PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE November 10, 2015

Apps Permissions in the Google Play Store

Analysis of over 1 million apps in Google's Android operating system in 2014 shows apps can seek 235 different kinds of permissions from smartphone users. The average app asks for five permissions.

BY *Kenneth Olmstead* AND *Michelle Atkinson*

FOR FURTHER INFORMATION ON THIS REPORT:

Kenneth Olmstead, Research Associate
Lee Rainie, Director, Internet, Science and Technology research
Dana Page, Senior Communications Manager
202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Kenneth Olmstead, Michelle Atkinson. "Apps Permissions in the Google Play Store." Pew Research Center. October 2015. Available at: http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/

About This Report

The research presented here is based on an analysis of 1,041,336 apps available in the Google Play Store, which provides apps for smartphones using Google's Android operating system. Data about these apps was collected for analysis from June 2014 through September 2014. However, it does not cover the apps ecosystem for iPhones, Windows phones, Blackberry phones or any of the other smartphone operating systems. It is intended to be a comprehensive look at how permissions are used in the Android ecosystem from the vantage point of how users are informed about how their information is collected and used. In addition, this report contains data about users' behaviors and attitudes around apps based on a nationally representative online survey conducted Jan. 27 to Feb. 16, 2015, as well as data about overall smartphone ownership from a nationally representative telephone survey conducted June 10 to July 12, 2015.

This report is a collaborative effort based on the input and analysis of the following individuals. Find related reports online at www.pewresearch.org/internet

Kenneth Olmstead, *Research Associate*
Michelle Atkinson, *Data Architect*
Aaron Smith, *Associate Director, Research*
Johnathon Hege, *Senior Data Architect*
Russell Heimlich, *Web Developer*
Dana Amihere, *Web Developer*
Seth Rubenstein, *Senior Web Developer*
Shannon Greenwood, *Assistant Digital Producer*
Lee Rainie, *Director, Internet, Science, and Technology Research*
Maeve Duggan, *Research Associate*
Margaret Porteus, *Information Graphics Designer*
Dana Page, *Senior Communications Manager*

In addition to Pew Research Center staff several outside experts were consulted on this report and we would like to thank: Jason Hong, Associate Professor in the Human-Computer Interaction Institute, part of the School of Computer Science at Carnegie Mellon University, and Jennifer King, Ph.D. candidate, UC Berkeley School of Information.

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

Summary of Findings

Today, 68% of Americans own a smartphone of some kind and an increasing number of digital interactions occur within the context of mobile apps. Apps (short for "applications") are programs that users can download to their smartphone or tablet computer. They can serve a nearly unlimited range of functions — from simple tools like a calculator to advanced digital assistants. They allow users to tailor their powerful pocket computer into a device with hundreds of potential uses that meet their owners' specific needs.

In order to function, apps may require access to both the capabilities of the devices they reside on as well as the user information contained on those devices. As users go about their lives, their mobile devices produce a vast trove of personal information and data, ranging from the user's location to a history of his or her phone calls or text message interactions. This puts apps at the center of debates about privacy in the digital age.

All of this information can be crucial to the functioning of mobile apps. But actually accessing a device's data or capabilities requires app developers to request it from end users in one way or another – often by asking users to click through an "I accept" box. Permissions are the mechanism by which app developers disclose how their apps will interact with users' devices and personal information on devices running Google's Android operating system. Once that permission is granted, the apps can amass insights from the data collected by the apps on things such as the physical activities and movements of users, their browsing and media-use habits, their social media use and their personal networks, the photos and videos they shoot and share, and their core communications. A newly released Pew Research Center survey from February 2015 finds that users place significant emphasis on how much information their apps collect from them: 90% of app users indicate that having clear information about how apps will access or use their personal data is "very" or "somewhat" important to them when deciding to download an app. Fully 60% of apps users have chosen to not download an app after discovering how much personal information the app required.

Clearly users are concerned about the information their apps require, but less is known about what is happening on the other side of the transaction — the permissions and capabilities that apps are most likely to ask for.

There is clear interest in understanding how information about mobile apps is conveyed to users. To gain more insight into the nature of the app universe as a whole and the permissions that apps require to run, Pew Research Center collected information about over 1 million apps in the Google Play Store.

We collected material about apps available in the Google Play Store between June and September 2014. The Google Play Store makes apps available for download to roughly half the smartphones (45%) owned by Americans. At the time of the data collection, the Google Play Store offered 1,041,336 apps. It is important to note that this study only looks at apps in the Google Play Store and does not cover apps available to consumers across all platforms. Pew Research Center chose to study the Google Play Store not because it is representative of the entire universe of apps across all device types, but because of the combination of both the popularity of the store and the relatively public access to the data.

In addition, Google announced a new version of Android (6.0 or "Marshmallow") that does change the structure of permissions for Android apps, discussed in detail below. This version of Android, however, will not be available to most users at the time this report is released.[1] This report provides a comprehensive look at Android apps in mid-2014 and how permissions are still displayed for most Android users:

- In the overall apps universe, there were 235 distinct types of permissions being sought across 41 different categories of apps, ranging from social networking and news apps to gaming. A table listing all the permissions, their functions and their implications can be found here.
- The average (mean) app in this dataset required five permissions before a user could install it.
- The categories of Communications and Business apps required the largest number of permissions in order to function.
- The most popular permission sought during this period allowed apps to access the internet connectivity of the smartphone.
- Of the 235 total permissions most (165) were related to allowing apps to access hardware functions of the device such as controlling the vibration function, while 70 allowed apps to access some kind of personal information.

In addition to this analysis of the Google Play Store app universe, a separate Pew Research Center survey conducted Jan. 27 to Feb. 16, 2015 found that:

- 77% of smartphone owners reported downloading apps other than the ones that came pre-installed on their phone.

[1] According to Google as of October 2015 the previous version of Android (5.0 or 5.1 "Lollipop") was running on 23.5% of Android devices worldwide, Lollipop was released to the first around of devices in November 2014. The largest number of devices (38.9%) run KitKat or Android 4.4 which was first released on Google's Nexus 5 device on Oct. 31, 2013. For updated figures on Android versions see Google's developer dashboards.

- 60% of these app downloaders had chosen *not* to install an app when they discovered how much personal information it required in order to use it, while 43% had uninstalled an app after downloading it for the same reason.
- 90% of app downloaders said how their personal data will be used is "very" or "somewhat" important to them when they decide whether to download an app; by comparison, 57% said it is equally important to know how many times an app has been downloaded.

The findings in this study pertain specifically to apps running on the Android operating system. Pew Research Center examined the Android platform because information about these apps is available on the web via the Google Play Store website. Apps running on Apple's iOS platform are available only through the iTunes store and not via a standard website. Given the challenges of collecting data about these iPhone and iPad apps, they are not included in this analysis.

Elaborating on key findings in the apps permission environment

The Pew Research data collection in mid-2014 compiled information on the "permissions" that Android apps required users to agree to as a condition of use. These might include simple hardware permissions — for example, allowing an app to adjust the volume of a users' phone. Other permissions seek more detailed and potentially sensitive personal information — for example, a user's contact lists or address book. At times, this can be crucial to the basic function of an app. At other times, such access can be a helpful convenience that allows the app to function more broadly, but it is not critical to the core mechanism of how the app functions. These permissions have wide implications for the kind of personal data Android phone users are sharing with the app's creator.

Some of the key additional findings in our analysis of the permissions in the Android marketplace include:

The most common permissions relate to allowing the app to access the smartphone's internet connectivity. The two most common permissions sought by Google Play apps help the app access the internet. These include the "full network access" permission (used by 83% of apps) as well as the "view network connections" permission (used by 69% of apps). The third- and fourth-most common permissions allow apps to access memory on the phone, a feature apps would need in order to save content to the device.

By category, communication and business apps require the largest number of permissions. Google breaks apps into 41 different categories, and app developers then choose which category they want their app to appear in. For this analysis, "games" was expanded into its 16 subcategories such as "arcade."[2] Among these categories, apps in the "communication" and "business" classifications require the most permissions in order to function. Communication apps require an average of nine permissions, while business apps require an average of eight. A table running through all the categories and examples of apps in each category can be found here.

The largest number of app permissions relate to hardware, rather than user information. To better understand what information apps could potentially access, Pew Research Center placed permissions into broad categories: 1) permissions that allow an app to access a hardware function of the device or 2) permissions that could potentially give the app access to *any* user information. Using this distinction, 70 permissions could allow an app to access user information, while 165 allow an app to control some hardware function of the device, such as allowing the app to control the vibration function of the device or control the camera flash.

[2] Eight apps were missing category information.

The apps universe is a "long tail" system. As of fall 2014, the overwhelming majority of Android apps have been installed by only a small number of users. Around half (47%) of all apps have been installed fewer than 500 times, and more than 90% have been installed fewer than 50,000 times. On the other end of the spectrum, a relatively small number of apps have been installed by vast numbers of users — a total of four apps have been installed over 1 billion times.[3] See Chapter 2 for more information on individual apps.

Why apps seek permissions

In spite of users' concerns about the privacy implications of apps permissions, it is a simple fact that permissions are required for even the most basic apps to function. Consider, for instance, a "flashlight" app that turns on the camera flash permanently (as opposed to "flashing" like it would when taking a picture), so that it can be used as a flashlight. Even an app this basic would require the "control flashlight" permission in order to function as advertised.

Complicating the matter even further for users, app developers cannot edit the description of each permission and therefore cannot include information about *why* each permission is needed. This information can be included in the description of the app itself, but not with each individual permission as the user sees them. Users would have to first know what the app is supposed to do, and then evaluate the permissions that app is requesting to decide whether they are appropriate or not.

Moreover, the pure number of permissions an app requests also does not necessarily reflect how much user information it is able to access. An app with a single permission could potentially access a wealth of user information, while an app with multiple permissions might be able to interact with the phone's hardware components but remain walled off from any personal data about the user.

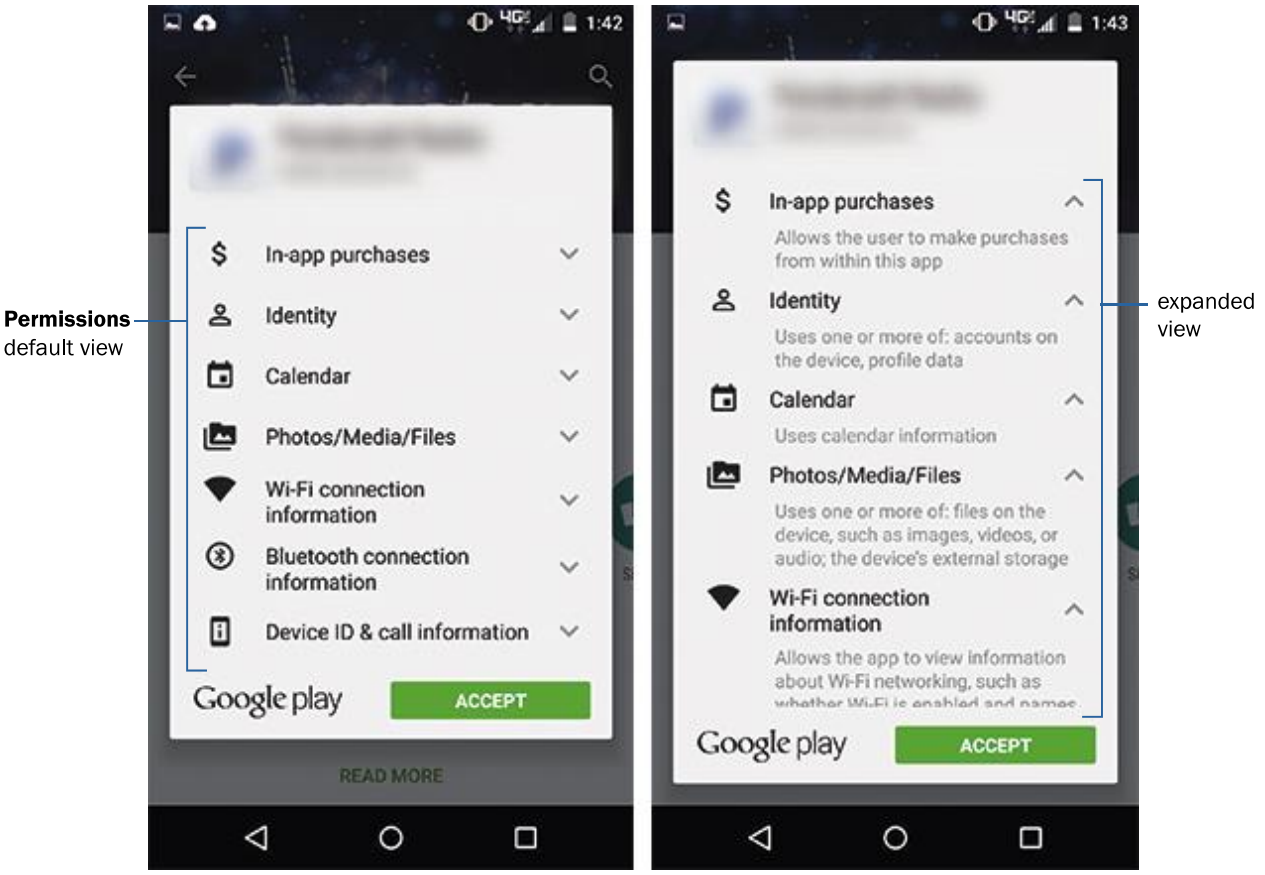
Ultimately —despite user concerns about the information being requested by the apps they use — the amount of personal information users are putting at risk depends almost entirely on the individual app, the permissions it requests and the context in which those permissions are being used.

[3] 7,293 apps were missing install information.

How to find permissions

There are several places users can find the permissions an app is requesting. The most visible place is when a user chooses to download an app on their device (the other is on the web at the Google Play Store site). On an Android smartphone (or tablet) when a user chooses to download an app, they tap the "install" icon and will see a screen that looks like this:

Typical Install Screen for Android Apps



Source: Google Play Store. Screenshot was taken using a Motorola X (2nd generation) running Android 5.1 (Lollipop). Taken on Sept. 3, 2015.

Note: Given the diversity of Android devices this screen may appear slightly differently depending on the device. This is how the screen appears on devices Android 5.1 or earlier, Android 6.0 will look different depending on the app being downloaded.

PEW RESEARCH CENTER

Once apps are installed on the phone, users can typically check to see which permissions they have granted by going to the app in the Google Play Store. Permissions are always available for the user

to see on each app's Google Play page (on the web or from a mobile device). They are also updated as the app is updated.

At the moment of download, the permissions regime is "all or nothing." In order to get an app installed on your device the first time you have to agree to all of the permissions (this regime has changed with the newest version of Android, discussed in detail below). It is also important to note that not all permissions discussed in detail in this report can be found on this screen. Android groups permissions into broader categories.

For example, the category "SMS" includes six separate permissions not all of which may be displayed on the screen above. Users can, however, see all of the permissions each app asks for in detail by going to the "settings" menu on their device and selecting "application manager" or "apps" depending on the device. The user can then select an app. Each app has a full list of the permissions it asks for here, which will contain the permissions as they are presented in this report (this is also possible through the web version of the Google Play Store).

It is important to note that this was how permissions worked until Fall 2015 when Google announced the release of Android 6.0 or "Marshmallow." While this operating system will not be available to most users for some time, it does overhaul the way permissions are displayed.[4] The main change is that on devices running Android 6.0, users will be able to toggle individual permissions on and off on an app-by-app basis. In addition, permissions will be displayed not at the moment of download, but when an app requires the particular permission. For example, an app that requires the user's location information would prompt the user to agree to the location permissions at the moment the app needs access, users would then be able to turn this permission off later.

This change puts the Android permission structure much closer to the way the same type of information is conveyed on Apple devices. While this is a major change in how permissions are displayed, the set of permissions themselves remains the same. The data studied here reflects the individual permissions users will still have to agree to, but they will be presented to the user using this new method.

[4] According to Google as of October 2015, the previous version of Android (5.0 or 5.1, "Lollipop") was running on 23.5% of Android devices worldwide. Lollipop was released to the first around of devices in November 2014. The largest number of devices, 38.9%, run KitKat or Android 4.4, which was first released on Google's Nexus 5 device on Oct. 31, 2013. For updated figures on Android versions see Google's developer dashboards.

How Android App Data Was Collected

Findings about Google apps permissions in this report are based on an analysis of data about 1,041,336 apps collected from the Google Play Store between June 2014 and September 2014. The data collection or scraping ("scraping" in this case refers to the process of copying the contents of a web page) began with a custom extension for the Google Chrome web browser created by Pew Research Center developers.

The extension opens the Google Play Store website and goes to the webpage for an app as designated by a unique app ID each app in the store receives. It then copies the content of that app's page, stores that information in a SQL database, and moves on to the next app in a continual process until no more app ID's are available. The extension engaged in data collection from June 18 to September 8, 2014.

There are now over 1.7 million apps as of October 2015.[5] Because this data is from 2014, apps introduced to the Google Play store after September 2014 are not included in this study and information about the apps included here may have changed during the time since this data was collected. The scraping process included all apps available through the Google Play Store website (except apps where there were errors in the scraping process). It did not differentiate between U.S. and non-U.S. apps and does include apps where some of the associated information is not in English.

About The Web Survey

Survey findings about apps usage and attitudes in this report are based on a Pew Research Center survey conducted between Jan. 27, 2015, and Feb. 16, 2015, among a sample of 461 adults ages 18 or older. The survey was conducted by the GfK Group using KnowledgePanel, its nationally representative online research panel. GfK selected a representative sample of 1,537 English-speaking panelists in the United States to invite to join the subpanel and take the first survey in January 2014. Of the 935 panelists who responded to the invitation (60.8%), 607 agreed to join the subpanel and subsequently completed the first survey (64.9%) whose results were reported in November 2014. This group has agreed to take four online surveys about "current issues, some of which relate to technology" over the course of a year and possibly participate in one or more 45- to 60-minute online focus group chat sessions.

[5] AppBrain, Oct. 12, 2015.

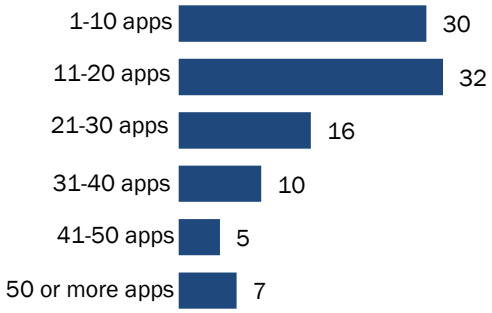
Chapter 1: The Majority of Smartphone Owners Download Apps

Apps, short for "applications," are a main feature of modern smartphones and tablet computers. They allow users to interact with their devices in new ways. From calendars to music players, apps offer myriad experiences to users, and that universe is expanding every day.

This growth in apps is paralleled by a growth in the amount of data these apps can collect from users. Smartphones can collect all kinds of data about users and their activities once users grant permission to apps to do so. The boundaries of what data is being collected are governed by privacy policies, terms of service and other legal agreements that users agree to when downloading apps to their device.

App Users Often Download Dozens of Apps

% of app downloaders who have downloaded the following number of apps to their smartphone



Source: Source: Pew Research Center Surveys, Jan.27-Feb. 16, 2015. N=461 Adults Ages 18+. The margin of error for all adults is +/- 5.8 percentage points.

PEW RESEARCH CENTER

Some 68% of American adults now own a smartphone, and an online survey of a representative sample of adults 18 and older by Pew Research Center finds that 77% of these smartphone owners have downloaded apps in the past (other than the ones that came pre-installed on their phone).[6] Fully 38% of these app downloaders report having more than 20 apps on their device and 7% report having 50 or more. This survey covered all smartphone owners, not only owners of Android devices.

At the same time, app downloaders tend to use a relatively small number of apps on a regular basis. Almost half of app downloaders report that they use five or fewer apps at least once per week, and just 16% indicate that they use more than 10 apps on a regular basis.

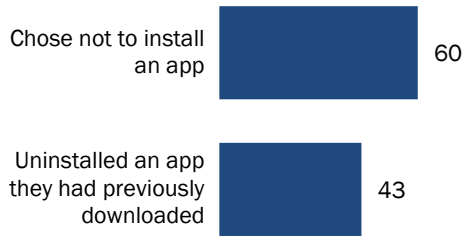
[6] The Pew Research Center survey findings on overall smartphone ownership are based on telephone interviews conducted June 10, 2015, through July 12, 2015, among a national sample of 2,001 adults, 18 years of age or older, living in all 50 U.S. states and the District of Columbia. Survey findings about apps usage and attitudes in this report are based on a Pew Research Center survey conducted between Jan. 27, 2015, and Feb. 16, 2015, among a sample of 461 adults ages 18 or older.

Overall, having clear information about how one's personal data will be used by an app is as important to prospective apps downloaders as user ratings and reviews: 90% of smartphone owners say that knowing how their personal data will be used is "very" or "somewhat" important when choosing whether or not to install an app. By comparison, 57% indicate that it is similarly important to know how many times the app has been downloaded, and 56% indicate that it is important to know the uses of the app.

In addition, a majority of app downloaders (60%) have chosen *not* to install an app when they discovered how much personal information the app required in order to use it, while 43% have uninstalled an app *after installing it* for the same reason.

Users Are Concerned About Apps and Personal Information

% of app downloaders who chose to do the following after discovering how much personal information the app required



Source: Pew Research Center Surveys, Jan. 27, 2015 to-Feb. 16, 2015. N=461 Adults Ages 18+. The margin of error for all adults is +/- 5.8 percentage points.

PEW RESEARCH CENTER

Surveys are useful for understanding users' attitudes and habits with their apps, but this mode of data collection cannot shed much light on the other side of the equation — namely, what's happening with the apps themselves and the ecosystems from which these apps emerge. Users often have difficulty recalling what specific permissions the different apps they have downloaded to their phone actually require and perhaps may not even fully understand these permissions in the first place.

More broadly, surveys of consumers cannot conclusively answer important research questions such as how many different mobile app permissions exist in the first place or how common it is for apps to request various types of permissions from potential users. Other researchers have examined the general subject of app permissions in the Android environment in various ways. Utilizing user comprehension surveys, research groups at the University of California and University of Washington have found that relatively few users pay attention to app permissions – and an even smaller number understand the permissions they are agreeing to. Other studies have found that the act of requesting access to user data is highly context-dependent, and that users who find it appropriate to share their data with one app might recoil at the idea of sharing the same data in a different context. Still others have examined situations in which apps can overreach when requesting permissions.

In an effort to build on this body of knowledge and examine these and other issues, Pew Research Center scraped the contents of over 1 million apps in the Google Play Store, an approach that was chosen not because it is representative of the entire universe of apps across all device types, but because of the combination of both the popularity of the store and the relatively public access to the data, as is laid out in the next chapter. This scraping collected a wide range of metadata about each app — including the permissions they require from users upon installation.

Chapter 2: An Analysis of Apps in the Google Play Store

Pew Research Center surveys and independent analysts have found that roughly one-third of all American adults – and about half of smartphone owners – have an Android smartphone. All apps for Android phones are housed in the Google Play Store, and each app has its own web page where information about the app is available. Each web page includes basic descriptive information such as what type of app it is; how much, if anything, the app costs to download; the app's content rating; and what information or other permissions the app requires from users.

To collect information on these apps, Pew Research Center scraped each app's page in the Google Play Store using the Chrome browser and a custom browser extension. The extension copied all of the information on each page and stored it in a database for later analysis. The data collection was conducted from June to September 2014, and captured information of about 1,041,336 unique apps (see the Methods section for a detailed description of this process).

Pew Research Center elected to study the Android ecosystem for two specific reasons. First, information about apps in the Google Play Store is freely available on the Google Play Store website and therefore easily aggregated. Second, the Google Play Store publishes information about app permissions along with the other metadata, and the issue of permissions is a key focus of this research.

Other platforms, such as iOS (Apple's mobile operating system), are more challenging for outside parties to access, and they handle the process of informing users about app behavior differently and in ways that are considerably more complicated to analyze. For these reasons, only apps within the Android ecosystem in mid-2014 are included in this analysis. It should be treated as a study of one app ecosystem and how it handles informing users about how their information is being collected and used.

Moreover, the situation in the Google Play Store has changed somewhat from the time these data were collected and the permissions regime that exists for those who now want to install apps on their Android phone. As noted above, the Android operating system was changed this summer when Google announced a new feature in the next version of the Android operating system. This new feature would allow users to turn off certain permissions on an app-by-app basis and to see all of the apps permissions in a single place (sometimes referred to as a "permissions dashboard"). While this change will be significant when it is fully available, it is still built upon the existing structure of permissions.

There are Dozens of App Categories in the Google Play Store

Category	# of Apps	% of Total	Example Apps
Education	83,885	8.06%	Pocket Physics, Nasa App
Entertainment	80,372	7.72%	YouTube, NBC
Personalization	75,090	7.21%	Premium Wallpapers, Digital Clock Widget
Tools	74,178	7.12%	Tiny Flashlight, Google Translate
Lifestyle	73,462	7.05%	Starbucks, Eventbrite
Books & Reference	62,946	6.04%	Bible, Amazon Kindle
Business	56,341	5.41%	Google Docs, Adobe Acrobat Reader
Travel & Local	51,740	4.97%	Southwest Airlines, TripAdvisor Hotels
Puzzle*	45,500	4.37%	Soduku Free, Cut the Rope
Music & Audio	40,580	3.90%	Spotify Music, Pandora Radio
Sports	36,908	3.54%	CBS Sports, ESPN
Casual*	35,662	3.42%	Candy Crush, Farmville
News & Magazines	30,877	2.97%	USA Today, The Wallstreet Journal
Arcade*	30,749	2.95%	Pac-Man 256, Frogger
Productivity	30,230	2.90%	Pocket, SwiftKey Keyboard
Health & Fitness	28,617	2.75%	Runkeeper, Weight Watchers Mobile
Finance	23,830	2.29%	Bank of America, Wells Fargo Mobile
Communication	22,338	2.15%	Skype, Snapchat
Social	20,849	2.00%	Twitter, Instagram
Shopping	17,326	1.66%	Amazon, eBay
Media & Video	15,985	1.54%	Livestream, Ringtone Maker
Transportation	14,727	1.41%	Uber, Citymapper
Medical	14,632	1.41%	MyChart, Doctor on Demand
Photography	12,526	1.20%	Snapfish, GoPro App
Action*	8,090	0.78%	Plants vs. Zombies
Card*	6,751	0.65%	Solitaire, World Series of Poker
Educational*	5,308	0.51%	Learning Colors, Vocabulary Builder
Racing*	4,931	0.47%	Furious Racing, Real Racing: 3
Comics	4,772	0.46%	Marvel Comics, DC Comics
Weather	4,375	0.42%	The Weather Channel, AccuWeather
Adventure*	3,858	0.37%	The Walking Dead, Dungeon Legends
Family	3,609	0.35%	Star Tracker, Elmo Loves ABC's
Libraries & Demo	3,488	0.33%	Katherine U.S. English Text-to-Speech Voice, Google Cardboard
Trivia*	3,103	0.30%	Trivia Crack, Family Feud
Simulation*	2,871	0.28%	The Sims 3, Farming Simulator
Casino*	2,397	0.23%	Slots, Bingo!
Strategy*	2,260	0.22%	World at Arms, Clash of Clans
Board*	2,101	0.20%	Domino!, Yahtzee
Word*	1,794	0.17%	Scrabble, Word Search
Role Playing*	1,602	0.15%	Doom & Destiny, The Bards Tale
Music*	668	0.06%	Rock Hero, Real Drum

Source: Google Play Store, June 18-Sept. 8, 2014.

Note: The "games" category was expanded to its subcategories. Each of the different subcategories of "games" is marked by an "*." If combined "Games" would make up 11% of total apps. Pew Research Center used the categories available in the Google Play Store and did not do any further categorization. Eight apps did not have category information.

PEW RESEARCH CENTER

At the time of the data collection, the Google Play Store broke apps down into 41 general categories. Education apps were the most common individual category, comprising 8% of the total number of apps available for download.[7]

Overall, eight categories of apps (Education, Entertainment, Personalization, Tools, Lifestyle, Books and Reference, Business, and Travel & Local) comprised more than half of the apps available for download (53.58% in total).

Music apps were the least prevalent category, comprising just 668 apps — or 0.06% of the more than 1 million total apps in the Store. When collecting this app data, Pew Research Center used the categories in the Google Play Store and conducted no additional categorization of the apps in the dataset.

The majority of apps in the Google Play Store (82%) were free to download at the time of the data collection. Most, but not all, apps that are free to download were supported by advertising. On average, free apps ask for two more permissions than paid apps (Six permissions vs. four permissions.)

Paid vs. Free Apps

	Number of apps	% of total
Free	851,872	81.8%
Paid	189,464	18.2%

Source: Google Play Store, June 18-Sept. 8, 2014

PEW RESEARCH CENTER

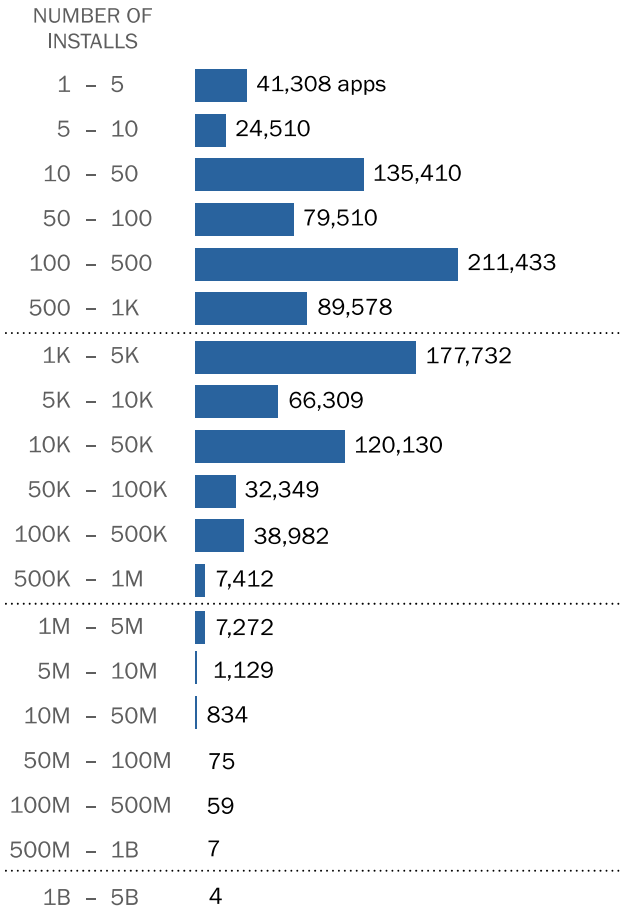
[7] The category of "games" has 17 subcategories displayed here. In the Google Play Store "Games" is a super category in which users can see all games combined together or browse by game category; here the subcategories of "Games" are displayed individually. "Games" reported as a single category would be the largest at around 11% of the Google Play Store. Eight apps did not have category information.

The Google Play Store contained more than 1 million apps, but the overwhelming majority of these apps had been installed by only a small number of users. Close to half (47%) of all apps available had been installed fewer than 500 times, and more than 90% had been installed fewer than 50,000 times. On the other end of the spectrum, a relatively small number of apps had been installed by vast numbers of users.[8]

Indeed, four apps were downloaded between 1 billion and 5 billion times as of September 2014 — Google Maps, Gmail, Google Play Services and YouTube. It is important to note that all four of these apps, however, are required downloads for all Android devices. Put another way, users did not necessarily choose to download these apps, they came preloaded on their device (or at least users were prompted to download them automatically when setting up their device for the first time).

Android Apps Have a Long Tail by Number of Installs

# of apps by the # of times they have been installed



Source: Source: Google Play Store, June 18-Sept 8, 2014
Note: 7,293 apps did not have install information.

PEW RESEARCH CENTER

In the next group of most downloaded apps, there are two that are not required by Google. Seven apps — Facebook, Google Play Books, Google+, Google Search, Google Text-to-Speech, Google Street View and WhatsApp — had been installed between 500 million and 1 billion times as of September 2014. Of those seven, Facebook and WhatsApp (a messaging app owned by Facebook) are not Google apps and are not required installs on Android devices.[9] Google did relax its pre-installed app requirement somewhat in August of 2015 when the firm removed Google+ and Google Play Books from the list of required apps.[10]

[8] 7,293 apps did not have install information
[9] Google Search is referred to as "Google" in the current version of the app referenced here.

There is also a wide variation in how often apps are updated. Around half (48%) of apps were updated sometime in 2014.[11] The main reasons apps stay updated are to keep up with Google updating the Android operating system and to deliver new features to their users. With half the apps not updating at all in 2014, it is clear that many apps are not trying to keep up with this process or are simply not being used.

[10] Hildenbrand, Jerry. "Your new phone will have less Google bloatware, and that's awesome." Androidcentral.com. August 19, 2015.
[11] Because the data was collected over several weeks and each app was scraped only once it is possible some apps were updated during that time period and that change was not collected.

Chapter 3: An Analysis of Android App Permissions

Most large internet companies use the same general methods for informing users about how their data will be used. These include agreements any frequent internet user would be familiar with such as privacy policies or terms of service. This study looks at one type of agreement: the permissions required by apps on Android devices.

In the Android operating system, this point of contact is a three-way relationship between the user, Google (the designer and provider of the Android operating system) and third-party app developers. Google moderates the relationship between the user and the third-party app developer using a set of "permissions" for each app a user downloads. Permissions are Google's way of requiring developers to disclose how the app will be interacting with the user's device and what information the app will have access to.

In the Android ecosystem, the burden is on the developer to choose the correct permissions that describe to the user what the app is doing. This is not to say Google is entirely hands off, but the first step begins with the app developer.

App Permissions Vary a Bit by Category

Category	Average (mean) # of Permissions	Category	Average (mean) # of Permissions
Communication	9	Education	5
Business	8	Entertainment	5
Casino	7	Family	5
Lifestyle	7	Health & Fitness	5
Role Playing	7	Medical	5
Shopping	7	Music	5
Social	7	Productivity	5
Transportation	7	Racing	5
Travel & Local	7	Simulation	5
Finance	6	Tools	5
Media & Video	6	Trivia	5
Music & Audio	6	Weather	5
News & Magazines	6	Arcade	4
Photography	6	Board	4
Sports	6	Books & Reference	4
Strategy	6	Card	4
Action	5	Casual	4
Adventure	5	Comics	4

Source: Google Play Store, June 18-Sept 8, 2014.

Note: "Games" was expanded into its subcategories for this list. 8 apps did not have category information.

PEW RESEARCH CENTER

After an app developer has built an app, chosen the correct permissions, and has created the list to which users will eventually agree, Google scans the app for malware and malicious code.

Permissions range from allowing the app to interact with specific hardware on the device (such as the camera flash) to allowing the app to access a user's contact list. The user must agree to the entire list before downloading the app.

Again, it is important to note that the above information describes how the Android operating system functioned through June 2015, when Google announced a new feature in the next version

of the Android operating system (Android 6.0, referred to as “Marshmallow,” was released in the fall of 2015). This new feature would allow users to turn off certain permissions on an app-by-app basis and to see all of the apps permissions in a single place (sometimes referred to as a “permissions dashboard”). See the “How to Find Permissions” section above for a detailed explanation of the updates in Android 6.0.

Google App Permissions Basics

Documenting the various permissions that different apps require of users is a key focus of this study. This section of the report examines the range of app permissions in the Google Play Store, with a focus on permissions that have the potential to allow apps to collect or share users' personal information.

In total, the 1,041,336 apps in this dataset contain 235 unique permissions. The most permission-hungry apps can require a large number of permissions from users: the single highest number of permissions required by any app was 127, although it is generally quite rare for apps to require this many. Most apps request only a handful of permissions. The average (mean) app requests five permissions. Indeed, this analysis found that nearly 100,000 apps request no permissions at all.

Top App Permissions in the Google Play Store

Permission	What the Permission Does *"Allows the app to ..."*	Number of apps	% of apps	Hardware Permission or User Information
Full network access	... create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.	855,873	83%	Hardware
View network connections	...view information about network connections such as which networks exist and are connected.	714,607	69%	Hardware
Test access to protected storage	... test a permission for USB storage that will be available on future devices. Allows the app to test a permission for the SD card that will be available on future devices	562,442	54%	Hardware
Modify or delete the contents of your USB storage	...write to the USB storage. Allows the app to write to the SD card.	559,941	54%	User info
Read phone status and identity	... access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.	361,616	35%	User info
Prevent device from sleeping	... prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.	279,775	27%	Hardware
Precise location (GPS and network-based)	... get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are, and may consume additional battery power.	246,750	24%	User info
View Wi-Fi connections	... view information about Wi-Fi networking, such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.	235,093	23%	User info
Control vibration	... control the vibrator.	220,594	21%	Hardware
Approximate location (network-based)	... get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.	216,770	21%	User info

Source: Google Play Store, June 18-Sept. 8, 2014.
Note: Descriptions of each permission are how they appear to a user.

PEW RESEARCH CENTER

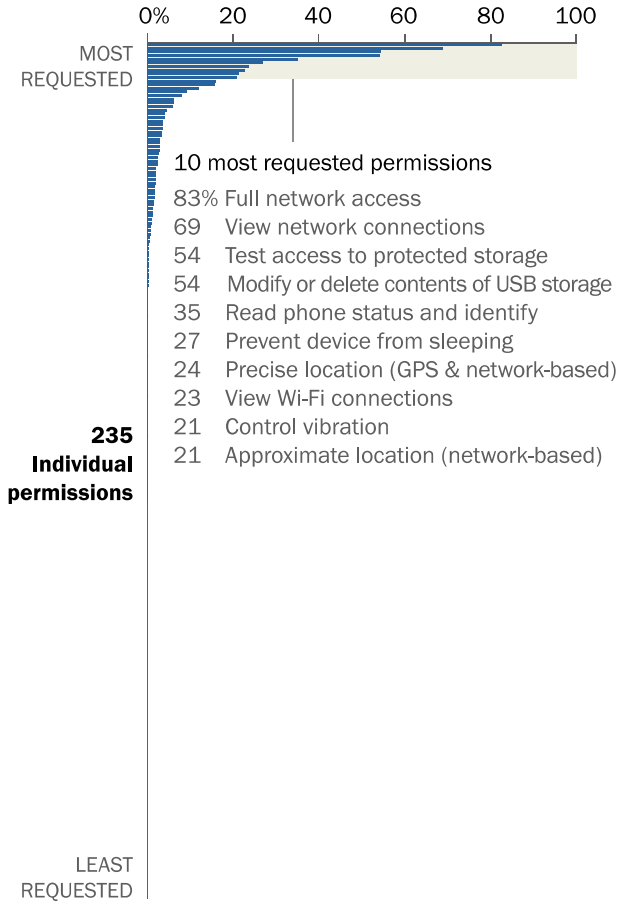
Ultimately, in the apps that were part of this data collection, a relatively small number of permissions appear in a wide range of apps: out of the 235 total permissions, just 10 are used by more than 20% of the apps in the Google Play Store. Conversely, a large number of permissions are used by only a small handful of apps: 147 of the 235 permissions identified are used in fewer than 1,000 individual apps (that works out to 0.09% of the total number of apps.)

Of course, the total number of permissions an app requests does not necessarily reflect how much user information it is able to access. An app with a single permission could potentially access a wealth of user information, while an app with multiple permissions might be able to interact with only the phone's hardware components but remain walled off from any actual end user data.

The analysis that follows takes a deeper look at the types of permissions in the Google Play Store. In particular, it examines the relative prevalence of two different types of permissions: permissions that could in any way allow an app to access user information and permissions that only allow an app to interact with the device itself (and not the data residing on the device).

Permissions Have a Long Tail of Apps that Request them

% of apps requesting each permission



Source: Google Play Store, June 18-Sept 8, 2014.

PEW RESEARCH CENTER

It is important to note here that these distinctions define "user information" in the broadest possible sense. Permissions were given the distinction of accessing "user information" if they hypothetically gave access to *any* user information. Whereas permissions that access the device hardware allow an app to *only* access functions of the device itself.

This distinction was created by Pew Research Center to help differentiate between permissions that access any user information and those that do not. Google also makes a similar distinction by

categorizing permissions into several levels of security. The two most common are “Normal” and “Dangerous.” This distinction is slightly different than the one used in this report and can be read in detail here.

The main difference is that the distinction in this report uses a much more broad definition of “access to user information” to include permissions that access even the most trivial of user information. Permissions that could access user information fall on a continuum with some granting access to sensitive user information and some granting access to very little, if any, sensitive information. The goal of the distinction used in this report was to not make judgements about what is “sensitive” user information and what is not, as that can often be a highly subjective question. Instead permissions were simply categorized as accessing *any* user information or *none*. Permissions that do not access user information can still be harmful to the device, but that is a different question than what is studied here.

Permissions that control device hardware

Of the 235 unique permissions collected in this scraping, 165 allow the app to interact with just the hardware components of a device and do not allow access to any user information.

The two most common permissions, for example, help apps connect to the internet. The "Full Network Access" permission (used by 83% of apps) allows an app to access whatever network the device is connected to at the time, while the "View Network Connections" permission (used by 69% of apps) allows the app to see what networks the device has access to. Any app requiring access to the internet in order to function properly would need to have one or both of these permissions. While these two permissions are near-ubiquitous, they do not, by themselves, allow their associated apps to access any user information directly.

Some other examples of this type of permission include:

- Control Flashlight – This permission allows an app to interact with the built-in flash in most smartphones and tablets. Usually this flash is for the camera, but apps can use this to create a "flashlight" by permanently turning the flash on and off.
- Set Wallpaper – This allows an app to set the image in the background of the home screen on a device (commonly called the "wallpaper" on Android devices).
- Control Vibration – This allows the app to control the vibration function found in most smartphones.

These permissions are not necessarily entirely benign. If used incorrectly (or maliciously), an app with one of these permissions could potentially damage a user's device. But ultimately these permissions by themselves do not allow an app to access user information. The next section will cover permissions that do, in theory, give an app access to some kind of user information.

Permissions that access user information

The second category of permissions includes those that allow apps to access user information of one kind or another. This category of permissions is generally less common than permissions that control device hardware — out of the 235 unique permissions identified in this scraping, 70 could potentially access user information.

Examples of this type of permission might include permissions that allow an app to modify or delete photos from a user's photo library or to read the contents of a user's contact list. As these examples illustrate, these permissions exist on a continuum in terms of the volume and type of information they might allow an app to access.

Top App Permissions That Could Access User Information

Permission	What the Permission Does *"Allows the app to ..."*	# of Apps	% of Apps
Modify or delete the contents of your USB storage	... write to the USB storage. Allows the app to write to the SD card.	559,941	54%
Read phone status and identity	... access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.	361,616	35%
Precise location (GPS and network-based)	... get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are and may consume additional battery power.	246,750	24%
View Wi-Fi connections	... view information about Wi-Fi networking, such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.	235,093	23%
Approximate location (network-based)	... get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.	216,770	21%
Find accounts on the device	... get the list of accounts known by the device. This may include any accounts created by applications you have installed. Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed.	162,925	16%
Take pictures and videos	... take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.	124,733	12%
Directly call phone numbers	... call any phone number, including emergency numbers, without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services.	84,290	8%
Read your contacts	... read data about your contacts stored on your tablet, including the frequency with which you've called, emailed or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.	64,377	6%
Read call log	... read your tablet's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge. Allows the app to read your phone's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge.	42,797	4%

Source: Google Play Store, June 18-Sept. 16, 2014
Note: Descriptions of each permission are how they appear to a user.

PEW RESEARCH CENTER

In addition, it is extremely challenging to judge the potential damage to a smartphone user that could be caused by access to any particular piece of personal- or phone-collected information. It is certainly the case that a permission such as "View Wi-Fi connections" would expose very little user information to the app, since it simply grants the app access to see what Wi-Fi networks are available and collect basic information about them. But without knowing how apps are using the information they collect used it is hard to decide what user information is "sensitive"; therefore any user information is treated as potentially sensitive for the purpose of this analysis. At the same time, this judgement is highly contextual, and users should not necessarily view these permissions as inherently dangerous or detrimental to their privacy.

The most-common permission that *could* access user information is "modify or delete the contents of your USB storage," and it is required by 54% of apps. This permission allows an app to look at information stored on a devices' external storage and delete or change that information.

This permission is a good illustration of the continuum on which these permissions exist. The level of "exposure" users might experience would depend both on the type of information the user has stored on their external storage and also on the setup of the device itself. Some devices store information on external storage, while others do not even have external storage in the first place. Ultimately, this permission could certainly give an app access to user information — but this potential is highly dependent on each user's individual situation and device.

The "record audio" permission is another example that has the potential to collect sensitive information, but is highly contingent on how it is used. This permission allows an app to turn on the microphone of the device and record audio — a relatively simple task, but one broad enough to potentially cause harm.

In 2013, Facebook created some controversy when it added a new feature to its app that utilized the "record audio" permission. The new feature let users opt-in to a service that would automatically detect what they were watching or listening to when posting to Facebook and include that information along with their posts.

This feature created an uproar among some users and pundits, who worried that Facebook could potentially use it to record and store everyday conversations. Facebook later clarified that the feature was entirely opt-in, would not record anything other than music, TV shows and movies, and would not store any of those recordings for any amount of time.

In each of these instances, it is difficult to determine just how much personal information (if any) a given permission might be able to access. At the same time, certain permissions clearly provide

access to sensitive information — regardless of the users' behavior or the individual circumstances of the device. For example, two permissions allow an app to ascertain the user's physical location at any given moment. One does this using the device's GPS and network connection ("precise location," used by 24% of apps), while the other does so using just the network connection ("approximate location," used by 21% of apps).

In this case, users do have the option of "overriding" the permission by turning off the location feature on their device entirely. In fact, 59% of Americans who own a smartphone and have downloaded apps had turned off the location tracking feature on their device or turned off the location feature in an app.

But users are not able to override all permissions in this manner. For example, the "read your contacts" permission allows an app to read all of the contact information stored on the device. This permission is used by 64,377 apps (6% of all apps studied here) and cannot be turned off — if a user agrees to allow an app to use this permission, he or she cannot selectively disable this feature (this will change somewhat with Android 6.0).

This distinction adds another layer of complexity to the permissions process and the ability of users to make informed decisions about the apps they download. Even with the system now in place in the newest version of Android, users will not have the ability to control *all* permissions, only a select set. See the section above for more detail on the newest updates to permissions in Android 6.0.

Methods

About the Google Play Store Data Collection

Findings about Google apps permissions in this report are based on an analysis of data about 1,041,336 apps collected from the Google Play Store between June 2014 and September 2014. The data collection or scraping ("scraping" in this case refers to the process of copying the contents of a web page) began with a custom extension for the Google Chrome web browser created by Pew Research Center developers.

When run, the extension would open the Google Play Store website and go to the webpage for an app as designated by a unique app ID number each app in the store receives. It would then copy the content of that app's page, store that information in a SQL database, and move on to the next app in a continual process until no more app ID's were available. The extension engaged in data collection from June 18, 2014 to September 8, 2014.

The initial list of app ID's to search was collected from a site that mirrors the Google Play Store called Androidpit.com (the site no longer mirrors the store as of this publication). As individual apps were scraped, the extension would collect the app ID numbers from the "related" apps listed on each app's page. These "related" app IDs were then added to the initial list of apps to scrape in a sequential process, until eventually there were no new app IDs.. If an app was removed from the Google Pay Store during this process it would return a 404 error and its ID would be removed from the database.

Google Play Apps Scraped by Day

June 18-September 8, 2014

Date	Apps Scraped	Date	Apps Scraped	Date	Apps Scraped	Date	Apps Scraped	Date	Apps Scraped
6/18/2014	9,111	7/8/2014	16,579	7/27/2014	12,181	8/15/2014	14,904	9/3/2014	12,179
6/19/2014	6,585	7/9/2014	13,859	7/28/2014	9,747	8/16/2014	4,048	9/4/2014	3,010
6/20/2014	40,216	7/10/2014	9,521	7/29/2014	22,996	8/17/2014	11,603	9/5/2014	8,409
6/21/2014	21,262	7/11/2014	22,810	7/30/2014	26,842	8/18/2014	9,620	9/6/2014	11,710
6/22/2014	21,918	7/12/2014	11,413	7/31/2014	18,422	8/19/2014	11,807	9/7/2014	17,873
6/23/2014	21,101	7/13/2014	13,434	8/1/2014	15,842	8/20/2014	10,643	9/8/2014	7,135
6/24/2014	8,733	7/14/2014	22,830	8/2/2014	9,509	8/21/2014	8,477		
6/25/2014	18,925	7/15/2014	18,201	8/3/2014	13,266	8/22/2014	28,740		
6/26/2014	2,475	7/16/2014	19,190	8/4/2014	8,264	8/23/2014	15,107		
6/27/2014	2,557	7/17/2014	24,616	8/5/2014	15,256	8/24/2104	18,233		
6/29/2014	4,088	7/18/2014	24,442	8/6/2014	15,545	8/25/2014	13,192		
6/30/2014	7,901	7/19/2014	8,628	8/7/2014	10,934	8/26/2014	14,252		
7/1/2014	10,844	7/20/2014	23,081	8/8/2014	17,915	8/27/2014	3,529		
7/2/2014	14,738	7/21/2014	8,989	8/9/2014	7,182	8/28/2014	6,195		
7/3/2014	8,857	7/22/2014	11,396	8/10/2014	13,440	8/29/2014	7,159		
7/4/2104	8,227	7/23/2014	6,837	8/11/2014	5,206	8/30/2014	6,206		
7/5/2014	4,797	7/24/2014	4,369	8/12/2014	10,112	8/31/2014	6,849		
7/6/2014	7,023	7/25/2014	3,371	8/13/2014	12,034	9/1/2014	12,572		
7/7/2014	6,607	7/26/2014	19,933	8/14/2014	13,742	9/2/2014	9,986		

Source: Google Play Store, June 18-September 8, 2014

PEW RESEARCH CENTER

About the Survey Findings

The Pew Research Center survey findings reported here come from two surveys conducted in 2015. **The overall smartphone ownership number is based on telephone interviews conducted June 10, 2015, through July 12, 2015 among a national sample of 2,001 adults, 18 years of age or older, living in all 50 U.S. states and the District of Columbia.** A total of 701 respondents were interviewed on a landline telephone, and 1,300 were interviewed on a cellphone, including 709 who had no landline telephone. The survey was conducted by interviewers at Princeton Data Source under the direction of Princeton Survey Research Associates International. A combination of landline and cellphone random digit dial samples were used; both samples were provided by Survey Sampling International. Interviews were conducted in English and Spanish. Respondents in the landline sample were selected by

randomly asking for the youngest adult male or female who was at home. Interviews in the cellphone sample were conducted with the person who answered the phone, if that person was 16 years of age or older. For detailed information about our survey methodology, visit: http://www.pewresearch.org/methodology/u-s-survey-research/

The combined landline and cellphone samples are weighted using an iterative technique that matches gender, age, education, race, Hispanic origin and nativity, and region to parameters from the 2013 Census Bureau's American Community Survey and population density to parameters from the Decennial Census. The sample also is weighted to match current patterns of telephone status (landline only, cellphone only or both landline and cellphone), based on extrapolations from the 2014 National Health Interview Survey. The weighting procedure also accounts for the fact that respondents with both landline and cellphones have a greater probability of being included in the combined sample and adjusts for household size among respondents with a landline phone. The margins of error reported and statistical tests of significance are adjusted to account for the survey's design effect, a measure of how much efficiency is lost from the weighting procedures.

Group	Unweighted sample size	Plus or minus...
Total sample	2,001	2.5 percentage points

Findings on apps usage and attitudes in this report are based on a Pew Research Center survey conducted between Jan. 27, 2015, and Feb. 16, 2015, among a sample of 461 adults ages 18 or older. The survey was conducted by the GfK Group using KnowledgePanel, its nationally representative online research panel. GfK selected a representative sample of 1,537 English-speaking panelists to invite to join the subpanel and take the first survey in January 2014. Of the 935 panelists who responded to the invitation (60.8%), 607 agreed to join the subpanel and subsequently completed the first survey (64.9%) whose results were reported in November 2014. This group has agreed to take four online surveys about "current issues, some of which relate to technology" over the course of a year and possibly participate in one or more 45- to 60-minute online focus group chat sessions.

KnowledgePanel members are recruited through probability sampling methods and include both those with internet access and those without. KnowledgePanel provides internet access for those who do not have it and, if needed, a device to access the internet when they join the panel. A combination of random digit dialing (RDD) and address-based sampling (ABS) methodologies have been used to recruit panel members (in 2009 KnowledgePanel switched its sampling methodology for recruiting panel members from RDD to ABS). The panel comprises households

with landlines and cellular phones, including those only with cellphones and those without a phone. Both the RDD and ABS samples were provided by Marketing Systems Group (MSG).

KnowledgePanel continually recruits new panel members throughout the year to offset panel attrition as people leave the panel. Respondents were selected randomly from eligible adult household members of the panel. All sampled members received an initial email on Aug. 5, 2014, to notify them of the survey that included a link to the survey questionnaire. One standard follow-up reminder was sent three days later to those who had not yet responded.

The final sample for this survey was weighted using an iterative technique that matches gender, age, education, race, Hispanic origin, household income, metropolitan area or not, and region to parameters from the March 2013 Census Bureau's Current Population Survey (CPS). In addition, the sample is weighted to match current patterns of internet access from the October 2012 CPS survey. This weight is multiplied by an initial base or sampling weight that corrects for differences in the probability of selection of various segments of the sample and by a panel weight that adjusts for any biases due to nonresponse and noncoverage at the panel recruitment stage (using all of the parameters mentioned above as well as home ownership status).

Sampling errors and statistical tests of significance take into account the effect of weighting at each of these stages. Sampling error for the total sample of 498 respondents is plus or minus 5.6 percentage points at the 95% level of confidence.

Data on smartphone ownership is taken from a nationally representative telephone survey conducted June 10, 2015 through July 12, 2015, among 2,001 American adults age 18+. Data on app downloading and app usage is based on an online survey conducted Jan. 27, 2015 through - Feb. 16, 2015 among 461 Americans age 18+. The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

	Jan. 27-Feb. 16, 2015 survey	
Group	Unweighted sample size	Plus or minus ...
All adults	461	5.8 percentage points
Smartphone owners who have downloaded apps	242	7.2 percentage points

Sample sizes and sampling errors for other subgroups are available upon request. The margins of error reported and statistical tests of significance are adjusted to account for the survey's design effect, a measure of how much efficiency is lost from the weighting procedures.

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls.

Survey Questions

PEW RESEARCH CENTER'S INTERNET PROJECT/GFK PRIVACY PANEL
SURVEY #4 TOPLINE
JANUARY 27-FEBRUARY 16, 2015
TOTAL N=461 ADULTS, AGES 18 AND OLDER
SURVEY CONDUCTED ONLINE
MARGIN OF ERROR FOR ALL ADULTS IS +/- 5.8 PERCENTAGE POINTS

Among smartphone users [n=300]

APP4 Have you ever downloaded any apps yourself, or do you only use the apps that came preloaded with your phone?

77 Yes, have downloaded apps

23 No, have not downloaded apps

0 Refused

Among smartphone owners who have downloaded apps [n=242]

APP1 How many applications or "apps" do you currently have on your cell phone? Just your best guess is fine…

30 1-10

32 11-20

16 21-30

10	31-40
5	41-50
7	More than 50
0	Refused
38	NET More than 20 apps

Among smartphone owners who have downloaded apps [n=242]

APP2a How many of these apps do you use regularly (that is, at least once a week)?

3	None
46	1-5
35	6-10
16	11+
0	Refused

Among smartphone owners who have downloaded apps [n=242]

APP5 When deciding whether or not to download an app, how important is it that…

	Very important	Somewhat important	Not very important	Not at all important	Refused	NET Important	NET Not important
The app has positive ratings and reviews from other users	51	37	8	4	0	88	12
The app has been downloaded a certain number of times	22	36	28	14	<1	57	42
The app provides clear information about how it will access or use your data	59	31	9	1	0	90	10
Someone you know has used the app	17	38	26	18	0	56	44