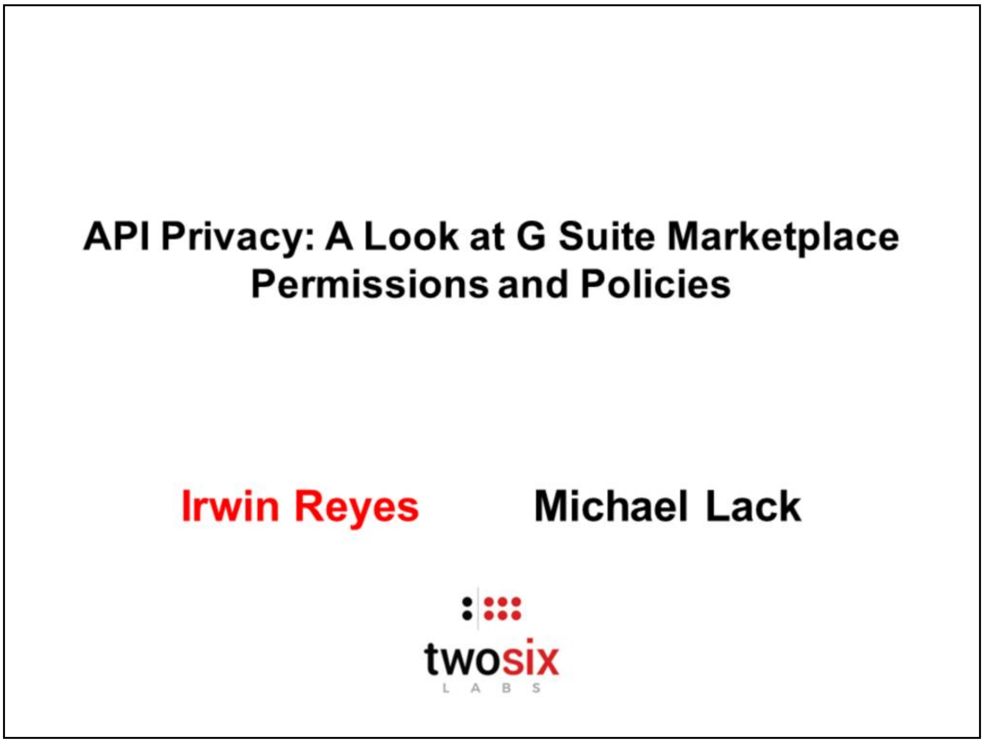
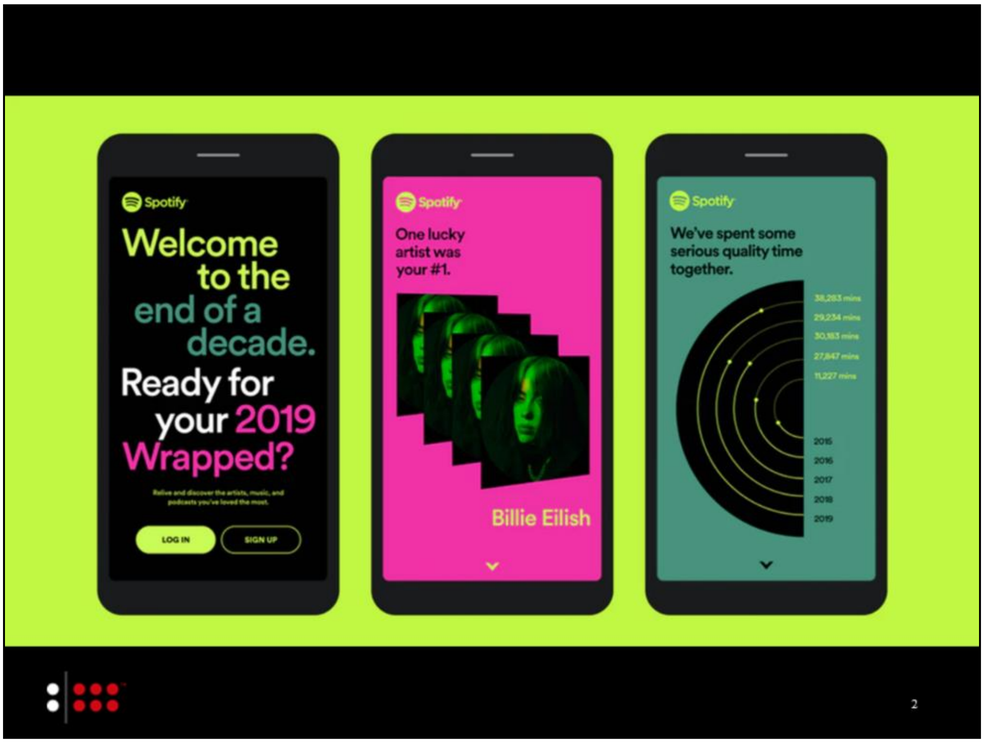


API Privacy: A Look at G Suite Marketplace Permissions and Policies

Irwin Reyes Michael Lack

twosix
LABS



Spotify

Welcome to the end of a decade. Ready for your 2019 Wrapped?

Relive and discover the artists, music, and podcasts you've loved the most.

Spotify

One lucky artist was your #1.

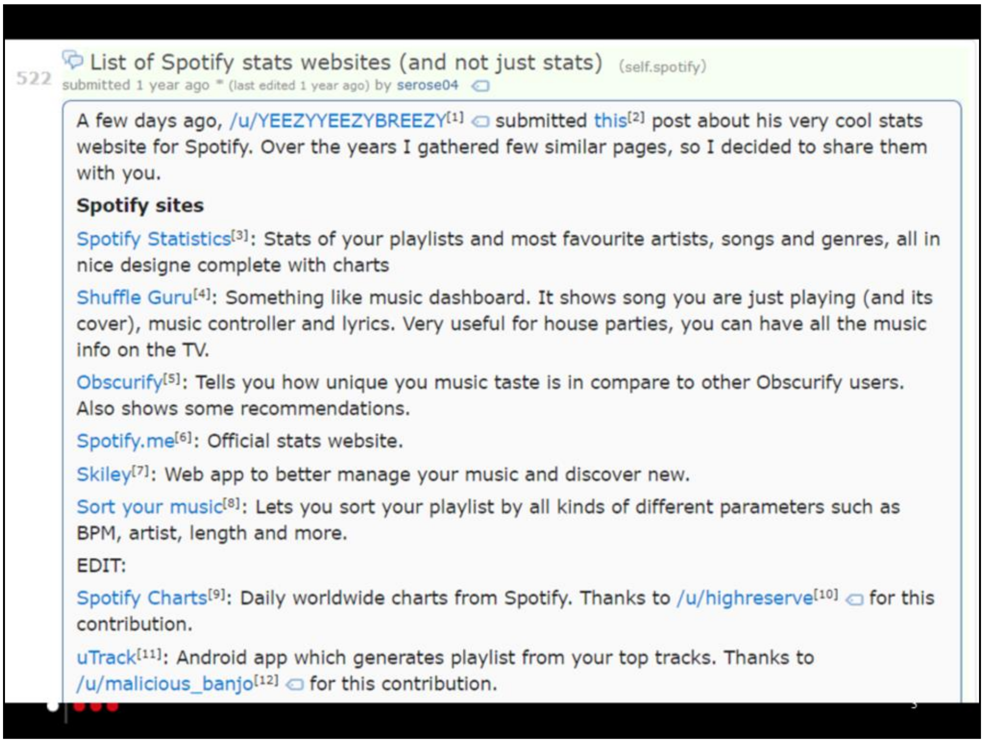
Billie Eilish

Spotify

We've spent some serious quality time together.

The story actually begins with Spotify. A popular streaming service.

At the end of 2019, they released Spotify Wrapped: Statistics about your listening habits over the course of the year.



522 List of Spotify stats websites (and not just stats) (self.spotify)
submitted 1 year ago * (last edited 1 year ago) by serose04

A few days ago, /u/YEEZYYEEZYBREEZY[1] submitted this[2] post about his very cool stats website for Spotify. Over the years I gathered few similar pages, so I decided to share them with you.

Spotify sites

Spotify Statistics[3]: Stats of your playlists and most favourite artists, songs and genres, all in nice designe complete with charts

Shuffle Guru[4]: Something like music dashboard. It shows song you are just playing (and its cover), music controller and lyrics. Very useful for house parties, you can have all the music info on the TV.

Obscurify[5]: Tells you how unique you music taste is in compare to other Obscurify users. Also shows some recommendations.

Spotify.me[6]: Official stats website.

Skiley[7]: Web app to better manage your music and discover new.

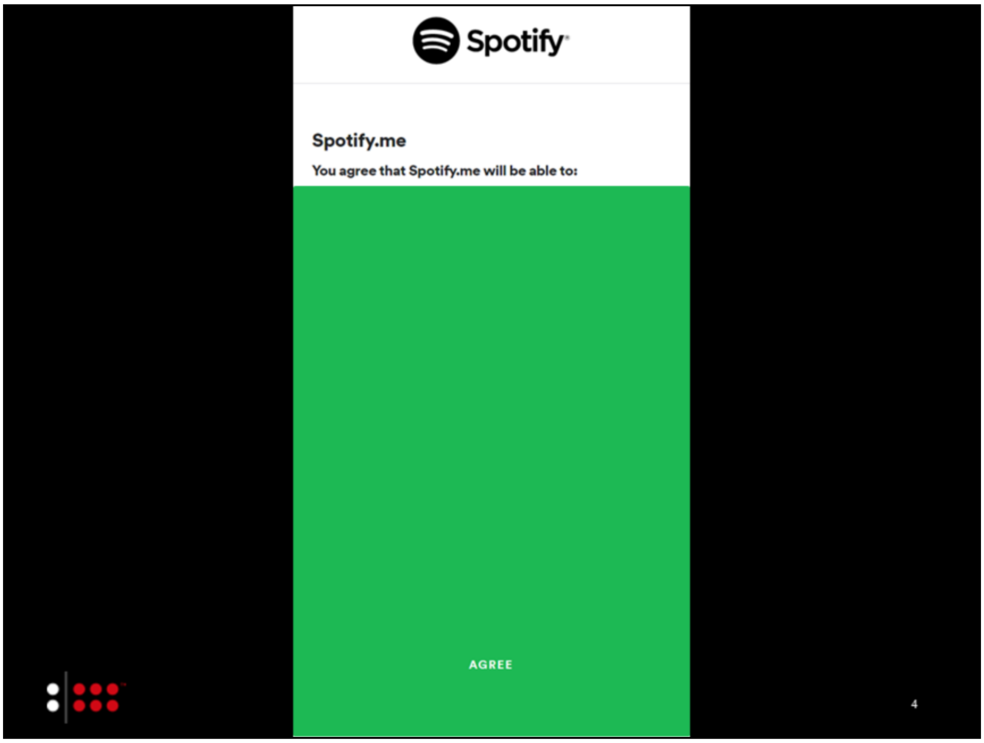
Sort your music[8]: Lets you sort your playlist by all kinds of different parameters such as BPM, artist, length and more.

EDIT:

Spotify Charts[9]: Daily worldwide charts from Spotify. Thanks to /u/highreserve[10] for this contribution.

uTrack[11]: Android app which generates playlist from your top tracks. Thanks to /u/malicious_banjo[12] for this contribution.

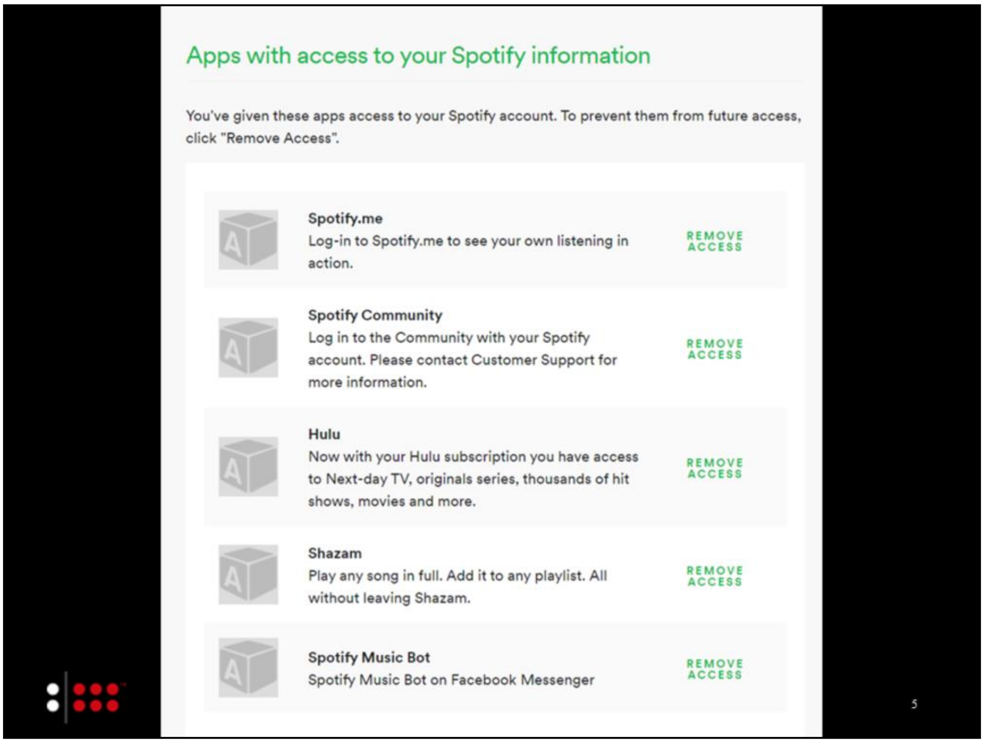
I thought this was really cool, and wanted more. Found a reddit post about other Spotify stats services. Nice!



Spotify.me

You agree that Spotify.me will be able to:

Of course I decided to install these services. By “install,” I mean consent to whatever terms and permissions this nag screen showed.



Apps with access to your Spotify information

You've given these apps access to your Spotify account. To prevent them from future access, click "Remove Access".

Spotify.me
Log-in to Spotify.me to see your own listening in action.
REMOVE ACCESS

Spotify Community
Log in to the Community with your Spotify account. Please contact Customer Support for more information.
REMOVE ACCESS

Hulu
Now with your Hulu subscription you have access to Next-day TV, originals series, thousands of hit shows, movies and more.
REMOVE ACCESS

Shazam
Play any song in full. Add it to any playlist. All without leaving Shazam.
REMOVE ACCESS

Spotify Music Bot
Spotify Music Bot on Facebook Messenger
REMOVE ACCESS

5

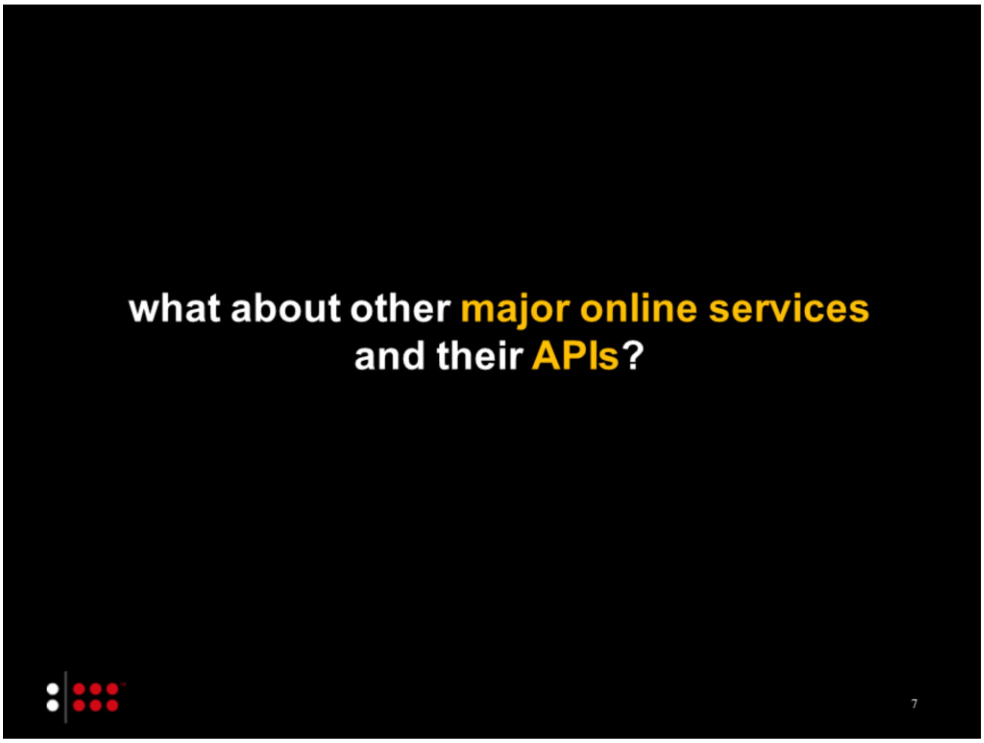
Before long, I realized I just granted a whole bunch of these things programmatic access to my Spotify account via the Spotify application programming interface (API).

But this is small potatoes. Who cares if external services can read my Spotify data? What’s the worst that could happen?

Well, this was the same mechanism that resulted in Mr. Zuckerberg being hauled in front of Congress in 2018.

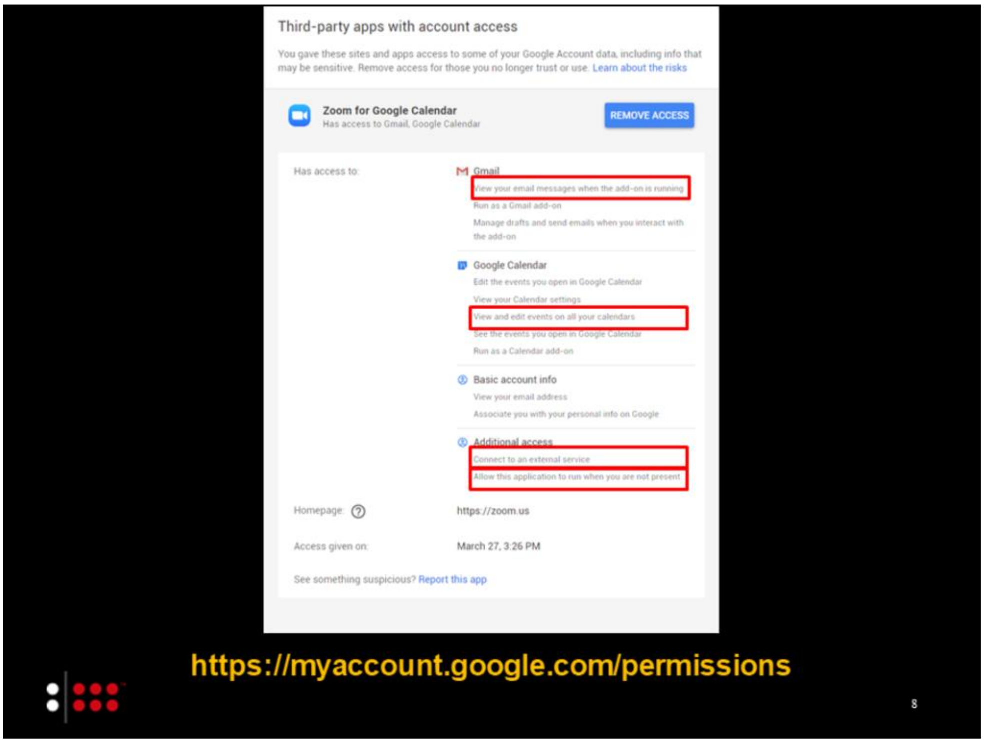
A researcher had written a quiz app that obtained programmatic access to people's Facebook data. The scope of that access was far broader than people expected (it collected data from quiz app users *and* their friends), and was later used in targeted political advertising. This was the Cambridge Analytica scandal.

Facebook eventually placed additional restrictions and safeguards on apps using the Facebook API. Limits on what personal data third-party apps can access, and authorizations expiring if the user hasn't used an app for a while.



what about other **major online services** and their **APIs**?

This got me thinking: Have other major online services placed similar safeguards on their APIs?



Third-party apps with account access

You gave these sites and apps access to some of your Google Account data, including info that may be sensitive. Remove access for those you no longer trust or use. Learn about the risks

Zoom for Google Calendar
Has access to Gmail, Google Calendar

Has access to:

Gmail
- View your email messages when the add-on is running
- Run as a Gmail add-on
- Manage drafts and send emails when you interact with the add-on

Google Calendar
- Edit the events you open in Google Calendar
- View your Calendar settings
- View and edit events on all your calendars
- See the events you open in Google Calendar
- Run as a Calendar add-on

Basic account info
- View your email address
- Associate you with your personal info on Google

Additional access
- Connect to an external service
- Allow this application to run when you are not present

Homepage: https://zoom.us

Access given on: March 27, 3:26 PM

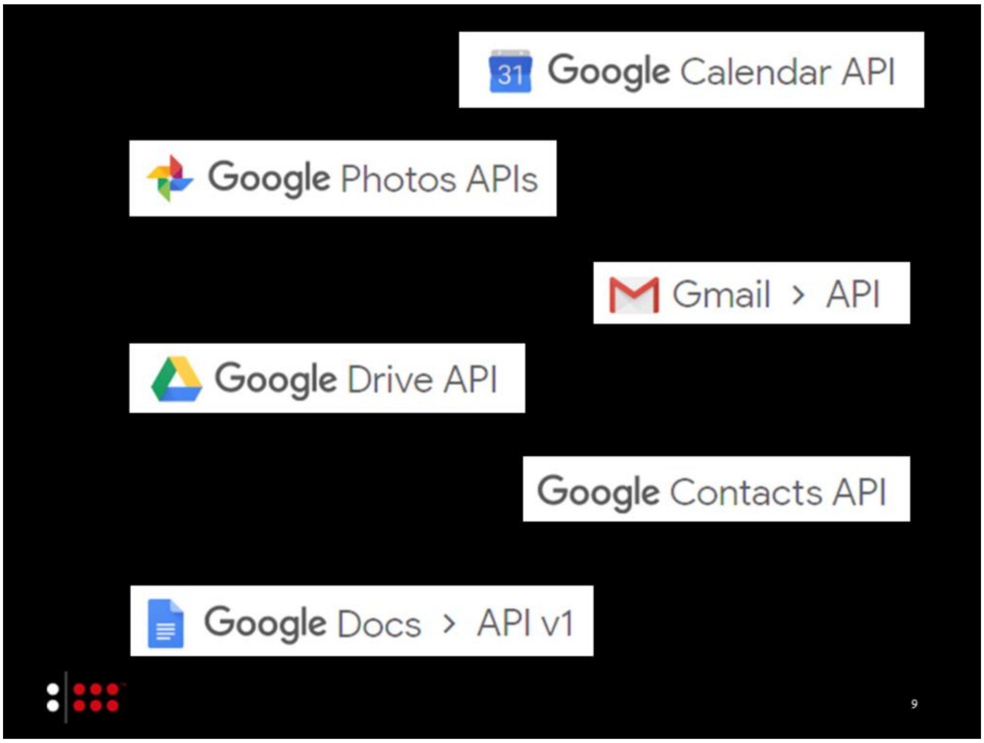
See something suspicious? Report this app

https://myaccount.google.com/permissions

8

Looked at company Google account. We use Zoom a lot internally, and my account automatically had Zoom integration authorized.

Some interesting permissions.



Google Calendar API

Google Photos APIs

Gmail › API

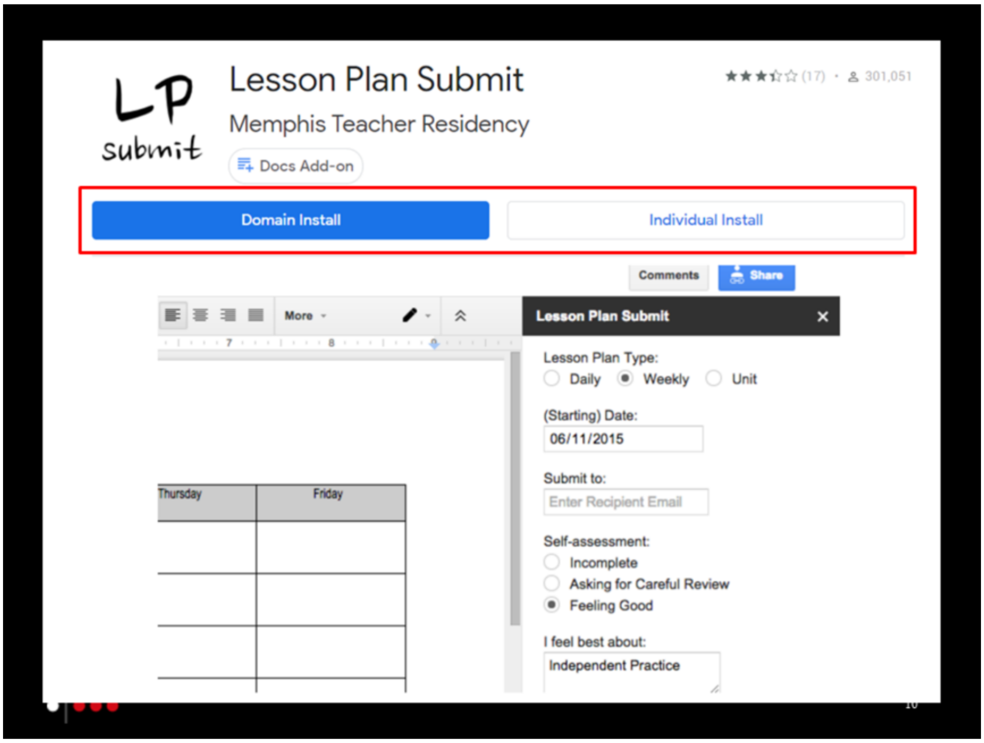
Google Drive API

Google Contacts API

Google Docs › API v1

Google offers a large number of APIs, that give third-party software programmatic access to private user data.

This is just a small sample.



Lesson Plan Submit ×

Lesson Plan Type: ○ Daily ● Weekly ○ Unit

(Starting) Date: 06/11/2015

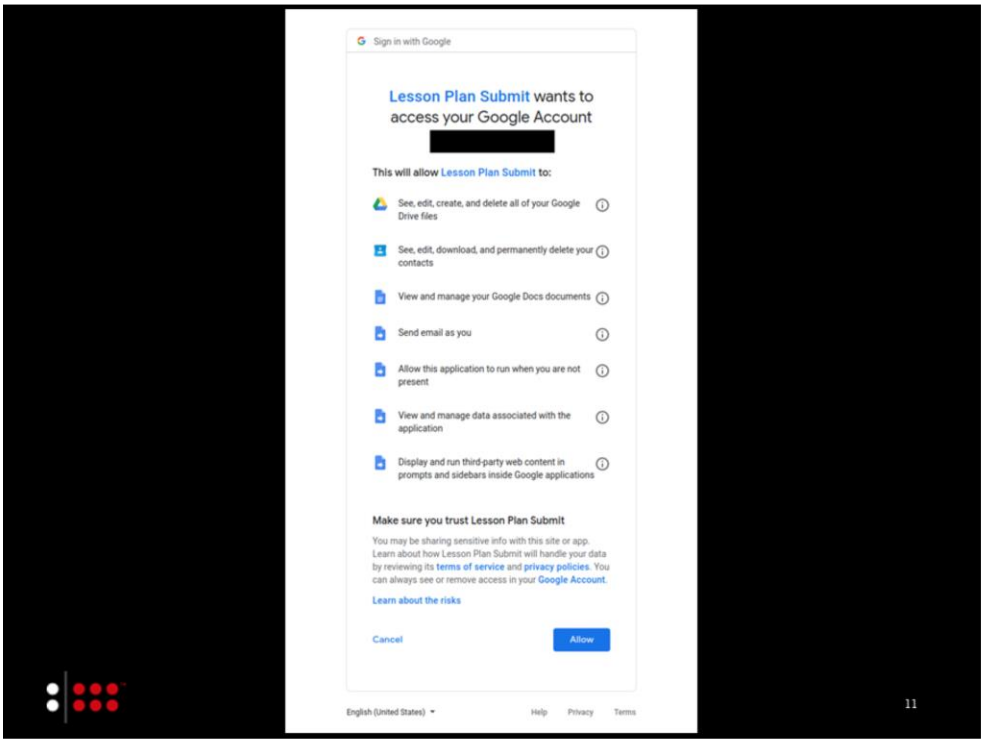
Submit to: Enter Recipient Email

Self-assessment:
○ Incomplete
○ Asking for Careful Review
● Feeling Good

I feel best about: Independent Practice

Google uses OAuth to allow users to authorize third-party software to access their private data held on Google servers.

If I want to authorize an app, I have to be logged into Google, find where the app is being offered, then install it onto my account.



Lesson Plan Submit wants to access your Google Account

[redacted]

This will allow Lesson Plan Submit to:

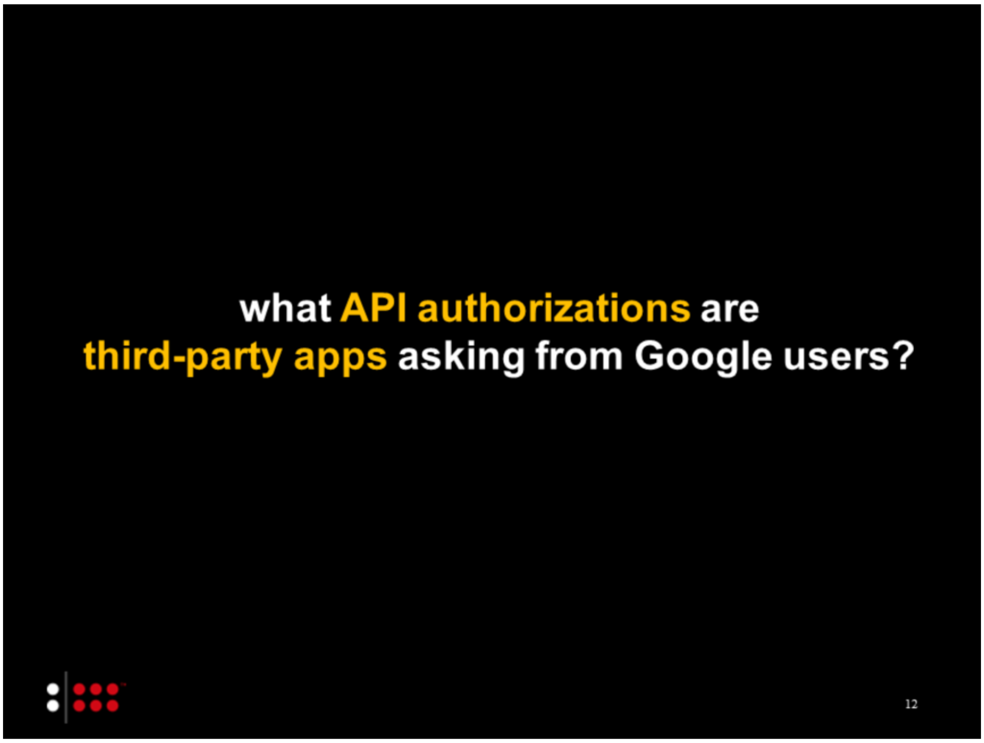
- See, edit, create, and delete all of your Google Drive files
- See, edit, download, and permanently delete your contacts
- View and manage your Google Docs documents
- Send email as you
- Allow this application to run when you are not present
- View and manage data associated with the application
- Display and run third-party web content in prompts and sidebars inside Google applications

Make sure you trust Lesson Plan Submit

You may be sharing sensitive info with this site or app. Learn about how Lesson Plan Submit will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

The app installation process will notify me of the app’s API permissions and ask for my permission.

This screen is generated by Google, and is standard for all apps that ask for authorization for user data. Same prompt for web apps, mobile apps, Slack addons, etc.

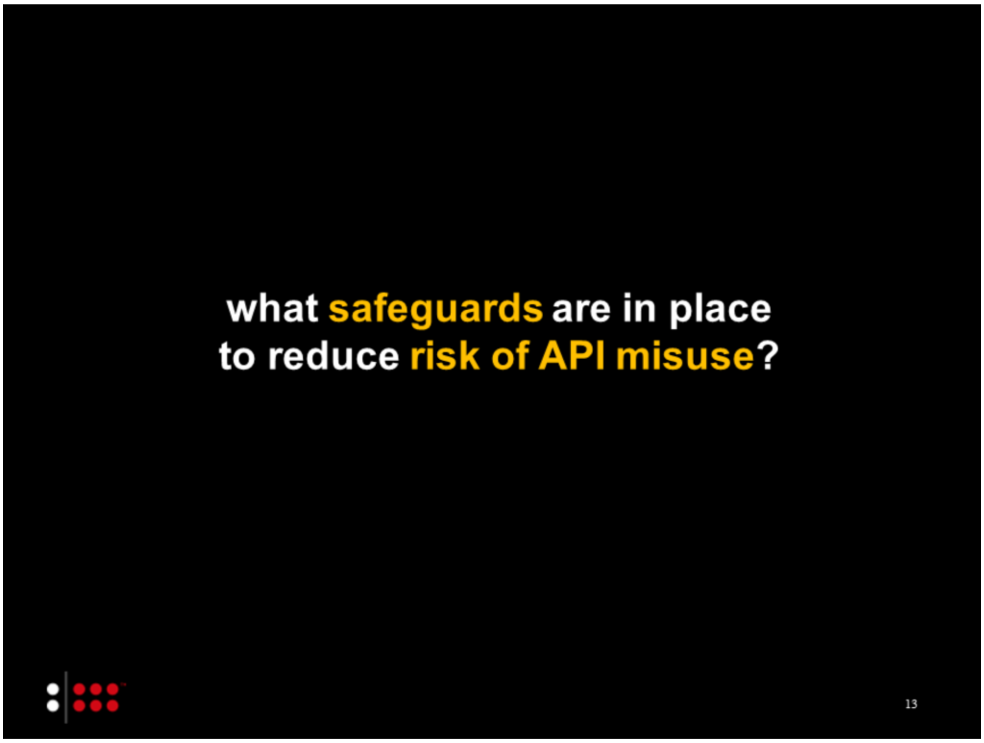


what API authorizations are third-party apps asking from Google users?

12

There’s a whole ecosystem of software products that request access to Google user data. Totally legitimate purposes, like email apps, Slack bots, document editors that save to Google Drive, etc.

Got me thinking about research questions though.

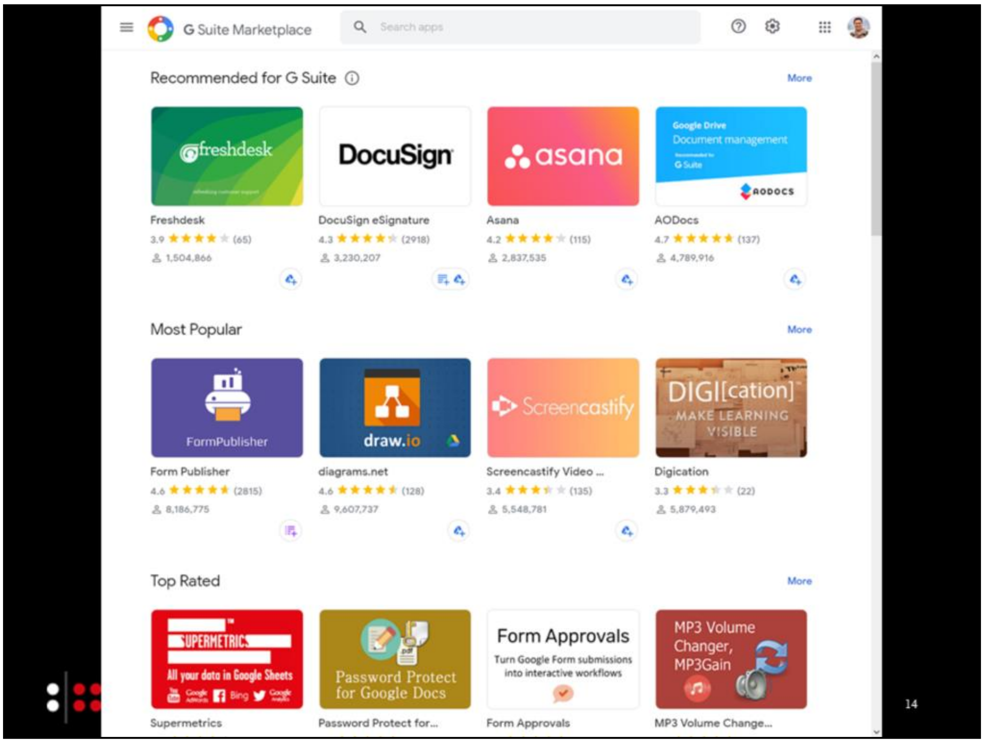


what **safeguards** are in place
to reduce **risk of API misuse**?

13

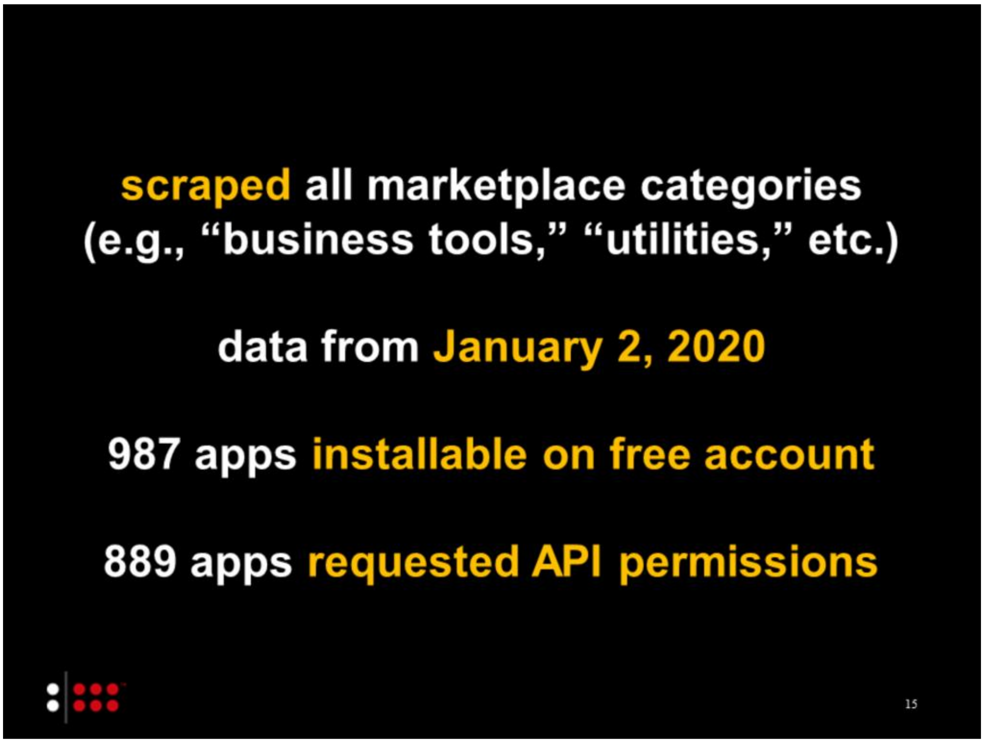
There’s a whole ecosystem of software products that request access to Google user data. Totally legitimate purposes, like email apps, Slack bots, document editors that save to Google Drive, etc.

Got me thinking about research questions though.



The G Suite Marketplace is a convenient centralized repository of web apps that integrate with Google APIs

Mostly business and productivity focused.



scraped all marketplace categories (e.g., “business tools,” “utilities,” etc.)

data from January 2, 2020

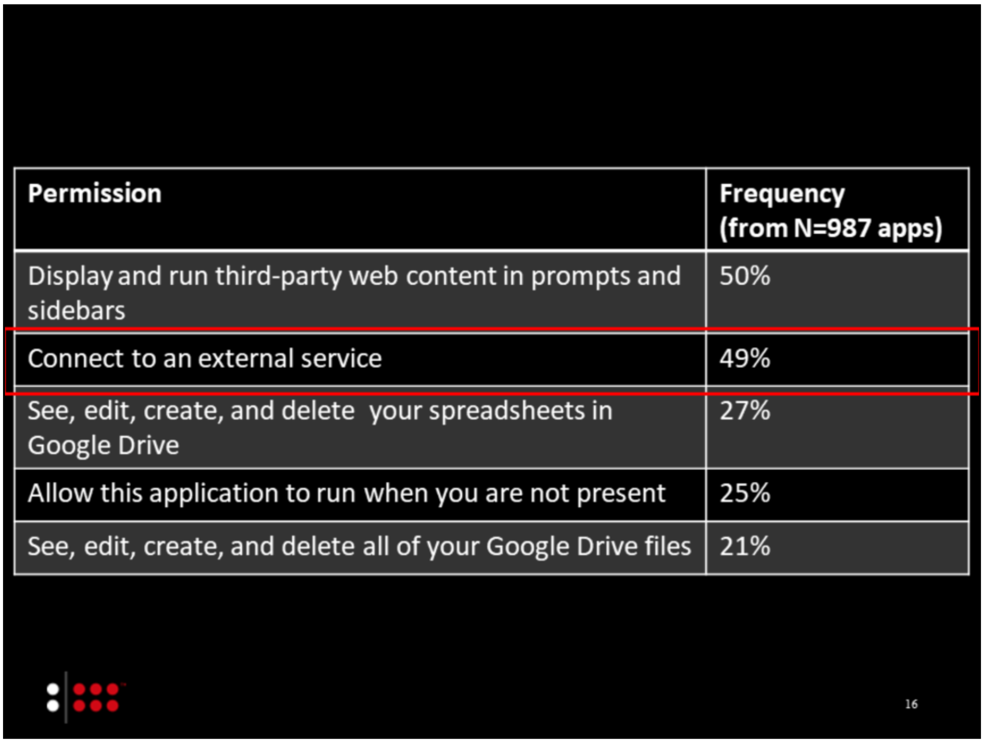
987 apps installable on free account

889 apps requested API permissions

15

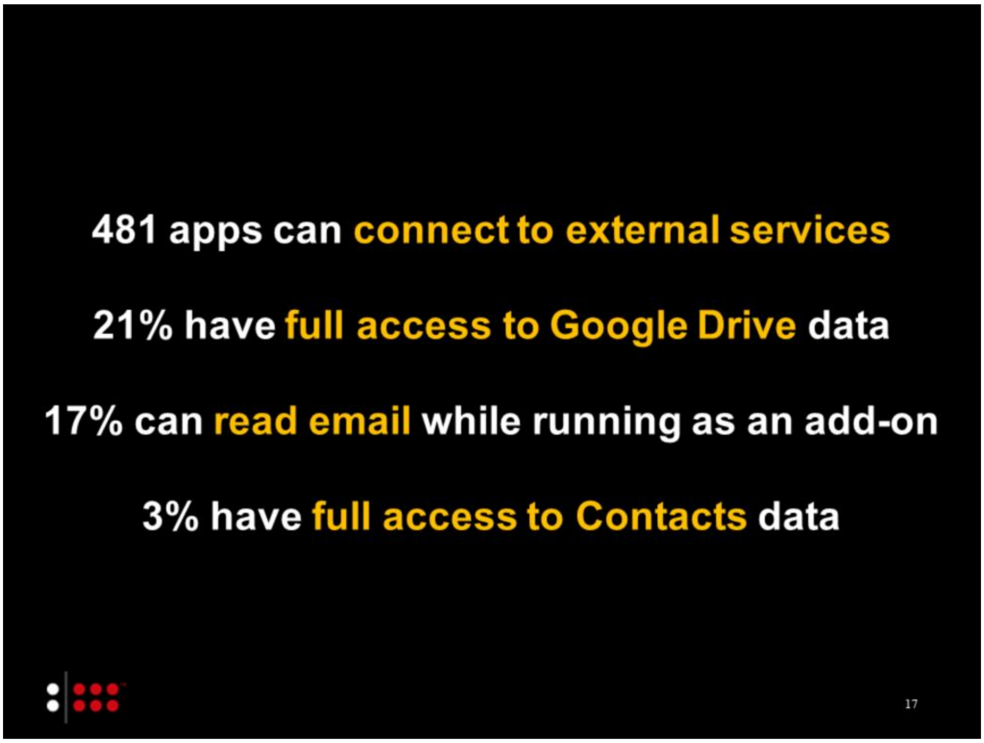
Scraped the G Suite marketplace.

Corpus of 987 installable apps. Some apps were only installable on proper G Suite accounts with admins (i.e., organizations)



Permission	Frequency (from N=987 apps)
Display and run third-party web content in prompts and sidebars	50%
Connect to an external service	49%
See, edit, create, and delete your spreadsheets in Google Drive	27%
Allow this application to run when you are not present	25%
See, edit, create, and delete all of your Google Drive files	21%

Most common permissions requested



481 apps can **connect to external services**

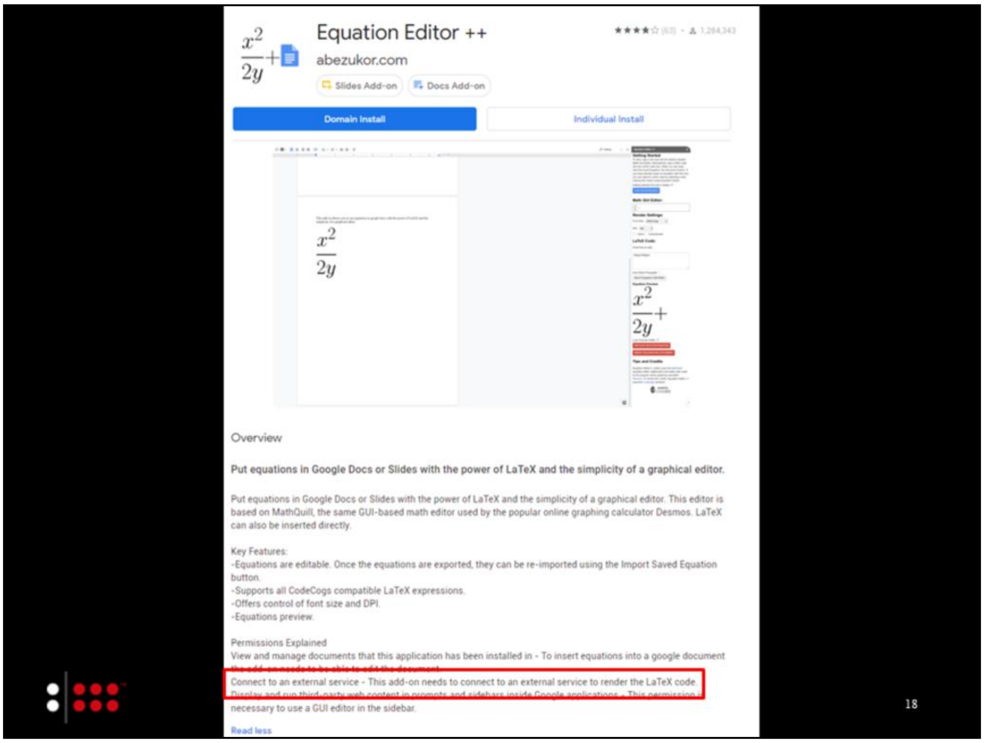
21% have **full access to Google Drive** data

17% can **read email** while running as an add-on

3% have **full access to Contacts** data

17

Most common permissions requested for apps that can connect to an external service.



Equation Editor ++

abezukor.com

★★★★☆ (63) · 1,284,343

Overview

Put equations in Google Docs or Slides with the power of LaTeX and the simplicity of a graphical editor.

Put equations in Google Docs or Slides with the power of LaTeX and the simplicity of a graphical editor. This editor is based on MathQuill, the same GUI-based math editor used by the popular online graphing calculator Desmos. LaTeX can also be inserted directly.

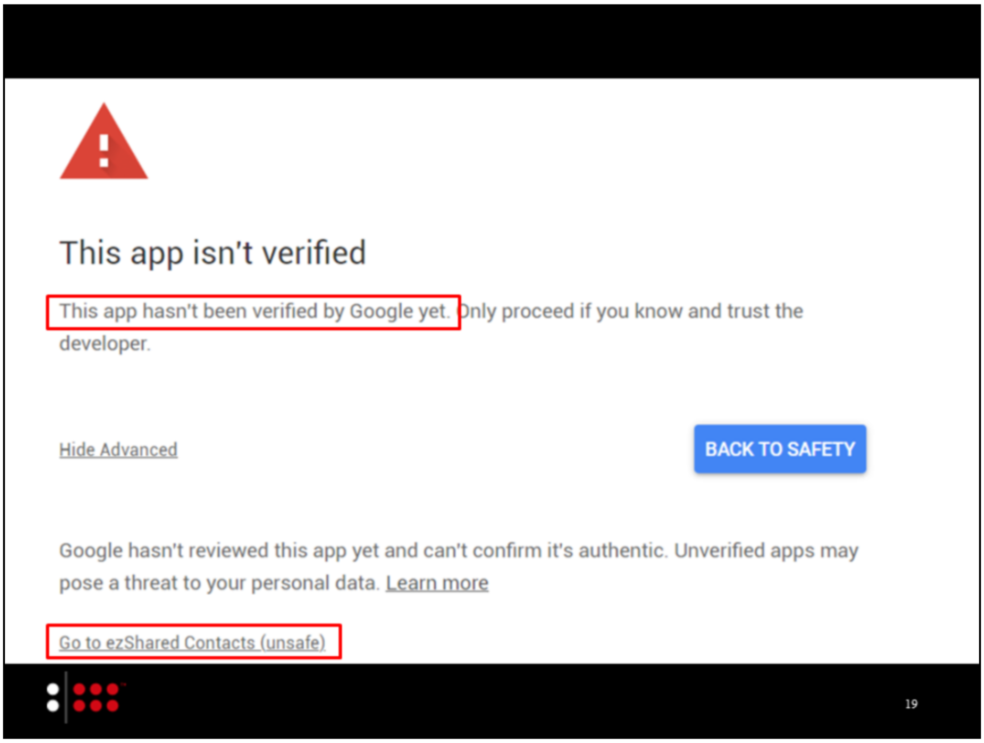
Key Features:
-Equations are editable. Once the equations are exported, they can be re-imported using the Import Saved Equation button.
-Supports all CodeCogs compatible LaTeX expressions.
-Offers control of font size and DPI.
-Equations preview.

Permissions Explained
View and manage documents that this application has been installed in - To insert equations into a google document the add-on needs to be able to edit the document.
Connect to an external service - This add-on needs to connect to an external service to render the LaTeX code.
Display and run third-party web content in prompts and sidebars inside Google applications - This permission is necessary to use a GUI editor in the sidebar.

Read less

There’s no mandatory disclosure for what external services are used or for what purpose.

Developers can voluntarily disclose this in the app description or the privacy policy, but that’s optional. User has to go out of the way to find out, and not even reliable.



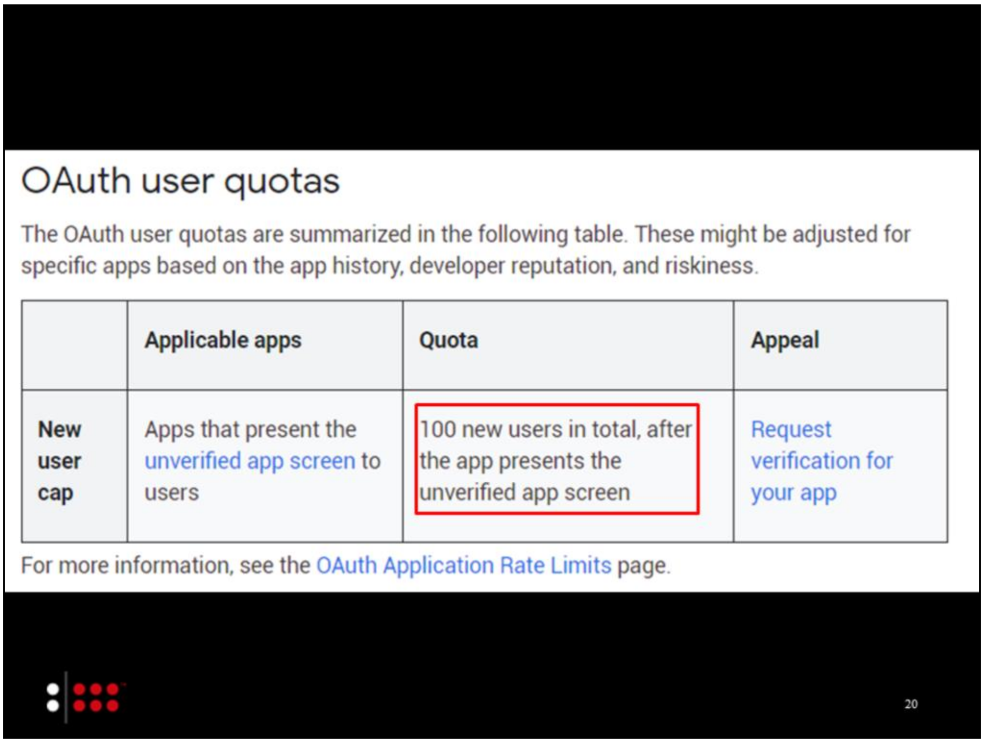
This app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.

Google hasn't reviewed this app yet and can't confirm it's authentic. Unverified apps may pose a threat to your personal data. Learn more

Given these risks, what's the platform doing?

Some apps threw this warning at installation. Something about app verification, but can still be installed.



OAuth user quotas

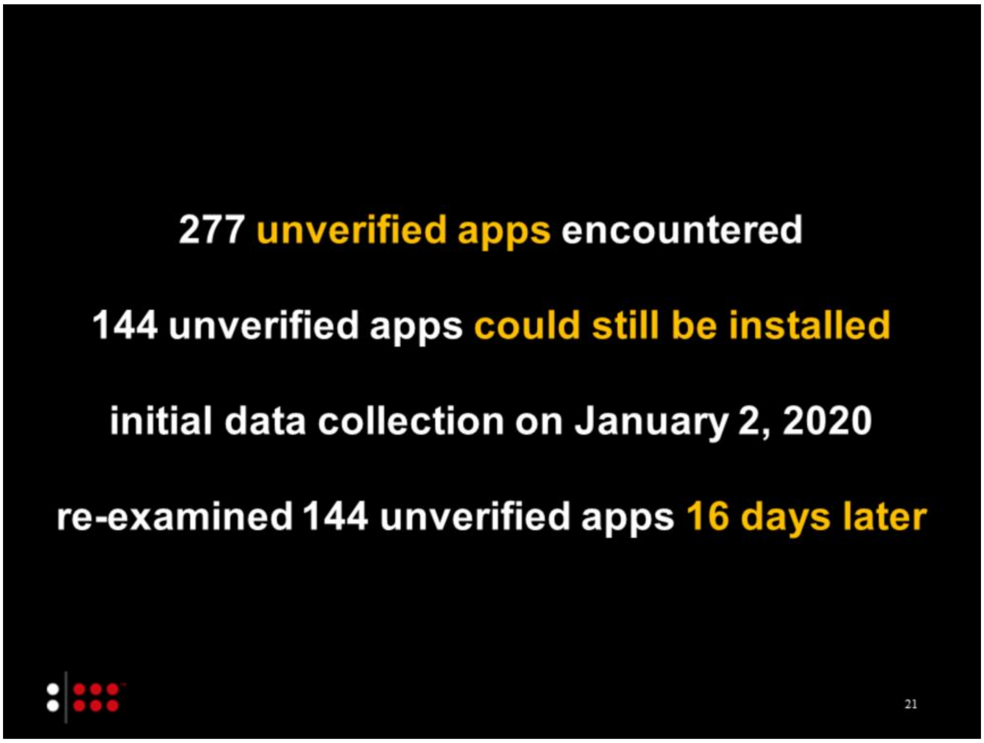
The OAuth user quotas are summarized in the following table. These might be adjusted for specific apps based on the app history, developer reputation, and riskiness.

	Applicable apps	Quota	Appeal
New user cap	Apps that present the unverified app screen to users	100 new users in total, after the app presents the unverified app screen	Request verification for your app

For more information, see the OAuth Application Rate Limits page.

Apps require verification if they use “sensitive” or “restricted” scopes for API authorizations. The most stringent review is for the Gmail and Drive scopes.

Apps under review have a limit on new users, but subject to Google’s discretion. What does this discretion look like?

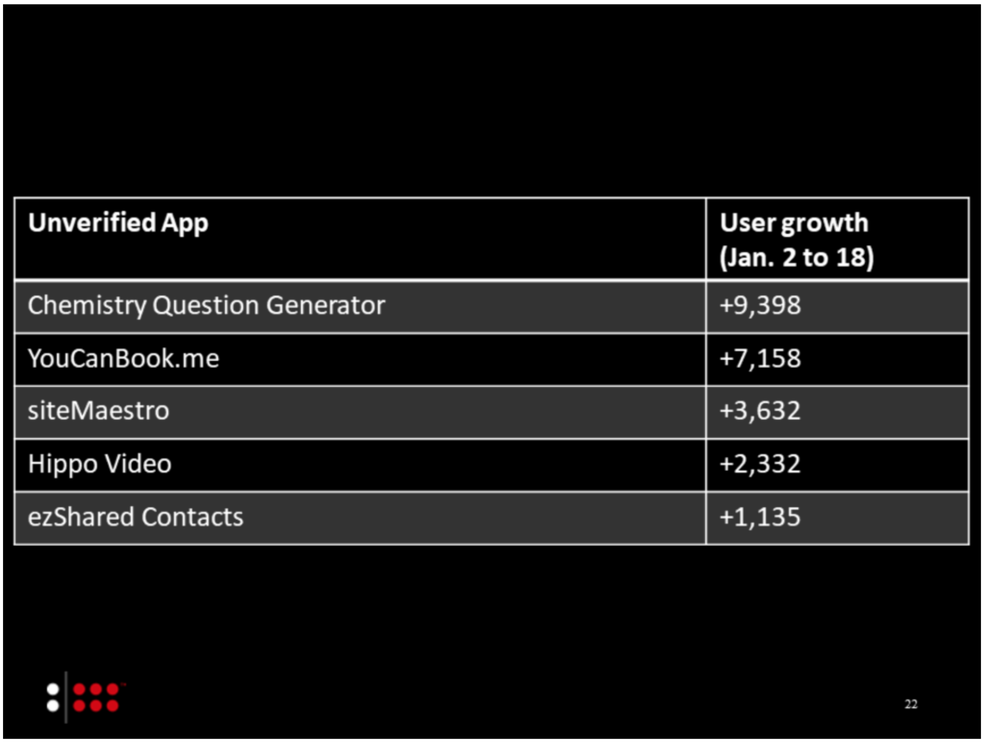


277 unverified apps encountered

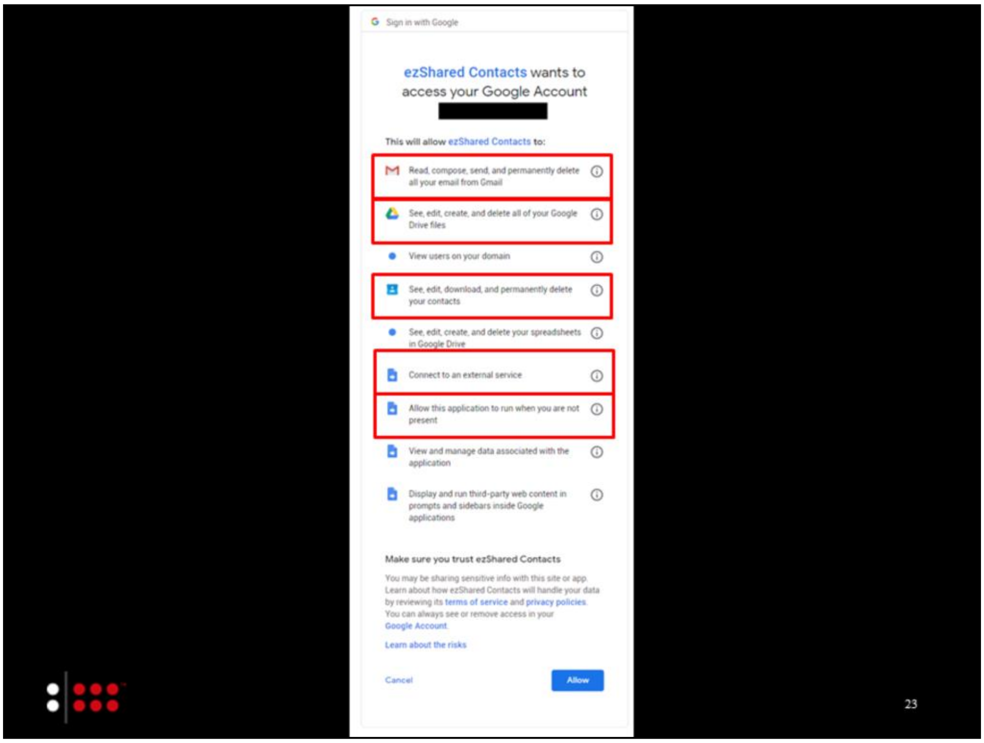
144 unverified apps could still be installed

initial data collection on January 2, 2020

re-examined 144 unverified apps 16 days later



Unverified App	User growth (Jan. 2 to 18)
Chemistry Question Generator	+9,398
YouCanBook.me	+7,158
siteMaestro	+3,632
Hippo Video	+2,332
ezShared Contacts	+1,135



ezShared Contacts wants to access your Google Account

[redacted]

This will allow ezShared Contacts to:

- Read, compose, send, and permanently delete all your email from Gmail
- See, edit, create, and delete all of your Google Drive files
- View users on your domain
- See, edit, download, and permanently delete your contacts
- See, edit, create, and delete your spreadsheets in Google Drive
- Connect to an external service
- Allow this application to run when you are not present
- View and manage data associated with the application
- Display and run third-party web content in prompts and sidebars inside Google applications

Make sure you trust ezShared Contacts

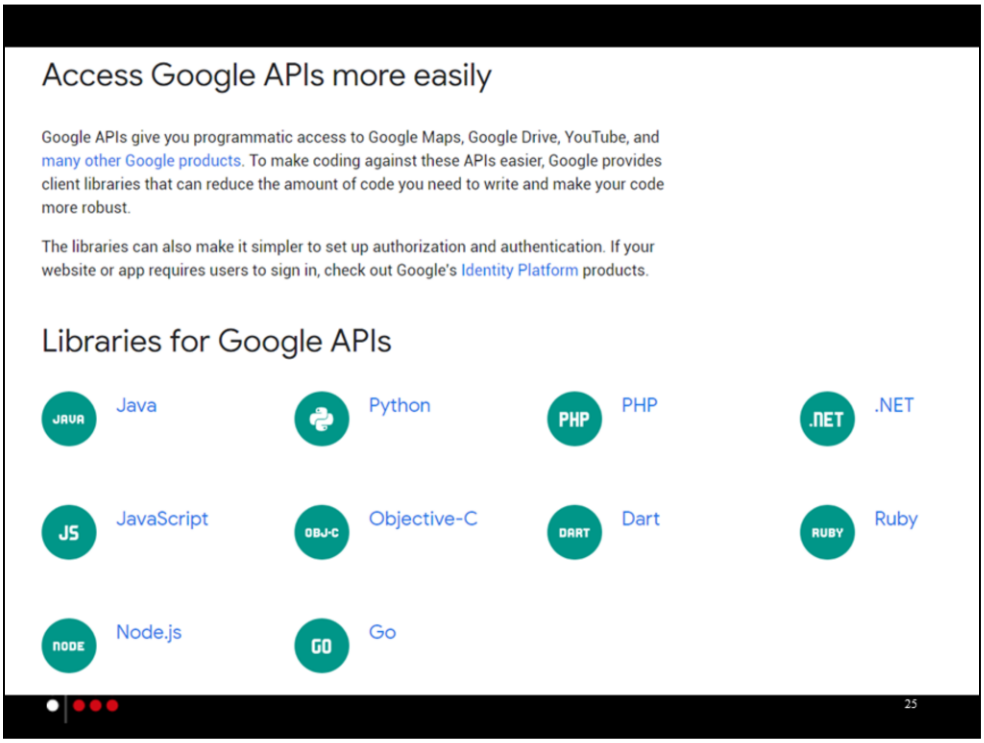
You may be sharing sensitive info with this site or app. Learn about how ezShared Contacts will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

what’s next?

24

Close off with thoughts on future research directions



Access Google APIs more easily

Google APIs give you programmatic access to Google Maps, Google Drive, YouTube, and many other Google products. To make coding against these APIs easier, Google provides client libraries that can reduce the amount of code you need to write and make your code more robust.

The libraries can also make it simpler to set up authorization and authentication. If your website or app requires users to sign in, check out Google's Identity Platform products.

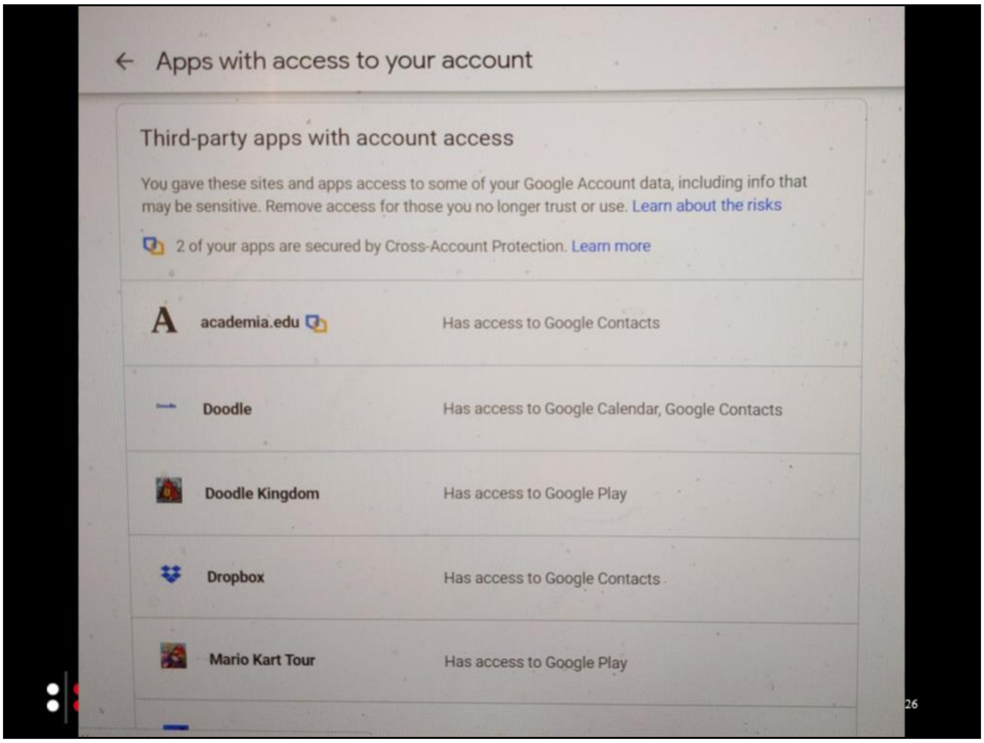
Libraries for Google APIs

Java	Python	PHP	.NET
JavaScript	Objective-C	Dart	Ruby
Node.js	Go		

This initial investigation only looked at web apps offered on the G Suite Marketplace.

There are many other classes of software that integrate with these APIs: mobile apps, desktop apps, etc.

Worth it to look at a broader set of software that use these APIs.



← Apps with access to your account

Third-party apps with account access

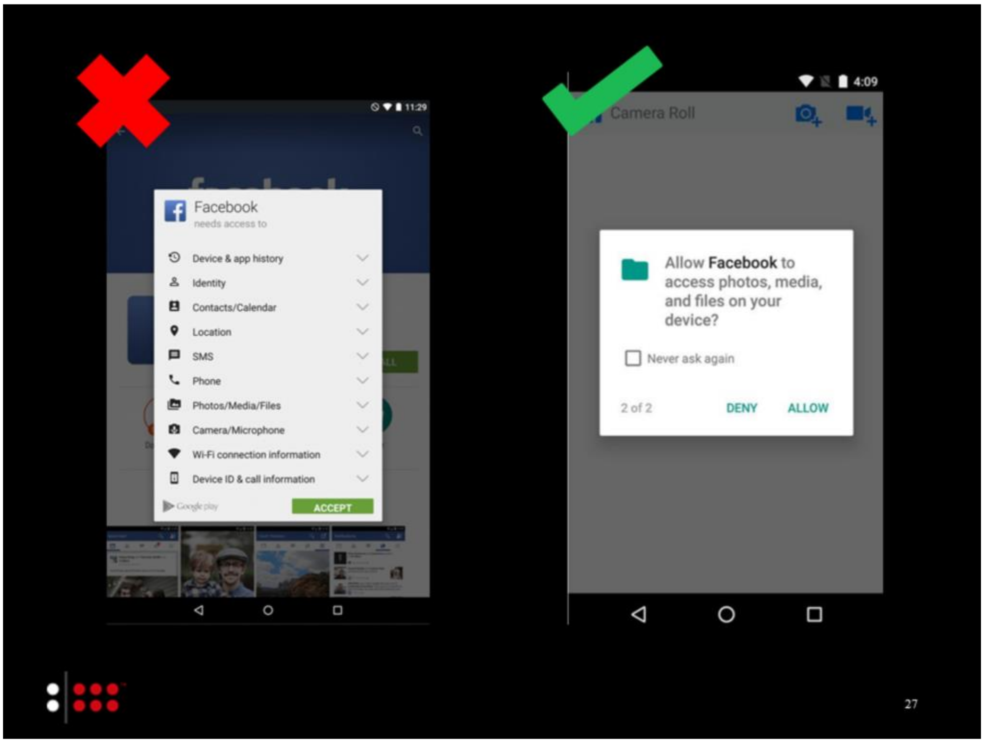
You gave these sites and apps access to some of your Google Account data, including info that may be sensitive. Remove access for those you no longer trust or use. Learn about the risks

2 of your apps are secured by Cross-Account Protection. Learn more

academia.edu	Has access to Google Contacts
Doodle	Has access to Google Calendar, Google Contacts
Doodle Kingdom	Has access to Google Play
Dropbox	Has access to Google Contacts
Mario Kart Tour	Has access to Google Play

I asked a friend to look at his Google account for API authorizations. Found lots.

How prevalent are these apps? What permissions do they use? How long have they been authorized? Are users surprised?



Facebook
needs access to

- Device & app history
- Identity
- Contacts/Calendar
- Location
- SMS
- Phone
- Photos/Media/Files
- Camera/Microphone
- Wi-Fi connection information
- Device ID & call information

Google play ACCEPT

Camera Roll

Allow **Facebook** to access photos, media, and files on your device?

□ Never ask again

2 of 2 DENY ALLOW

How about controls and disclosure?

We’ve learned a lot about how users navigate permissions on mobile devices. Install-time permissions are out, and run-time permissions are in.

Users can understand context and infer when and why an app needs to exercise a certain privilege. Can we do the same for web API authorizations?

THANKS!

apiprivacy.irwinreyes.com

@irwinreyescom

irwin.reyes@twosixlabs.com