded the iOS apps onto one iPhone 5s that ran iOS version 8.1.1, and the Android apps onto one Samsung Galaxy S5 that ran OS version 4.4.4. Due to storage restrictions on the iPhone device, apps were downloaded in groups of 50, backed up to preserve the app version, and stored on an external drive.

Reviewers, following a set of instructions, examined the electronically captured app promotion pages (that had been saved as .html files) to answer a series of questions about the app, including app topic, age range, and whether any disclosures were found. Reviewers were also instructed to click on the website address listed on the app promotion page in the field for "[developer's] website" (and, for the iTunes App Store results, links found for "[App Name] Support"). Staff then saved and reviewed the resulting webpage (the "landing page" of the developer's website), and entered the answers to a series of questions into an electronic form.

Reviewers also clicked on all links found on the app promotion page or the developer website that appeared to lead to disclosures (e.g., staff clicked on all "Privacy Policy," "Terms of Service," and "End User License Agreement" links), and saved all relevant information, making sure to record exactly where the disclosure was found. In addition, reviewers read app descriptions found on each app promotion page and recorded the presence of any "short form" disclosures mentioned (e.g., explanations for permissions or notices regarding in-app purchases). Once reviewers completed the app promotion page and developer website review, staff conducted a quality check across the data to ensure consistency within the sample set.

After the app promotion page review, the reviewers began testing each app individually, closely following the same methodology for playing and interacting with the apps as was outlined in the December 2012 survey. This included playing with each app once, fully exploring the functionality to mimic a first time user's experience, while being as permissive to app permissions and features as possible. Any time an app requested a permission related to a device's functionality, such as for access to location data, staff permitted access. Staff also took screenshots of any additional privacy disclosures, as well as social network integration, in-app purchase capability, and advertising integration. To maintain a consistent testing environment, staff created baseline device configurations from which each app was opened, interacted with, and then closed. All findings were recorded in an electronic database.

As part of the testing process, staff also ran software that intercepted HTTP and HTTPS traffic to and from the mobile device by way of a proxy while the app was being used. Reviewers then saved the internet traffic associated with each app into individual files. Once all of the apps had been tested in this manner, staff reviewed the internet traffic that had been captured. In reviewing the internet traffic, staff looked for transmission of email addresses, usernames, passwords, device IDs, phone numbers, and geolocation information. Staff then conducted a quality check across the data to ensure accuracy and to eliminate false positives, and added the data to the electronic database.