See No Evil: Loopholes in Google's Data Safety Labels Keep Companies in the Clear and Consumers in the Dark

Project Lead: Jen Caltrider

Lead Researcher: Ali Talip Pınarbaşı

Writer: Anne Stopper

*Privacy Not Included

moz://a

Contents

About Mozilla

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. An internet that truly puts people first, where individuals can shape their own experience and are empowered, safe and independent.

Founded as a community open source project in 1998, Mozilla currently consists of two organizations: the non-profit Mozilla Foundation, which leads our movement building work; and its wholly owned subsidiary, the Mozilla Corporation, which leads our market-based work, including the development of the Firefox web browser. The two organizations work in close concert with each other and a global community of tens of thousands of volunteers under the single banner: Mozilla.foundation.mozilla.org

Executive Summary

Few people stop to question the accuracy of nutrition labels on packaged food. But food labeling wasn't always so trustworthy. Companies found it relatively easy to make false and misleading health claims on food packaging until the U.S. Supreme Court cracked down on the practice in 1973, and the U.S Food and Drug Administration (FDA) didn't introduce its standardized, mandatory "Nutrition Facts" label until 1990. It took three decades from when nutrition labels first appeared on food to when they provided consumers with accurate,

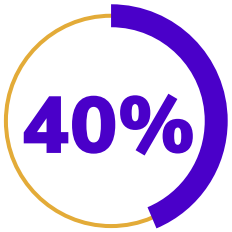
useful information about what they were eating. Today, nutrition labels have become so trusted that they're even required on fast food menus.

When it comes to knowing how online apps use our personal data, consumers are still largely unprotected, similar to the landscape in the early years of nutrition labeling. Mozilla began its *Privacy Not Included project in 2017 to make it easier for consumers to assess the privacy and security features of products that connect to the internet before they make a purchase.

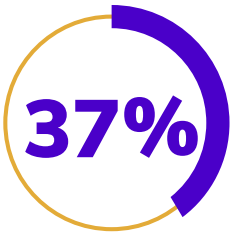
Mozilla's latest research tested Google's new data transparency system, its Play Store's Data Safety Form, to see how well it helped people understand what personal information an app collects and shares. In 2021 alone, Google Play's mobile apps generated $48 billion U.S. dollars in worldwide gross revenue.

When we identified 40 of the Play Store's most popular apps by number of global downloads and compared their privacy policies with the information they reported on Google's Data Safety Form, we found significant discrepancies:

In nearly 80% of the apps we reviewed, we found some discrepancies between the apps' privacy policies and the information they reported on Google's Data Safety Form.



16 out of 40 apps, or 40%, had major discrepancies between their privacy policies and their Data Safety Forms, earning a "Poor" grade.



15 apps, or 37.5%, received our middle grade, "Needs Improvement," which indicated some discrepancies between the privacy policies and the Data Safety Form.

Just 6 of the 40 apps, or 15%, received our "OK" grade, indicating few to no discrepancies between their privacy policies and their Data Safety Form. These apps include Stickman Legends Offline Games, Power Amp Full Version Unlocker, League of Stickman: 2020 Ninja, Google Play Games, Subway Surfers, and Candy Crush Saga.

- The most concerning problems involved the misleading information we found about how apps collect, share, and use data which lead to consumers not having accurate information to make important decisions about their privacy.

Our research also reveals major shortcomings in Google's Data Safety Form itself:

The form includes significant loopholes, like failing to require the apps to report data sharing with "service providers."

Google uses narrow definitions for data "collection" and "sharing," making it easier for app developers to mislead users.

Google also exempts "anonymized" data from its disclosure requirements, which is problematic due to questions about whether true anonymization is even possible.

Google appears to absolve itself of the responsibility to verify the information the apps provide on the form by expecting app developers to be completely honest in their self-reporting. "You alone are responsible for making complete and accurate declarations in your app store's listing on Google Play," the company says in its instructions to app developers.

To address these problems and help users figure out how apps are really using their data before they've downloaded them so they can learn more about privacy and make more informed choices, we've developed the following set of recommendations:

- Google, along with all app stores, should develop and adopt a universal standard app disclosure form that accurately, completely, and clearly describes how app developers use consumers' data.
- Most companies have global privacy policies that apply to all their websites and products, but mobile apps should have their own specific policies, which would increase the accuracy of their disclosures.
- Google, along with other hosting platforms, should be required to state clearly that the information on their data safety disclosures and labels is self-reported by app developers, and that they don't take responsibility for ensuring the veracity of the information.
- Google should regularly review the privacy policies of the apps in its Play Store and provide quarterly public reports about actions taken against those with discrepancies between their policies and the Google Data Safety Form, as well as against those who have failed to complete the form.
- Google should expand its definitions of data "collection" and "sharing" to enhance clarity about how apps are using consumers' data and to help protect users from misleading information. Google should also narrow its definition of "anonymization," or eliminate it for the same reasons.

These recommendations complement and reinforce Mozilla's broader recommendations on data protection and privacy. None of the recommendations require regulatory action, and they can all be undertaken

by companies immediately. However, it's our opinion that systemic and robust changes to protect consumer data privacy need strong regulatory measures and oversight.

Introduction

This report set out to answer two questions:

- Is Google's Data Safety Form effective at enhancing privacy transparency among apps in the Google Play Store?
- How accurately did app publishers in Google's Play Store fill out Google's Data Safety Form?

Overall, there were so many significant discrepancies between the apps' own privacy policies and the information they revealed on Google's Data Safety form that we've concluded the apps aren't self-reporting accurately enough to give the public any meaningful reassurance about the safety and privacy of their data. Further, Google isn't doing enough to ensure the information provided in their Data Safety Form is accurate and informative for consumers. The result is that consumers who want to protect their privacy and trust the information on Google's Data Safety Form are being misled, leading them to believe these apps are doing a better job protecting their privacy than they are.

First, the form: We analyzed the content and structure of Google's Data Safety Form.

The instructions ask the app publishers to provide information on the Data Safety Form about both the **types of data** they use/collect and the **purposes** for which they collect them. Below is an abridged version of that form.

Readers might find the full scope and scale of the information surprising: political/religious beliefs, sexual orientation, financial history including credit score, users' photos and videos, calendar events including attendees, search and browser history, and more.

Examples of Types of Data Included on Google's Data Safety Form

Category	Data Type	Description
Location	Approximate Location	User or device physical location to an area greater than or equal to 3 square kilometers, such as the city a user is in, or location provided by Android's ACCESS_COARSE_LOCATION permission.
	Precise Location	User or device physical location within an area less than 3 square kilometers, such as location provided by Android's ACCESS_FINE_LOCATION permission.
Personal Info	Name	How a user refers to themselves, such as their first or last name, or nickname.
	Email Address	A user's email address.
	User ID's	Identifiers that relate to an identifiable person. For example, an account ID, account number, or account name.

Purposes of Data Included on Google's Data Safety Form

Data Purpose	Description	Example
App functionality	Used for features that are available in the app	To enable app features, or authenticate users.
Analytics	Used to collect data about how users use the app or how it performs	To see how many users are using a particular feature, to monitor app health, to diagnose and fix bugs or crashes, or to make future performance improvements.

In addition to their data collection and sharing practices, Google asks app publishers to provide information about the following:

- The app's security practices (like data encryption)
- Whether the app follows Google's Families Policy
- Whether the app needs this data to function, or if users have a choice in sharing it
- If the app's safety section is verified by an independent third party
- If the app enables users to request data deletion if/when they decide to uninstall

Next, the apps: We split the Google Play Store apps into two categories - paid and free - and studied the 20 most popular apps by the number of global installations in each category. The 20 most popular paid apps had roughly 88 million total installations, and the 20 most popular free apps had an estimated 76 *billion* total installations.

We analyzed each app's own written privacy policy and compared how closely it aligned with the app's answers on Google's Data Safety Form. Then we assigned each app a grade based on how similar the information in the app's privacy policy was to its answers on the Data Safety Form.

Poor	Needs Improvement	OK
Low Similarity between Data Safety Form and Privacy Policy	Some degree of similarity between Data Safety Form and Privacy Policy	High similarity between Data Safety Form and Privacy Policy
Privacy policy and Data Safety Form widely differ in terms of collected data types, data sharing and their relevant purposes.	Privacy policy and Data Safety Form differ to some extent in terms of collected data types, data sharing, and their relevant purposes.	Privacy policy and Data Safety Form are aligned to a great degree with minor differences in terms of collected data types, data sharing and their relevant purposes.

Research Findings

Our findings revealed two main problems - one with the Data Safety Form and Google's confusing and ineffective rules for how companies can provide information, and the other with the app developers' honesty in self-reporting.

- The reporting rules Google imposes for how apps should use its Data Safety Form include complicated terminology and definitions that may allow the apps to exploit loopholes.
- The information app developers provide on the Data Safety form is self-reported, and not closely monitored by Google for accuracy.

Problems With the Data Safety Form

Loopholes and Poor Oversight

Our analysis reveals several serious shortcomings in both the Data Safety Form's content and mechanisms. The form relies mostly on the honor system of self-reporting. App developers fill in the form, without participation or intervention from Google. There's little evidence that Google works diligently to ensure the accuracy of the submissions, and this lack of enforcement renders the quality of

the information very poor in a great many cases.

Google's Data Safety Form uses many terms that are given either overly broad or overly narrow meanings, but which are likely not intuitive to many app users. Many of the apps are games used by minors. Terms like "service provider," "analytics," and "ephemeral processing" are unlikely to carry much meaning for adults who are not industry insiders, let alone for children and teens. We are particularly concerned with the reporting exemptions Google allows for "service providers" and for "specific legal purposes," which are so vague that they amount to huge amounts of data collection and/or sharing that apps aren't required to disclose and that consumers have no way of knowing about.

There are also other terminology traps on the form. Exemptions for "anonymous data" rely on the app developer's judgment of how effective their attempts to anonymize the user's information are, but there is no broad consensus among digital privacy advocates that common techniques to anonymize data are effective.

All of the above suggests that, despite its stated intent, Google's Data Safety Form is not promoting effective transparency in data handling.

We reached out to Google to ask how it handles the review and enforcement of app reporting with the following questions. We've included Google's responses in their entirety.

1. Q: How often does Google review the app disclosure information provided by the app companies on the Google Play Store Data Safety forms for discrepancies between the provided information and the apps' own privacy disclosures? Would it be possible to tell us how many apps Google reviewed for discrepancies in the past year?

A: Google Play's User Data policy requires developers to provide accurate information in their Data safety forms. We work closely with the developer community to ensure they understand the importance of providing accurate information so users can make informed decisions about what apps they use.

2. Q: With as much specificity as possible, what level of breach/discrepancies between an app's own privacy policy and the information it discloses on Google's Data Safety Form constitutes enforcement action on Google's part? Can you give a specific example of a situation that has resulted in an enforcement action, describing both the discrepancy and the enforcement action?

A: Only developers possess all the information required to reflect their data practices accurately in their apps' Data safety section. Developers alone are responsible for making complete and accurate Data safety section disclosures for their apps.

3. Q: What specific enforcement actions has Google taken against any apps in the Google Play Store regarding their Data Safety information within the past year? About how many enforcement actions has Google taken against apps in the past year?

A: If we find that a developer has provided inaccurate information in their Data safety form and is in violation of the policy, we will require the developer to correct the issue to comply. Apps that aren't compliant are subject to enforcement actions.

4. Q: Finally, Mozilla's research found instances where an app failed to complete/submit Google's Data Safety form, but we know the app is still operating in the Play Store. What steps, if any, has Google taken to ensure consistency and fairness in enforcement?

All developers that have an app published on Google Play must complete the Data safety form, including apps on closed, open, or production testing tracks. Developers no longer can publish a new app or an app update if their Data safety form is incomplete or has unaddressed issues. Non-compliant apps may face additional enforcement actions in the future.

Problems With the Apps

Inconsistent Self-Reporting

Top 20 Paid Apps

We graded the 20 most-installed paid apps with the following:

10 apps received our lowest grade, "Poor" - showing the lowest degree of similarity between Google's Data Safety Form and their privacy policies. Three of the top 5 most-installed paid apps - Minecraft, Human Sniper, and Geometry Dash - all also received the lowest grade.

5 apps received the middle grade, "Needs Improvement," exhibiting some discrepancies and some alignment between their privacy policies and the Data Safety Form. Monument Valley and The Room were among the apps with middle grades.

Only 3 of the top 20 paid apps qualified for our highest grade, "OK," having revealed close alignment between their privacy policies and their Data Safety Forms. Stickman Legends Offline Games, Power Amp Full Version Unlocker, and League of Stickman: 2020 Ninja were the best-graded apps in this category.

We didn't rate one paid app, "League of Stickman Best acti," due to its failure to fill out the Data Safety Form. We didn't rate another one, Terraria, because its own privacy policy doesn't include any information about data sharing or collection, so we were not able to compare it against Terraria's answers on the Data Safety Form.

Grading Table for Top 20 Paid Apps

Poor	Needs Improvement	OK	Not Graded
Minecraft	Shadow of Death: Dark Night	Stickman Legends Offline Games	League of Stickman Acti
Hitman Sniper	Bloons TD 6	Power Amp Full Version Unlocker	Terraria
Geometry Dash	The Room	League of Stickman: 2020 Ninja	
Evertale	Modern Combat 4: Zero Hour		
True Skate	Monument Valley		
Live or Die: Survival Pro			
Grand Theft Auto: San Andreas			
The Room Two			
Need for Speed: Most Wanted			
Nova Launcher Prime			

Minecraft is one of the most popular of the top 20 paid apps, with at least 10 million installations at the time of this research. This app only provides a link to its parent company - Microsoft's - privacy statement, which has no specific information about Minecraft's data use and privacy practices, so users have no way of knowing how the app itself treats their data.

We gave Minecraft our lowest rating due to both the number and severity of the discrepancies between its privacy policy - as non-specific as it is - and the information it revealed on the Data Safety Form. Its privacy policy explains how it collects and uses consumers' purchase history data, but it omits this information from its Data Safety Form. On the form, it declares it does not share any data, but in its policy, it states it shares personal data among Microsoft-controlled affiliates and subsidiaries, as well as some other vendors or agents. Minecraft also completely failed to disclose that it shares users' payment data for fraud prevention on the Data Safety Form, which is included in its privacy statement.

Top 20 Free Apps

Overall, the top 20 free apps fared better in our grading system than the top 20 paid apps. On data collection in particular, the majority of the free apps' privacy policies and Google's Data Safety Form disclosures are aligned.

We graded the 20 most popular free apps with the following:

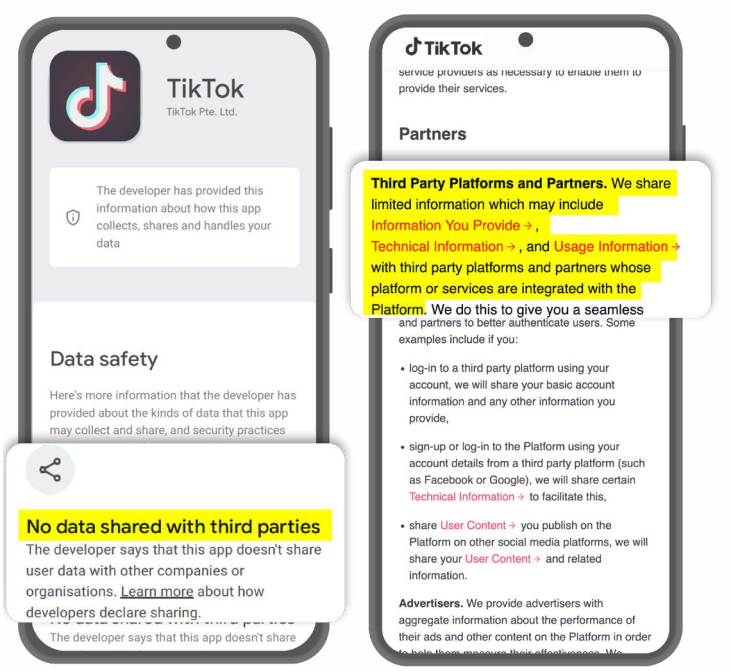
- 6 apps received our lowest grade, "Poor," as they demonstrated the lowest degree of similarity between Google's Data Safety Form and their privacy policies. These apps include Facebook, Messenger, Snapchat, and Twitter.
- 10 apps received our middle grade, "Needs Improvement," as they exhibited some discrepancies and some alignment, including YouTube, Gmail, Google Maps, and Instagram.
- 3 apps received our best grade, "OK." These apps were Google Play Games, Subway Surfers, andCandy Crush Saga. We didn't grade one app, UC Browser Safe, Fast, Private, because it didn't fill out the form.

Grading Table for Top 20 Free Apps

Poor	Needs Improvement	OK	Not Graded
Facebook	Youtube	Google Play Games	UC Browser - Safe, Fast,Private
Messenger	Google Chrome: Fast Secure	Subway Surfers	
Samsung Push Services	Google Maps	Candy Crush Saga	
SnapChat	Gmail		
Facebook Lite	WhatsApp Messenger		
Twitter	Instagram		
	Free Fire		
	TikTok		
	Spotify		
	Truecaller: Caller ID & Block.		

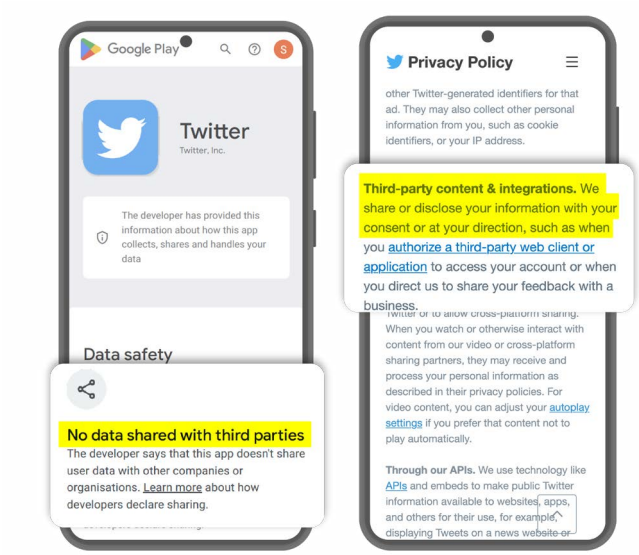
The free apps fared worse than the paid ones in accurately reporting their data-sharing policies. For instance, Snapchat, which earned a “poor” grade, says on its Data Safety Form that it doesn’t share any personal users’ data with third parties, but its privacy policy says it may share users’ data with “integrated third parties,” including third-party games in Chat and third-party Snap Kit integrations, and it states that it isn’t responsible for how they collect or use consumer data. Although Google’s own reporting rules make it optional for apps to disclose data sharing with a service provider, that exemption does not apply here, as there is no claim that the sharing of data to “integrated third parties” is for “provision of service.” For Google’s purposes on its Data Safety Form, a service provider is an agency that provides some form of service based on consumers’ data for use by the app developer. Many different companies act as service providers, including Google itself, which provides services like Google Analytics, Google Translate, and many others.

Another of the most popular and recognizable free apps, TikTok, earned our middle grade - “Needs Improvement” - largely for failing to disclose its data sharing practices. TikTok’s Data Safety Form says it doesn’t share data with third parties, but its privacy policy provides a list of third parties it does share data with, including “third party integration partners,” and third-party platforms like Facebook and Google. TikTok’s privacy policy also says it may share consumers’ personal data with advertisers and creators based on TikTok’s legitimate interests, without consumers’ prior consent. If consumers create content on TikTok, the app’s policy says it can share that content and related information on other social media platforms, but it doesn’t report this usage on the Data Safety Form.



Left: Tikok Data Safety Form | Right: TikTok Privacy Policy

Likewise, Twitter’s privacy policy says it shares personal data from users’ tweets with advertisers, third-party content and integrations, APIs, and “partners” it says help it operate Twitter’s products and services, but Twitter reports none of these practices on Google’s Data Safety form.



Left: Twitter Data Safety Form | Right: Twitter Privacy Policy

We also note that some of the most popular free apps from companies that are household names - like Spotify and Google's own "Google Play Games" app - have privacy policies that were either mostly or completely aligned with their disclosures on the Data Safety Form, reminding us that not all app developers are in a race to the bottom in terms of privacy practices.

Recommendations

Our research revealed major discrepancies between the information in app developers' privacy policies and the disclosures they made about data collection, use, and sharing on Google's Data Safety Form. It also revealed flaws in Google's Data Safety Form itself. Our first two recommendations address potential improvements across the wider tech industry in terms of strengthening the accuracy of data privacy disclosures and enforcement, while our last two recommendations are specific to Google's Data Safety Form and its Play Store Apps.

Our research closely mirrors the 2021 Washington Post investigation into the accuracy of the Apple App Store's new data privacy labels for apps. The investigation found that not only were many of the labels confusing and incomplete - they were also false. Like Google's system, Apple's apps were self-reporting on an honor system, and Apple also included a similar disclaimer on its labels noting that it hadn't verified the information the apps provided there. Both of these cases point to a clear problem with platforms and companies policing themselves, and with the apps' reporting. To that end, our recommendations follow:

1. Universal Standard App Disclosure: Platforms should adopt a universal data privacy disclosure form that accurately, completely, and clearly describes how app developers use consumers' data. This disclosure form could be either an industry-driven or regulatory initiative.

Collectively, the Google Play Store apps' data privacy disclosures, the Apple App Store's App Privacy Labels, and many other individual companies' piecemeal efforts to improve users' understanding and control of data privacy have fallen short. We propose drafting and implementing a universal standard app disclosure form - akin to the FDA's familiar "Nutrition Facts" labels for food - that all app developers would be required to complete. When app developers fail to complete the form or when their completed forms

reveal major discrepancies between it and their own privacy policies, platform owners should take enforcement action, including removing the apps from their stores and sites.

There's some momentum around the idea of shoring up regulatory review and power, as evidenced in President Biden's recent Wall Street Journal op-ed calling on congress to pass legislation on data privacy, safety, and competition. CNBC cited Biden's op-ed as a sign that legislation imposing guardrails on the tech industry "may be a rare area of hope for progress while working across the aisle." Additionally, a new Commerce Department report cited Apple and Google as "gatekeepers" of mobile app stores, leaving consumers at the mercy of their pricing and selection. The report calls for new legislation that would boost competition in the mobile app market, which would help both consumers and app developers.

2. App-Specific Privacy Policy Requirement: Platforms should require mobile apps to have their own specific policies, which would increase the accuracy of their disclosures.

With a few exceptions, none of the mobile apps we reviewed had a separate privacy policy dedicated to the specific mobile app in the Google Play Store. Most mobile app developers have a global privacy policy that applies to all their business operations, websites, and mobile apps. But there are significant differences between how websites and mobile apps operate. Requiring app developers to draft app-specific policies would force them to explain what types of personal data are collected via the app, what third-party tools are used, and for what purposes the data is collected/shared, ultimately improving users' understanding of the full picture of how each app uses their data.

3. Clearer Language About Disclosure Responsibility and Limitations: Google and other tech companies that own platforms hosting apps should state clearly that the information on their data safety disclosures and labels is self-reported by app developers, and that the companies who own the platforms are not responsible for vetting the information for accuracy.

Both Google and Apple include information on their Data Safety Form and App Store labels, respectively, noting that they aren't responsible for vetting the information the apps report about how they handle consumers' data. Apple includes a disclaimer in small print on each app's detail page that reads "This information has not been verified by Apple," which is easy to miss. As we noted earlier, Google includes language on its Data Safety Form that reads "Google Play reviews apps across all policy requirements; however, we cannot make determinations on behalf of the developers of how they handle user data." These statements amount to the tech giants' absolving themselves of responsibility to ensure the information on their own disclosures is accurate, but they owe it to consumers to be more forthcoming about their own role - or lack thereof - in the vetting process.

We don't recommend that consumers trust the information on these labels and disclosures. We could recommend that consumers do their own research into apps' privacy policies, but we acknowledge how daunting this is because of the technical language, length, changing nature, and other aspects of these policies. We do think Google, Apple, and other platform hosts should put prominent and clear disclaimers - in plain language - in these places stating that the information is self-reported by the apps and not vetted by the platform hosts.

4. Regular Compliance Reviews and Public Reports on Enforcement: Google should conduct regular reviews of the apps in its Play Store, releasing quarterly public reports on its findings and specific enforcement actions.

Google's instructions to app developers filling out its Data Safety Form says the following: "When Google becomes aware of a discrepancy between your app behavior and your declaration, we may take appropriate action, including enforcement action." Several app developers have reported that their apps were rejected for inclusion in the Play Store due to problems with their Data Safety Forms. But our own research revealed that there are currently other apps operating in the store that have failed to fill out the form, which leads us to conclude that Google's enforcement is inconsistent. Further, Google's answers to our questions above lacked specific details about its compliance and enforcement efforts.

With this report, we're offering Google many examples of discrepancies between apps' behavior and their declarations. We hope now that Google is aware of the discrepancies, it will review the apps and take appropriate enforcement action, if necessary, following its own policy.

> ***Overall, there were so many significant discrepancies between the apps' own privacy policies and the information they revealed on Google's Data Safety form that we've concluded the apps aren't self-reporting accurately enough to give the public any meaningful reassurance about the safety and privacy of their data.***

Releasing quarterly public reports of their review and enforcement actions would bolster transparency and public confidence in Google's efforts, and would help hold it accountable for applying its policies consistently and fairly across the board for apps in its Play Store.

5. Expand Some Definitions on the Data Safety Form and Restrict or Eliminate Others: Broadening its definitions of "collection" and "sharing," and restricting or eliminating its definition of "anonymized" data would make it harder for apps to fill out the Data Safety Form with misleading information and exploit loopholes. Removing exemptions for reporting data sharing with "service providers" would also strengthen consumer protections.

Google provides exemptions for certain data collection and data sharing activities. But allowing these exemptions heightens the risk that apps can mislead users. As we've noted, data sharing with "service providers" is exempt from disclosure requirements. Google could close some of its loopholes in this area by requiring disclosures for user information that the app never accesses itself, but that a third-party service provider like PayPal or Google Pay accesses. Additionally, Google should introduce much stricter requirements for defining "service providers," considering the potential privacy risks to users.

In a similar vein, Google should interpret "anonymization" very narrowly, or, better yet, eliminate it altogether. Anonymized data is exempt from disclosure requirements, and Google should be doing much more to make sure that the apps in its Play Store can't evade their disclosure requirements by claiming that data is anonymized. As industry experts and analysts have noted, it can be nearly impossible to truly anonymize data, and Scientific American concluded, based on a 2019 study, that consumers can't rely on anonymized data to conceal their identities. Google's changing its definitions of "collection," "sharing," and "anonymization" on its Data Safety Form would significantly help strengthen consumer protections.

Conclusion

The history of standardized nutrition labeling in the U.S. demonstrates that meaningful changes - the kind that becomes part of the cultural fabric and makes a positive difference in people's daily lives - often take a long time. But if the FDA eventually managed to create, implement, and enforce a standardized labeling system for something as complicated and varied as packaged foods, there's hope that we'll also reach a point when tech companies provide clear, honest, and comprehensive data privacy information to consumers.

The responsibility lies with three parties - Google, app developers, and consumers - to create a safe data privacy environment. Within the scope of our research, we believe that Google and app developers share the blame for the failure to improve data privacy

transparency in Google's Play Store.

But the responsibilities of each are not the same. Both Google and app developers have a role to play in ensuring that accurate and actionable information gets to consumers so that users can make informed choices. In this respect, both Google and app developers could do better. Google has an additional responsibility as the host of the Play Store to ensure that bad actors aren't permitted to flourish at the expense of the consumer, many of whom are from vulnerable populations, like young people. App developers often obfuscate or deflect on privacy disclosures, possibly with a profit motive. Google, who also has a profit motive, has not devoted the resources necessary to counter the threat.

We believe that Google's Data Safety Form, though flawed, is at least a first step towards better data privacy disclosures for consumers. Implementing our recommendations for Google's revisions to its Data Safety Form, combined with an increased level of accuracy and honesty in the apps' self-reporting, will significantly improve data privacy and transparency for Google Play Store's app users. Finally, creating and enforcing an effective universal standard app disclosure form across the tech industry, as we've recommended, would add a significant layer of protection for the public in helping people protect their own data.

Methodology

We began our analysis of Google's Data Safety Form on September 11, 2022, and concluded it on November 5, 2022.

We identified the top 20 most popular paid and unpaid apps in the Google Play Store by the number of total installations to select our sample set. We analyzed each selected app's individual data privacy policy and compared it to the information the app disclosed on Google's Data Safety Form, compiling discrepancies between the two for each app where and when we discovered them.

For grading the apps, we used the following three criteria:

- Are there discrepancies between the privacy policy and Google's Data Safety Form in terms of the types of personal data collected?
- Are there discrepancies between the privacy policy and Google's Data Safety Form in terms of the purposes for which data is collected and/or shared?
- Are there discrepancies between the privacy policy and Google's Data Safety Form in terms of types of personal data shared with third parties?

Assigning the Grades

1. Apps received our "Poor" score due to one of the following:

Having major discrepancies in terms of at least two of the following:

- Types of data collected
- Types of data shared
- Purposes for collection/sharing of data

And/or

Demonstrating severe failures to disclose the sharing of personal data for advertising, personalization, analytics, and/or marketing purposes.

2. Apps received our "Needs Improvement" score based on the following:

There were certain discrepancies between the apps' privacy policies and their disclosures on the Data Safety Form. However, these discrepancies were fewer and less severe compared to the apps in the "Poor" category.

These apps did not receive an "OK" grade because there were still multiple discrepancies that were severe to some extent.

3. Apps received our "OK" score based on the following:

These apps had few discrepancies, and their privacy policy largely aligned with disclosures made on the Data Safety Form. However, there were still minor discrepancies in terms of the types of data collected and shared and the purposes thereof.

For example, an app may have been transparent as to what types of data it shared and for which purposes, but it missed out on a few data types and how they can be used for product improvement purposes.

We also identified and explained potential problems with the Data Safety Form itself, including unclear or disputed definitions of key terms.

Acknowledgements

Project Lead:
Jen Caltrider

Lead Researcher:
Ali Talip Pınarbaşı

Writer:
Anne Stopper

***Privacy Not Included**
moz://a