

goto;

GOTO Copenhagen 2022

#GOTOCph

Investigating Privacy Issues on Mobile Platforms

@KrauseFx

18:43



inAppBrowser.com



InAppBrowser.com

Check if an in-app browser is injecting JavaScript code

Some iOS and Android apps make use of a custom in-app browser ([full details](#)). This causes potential security and privacy risks to the user.



JavaScript injection detected, with some potentially dangerous commands.

There might be additional JavaScript commands executed using "Isolated World" JavaScript, which can't be detected on this page.

Please read the Disclaimer below, as well as the [full explanation](#)

- Adds CSS code, allows app to customize appearance of website
- Monitors all taps happening on websites, including taps on all buttons & links
- Monitors all keyboard inputs on websites
- Gets the website title
- Gets information about an element based on coordinates, which can be used to track which elements the user clicks on

The New York Times



MacRumors

Forbes

9T@5Mac
APPLE INTELLIGENCE



MARKETING BREW

TC TechCrunch



YAHOO!

Mashable



BUSINESS
INSIDER

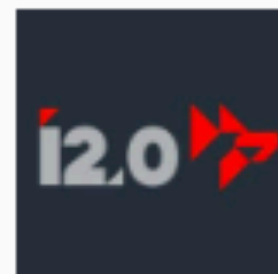
NEWS

纽约时报中文网
cn.nytimes.com

AXIOS

FREE METRO

THE AUSTRALIAN



CBS NEWS



Daily Mail

theguardian

The Washington Post



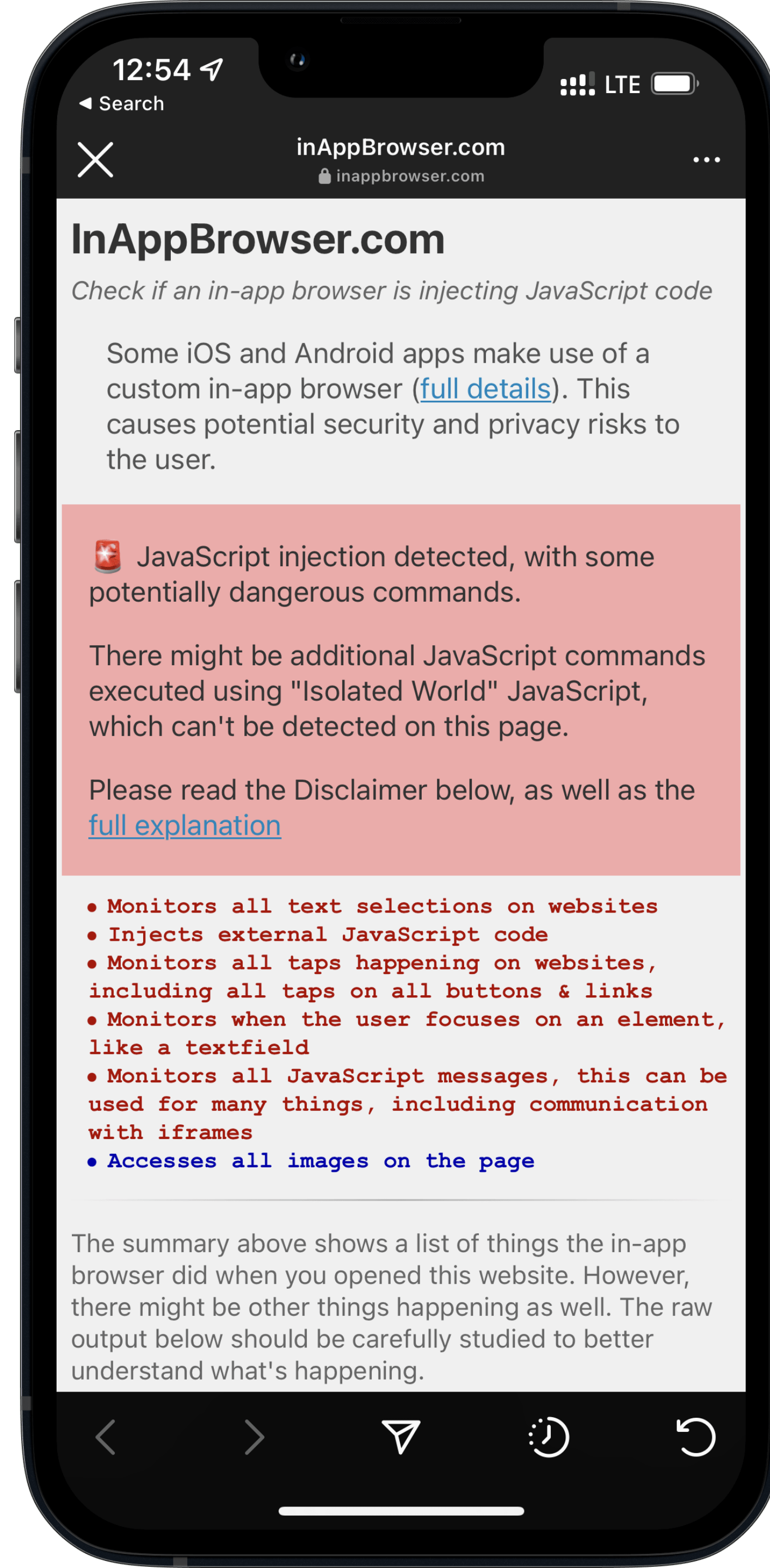
ORF

derStandard.at

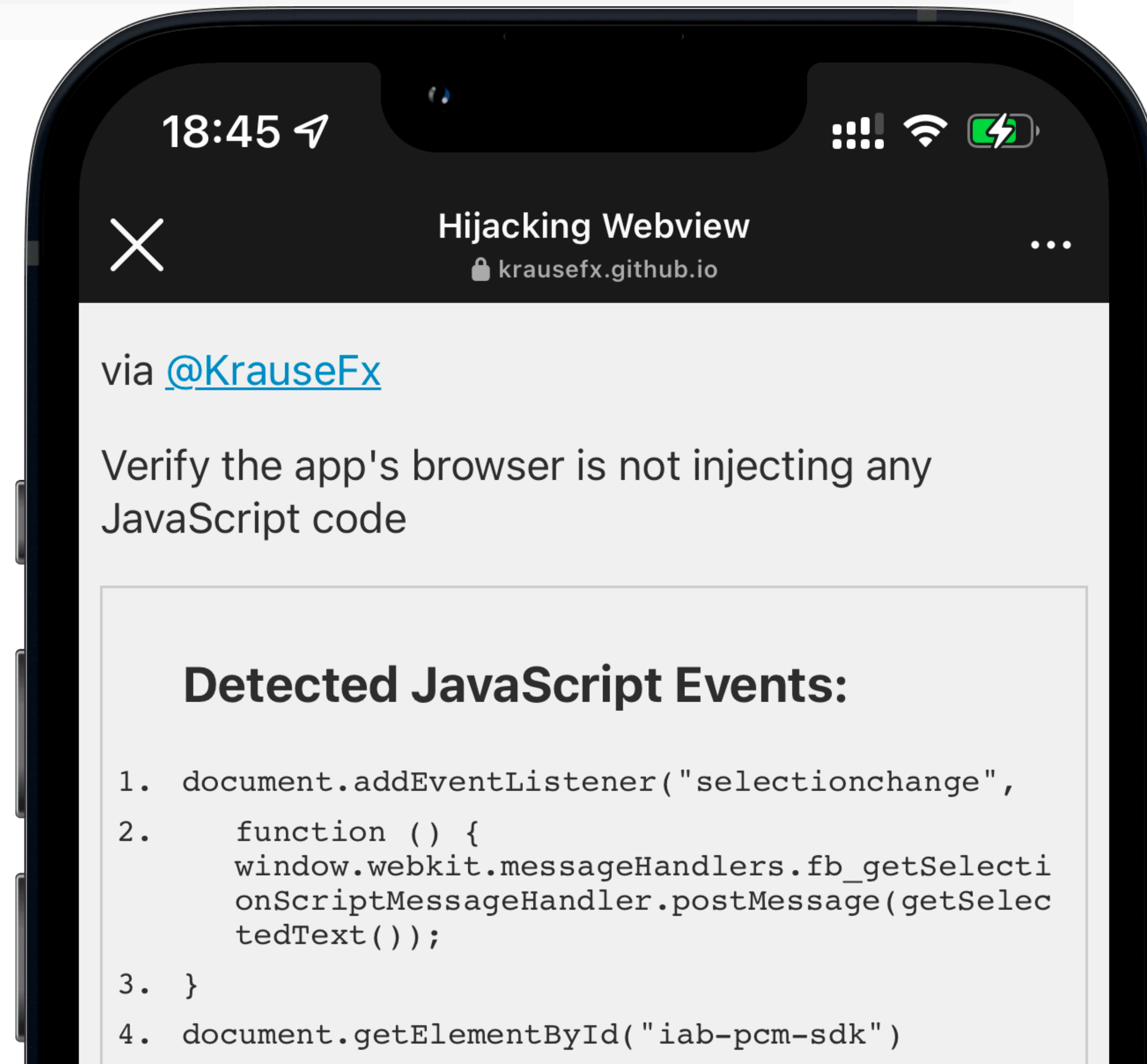
In-App Browsers

vs `SFSafariViewController`

Why I looked into it



```
document.getElementById = function(a, b) {  
    appendCommand('document.getElementById("' + a + '"')  
    return originalGetElementById.apply(this, arguments);  
}
```



Write a post

Responsible Disclosure



Tweet Analytics



Felix Krause  @KrauseFx · Aug 18



 **New Post: Announcing InAppBrowser - see what JavaScript commands get injected through an in-app browser**

 **TikTok, when opening any website in their app, injects tracking code that can monitor all keystrokes, including ...**

[Show this thread](#)



32.09K



18.08K



417

Impressions ⓘ

17M

Engagements ⓘ

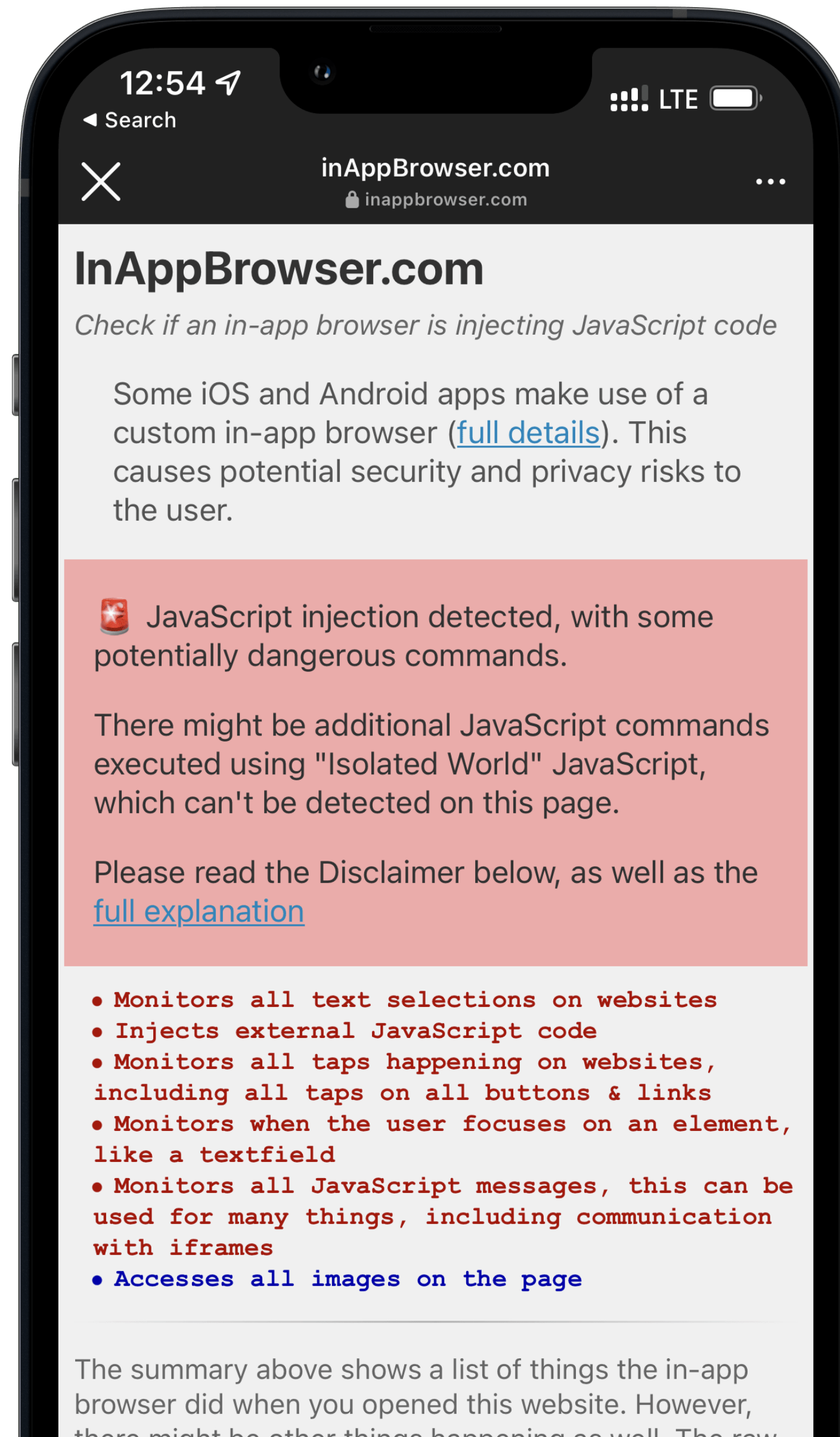
330K

Detail expands ⓘ

130K

Public Comments

inAppBrowser.com

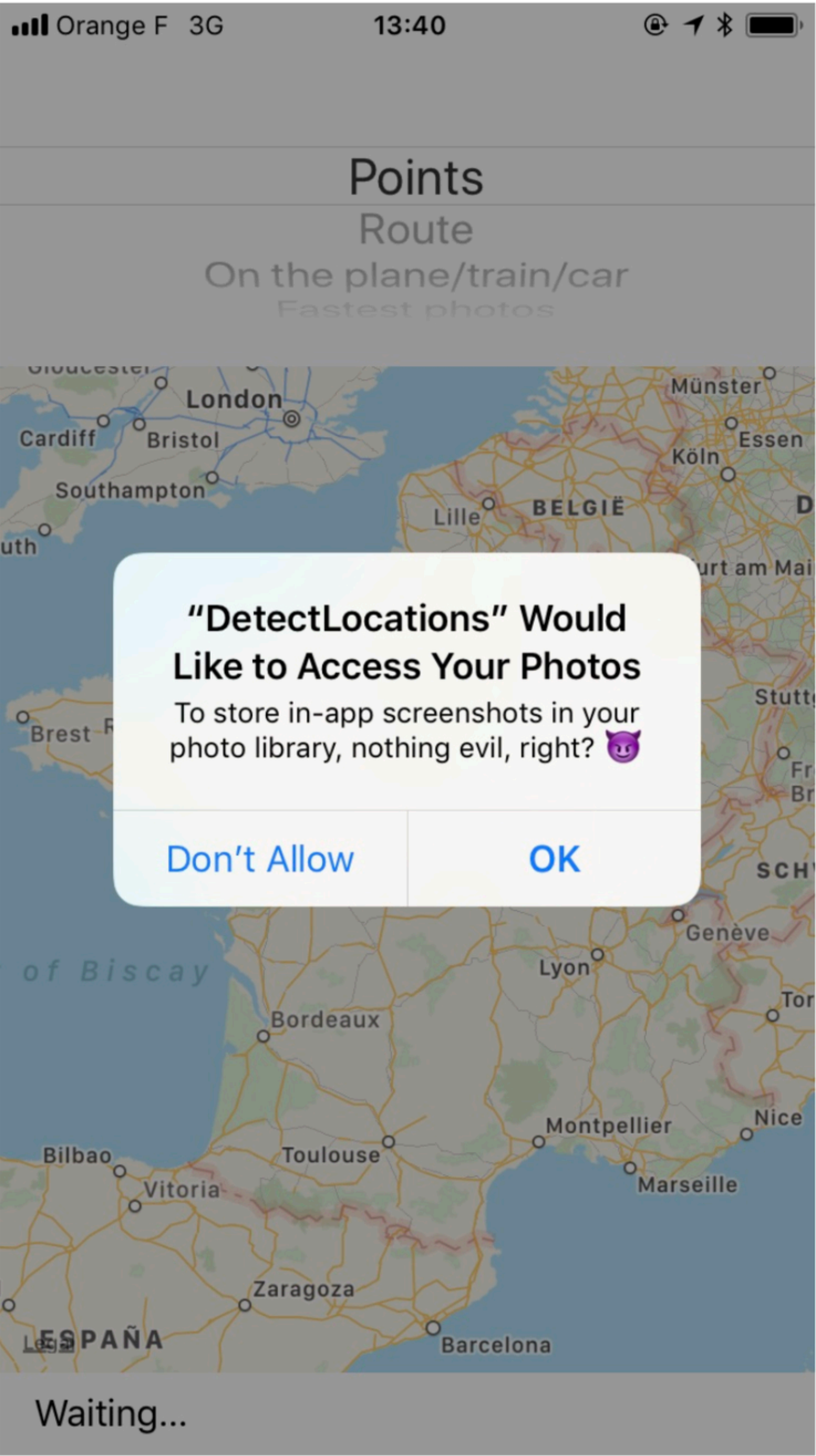


App	Option to open in default browser	Modify page	Fetch metadata	JS	Updated
TikTok		<u>Yes</u>	<u>Yes</u>	.js	2022-08-18
Instagram		<u>Yes</u>	<u>Yes</u>	.js	2022-08-18
FB Messenger		<u>Yes</u>	<u>Yes</u>	.js	2022-08-18
Facebook		<u>Yes</u>	<u>Yes</u>	.js	2022-08-18
Amazon		<u>None</u>	<u>Yes</u>	.js	2022-08-18
Snapchat		<u>None</u>	<u>None</u>		2022-08-18
Robinhood		<u>None</u>	<u>None</u>		2022-08-18

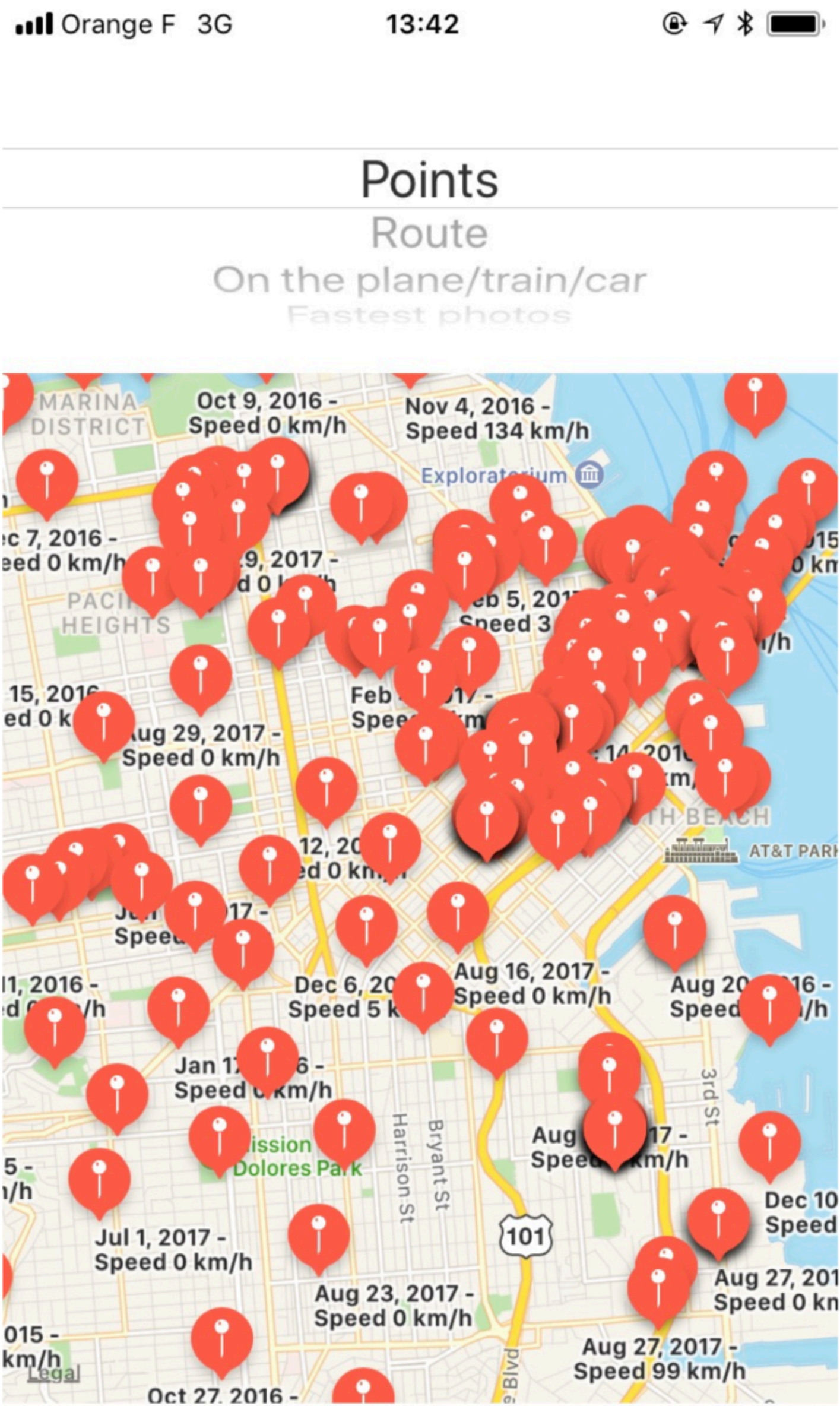
App	Technology	Updated
Twitter	SFSafariViewController	2022-08-15
Reddit	SFSafariViewController	2022-08-15
WhatsApp	Default Browser	2022-08-15
Slack	Default Browser	2022-08-16
Spotify	SFSafariViewController	2022-08-16

What else?

Permission Dialog

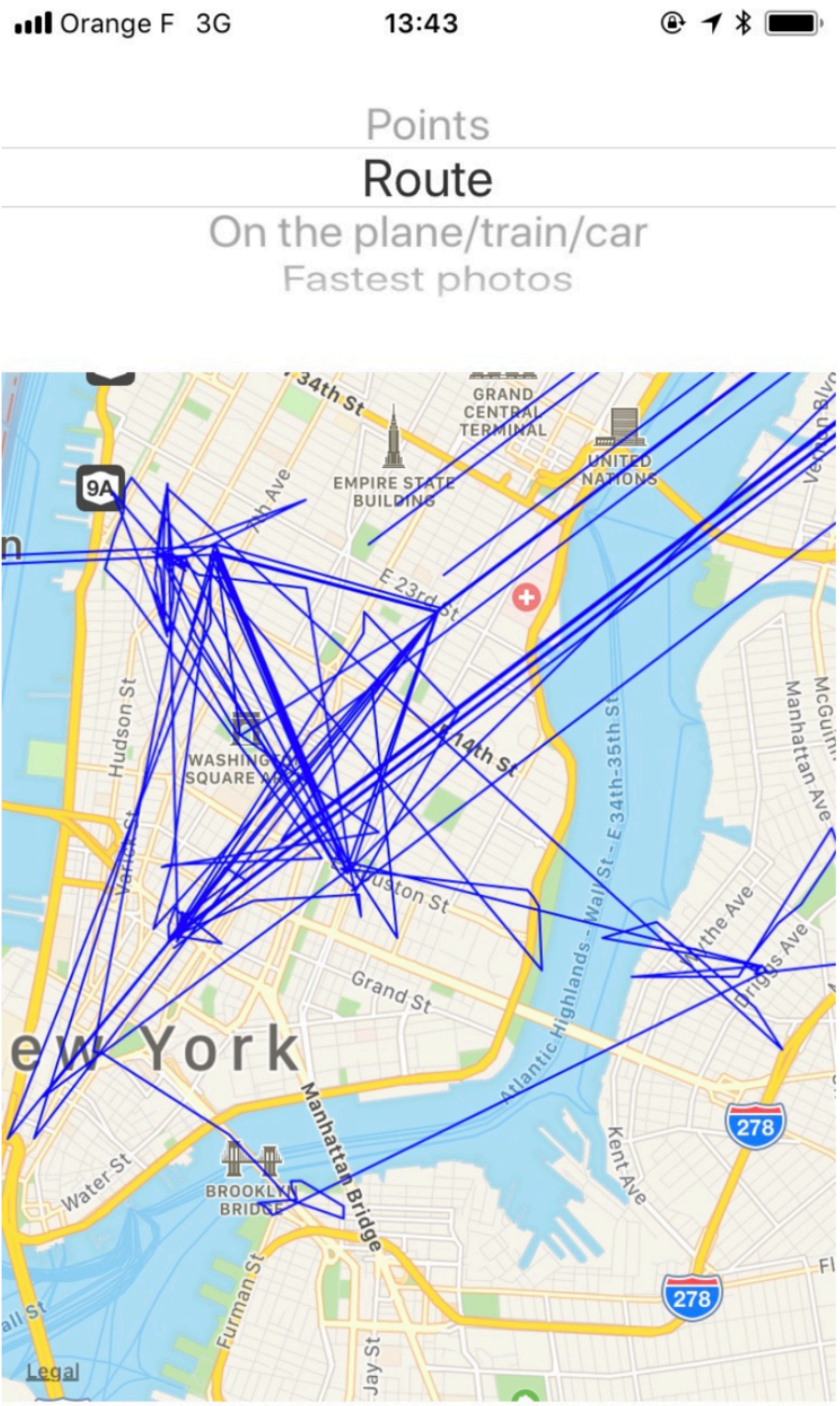


Map of locations



It took 0.58s to access 11983 locations

Rendering of Route

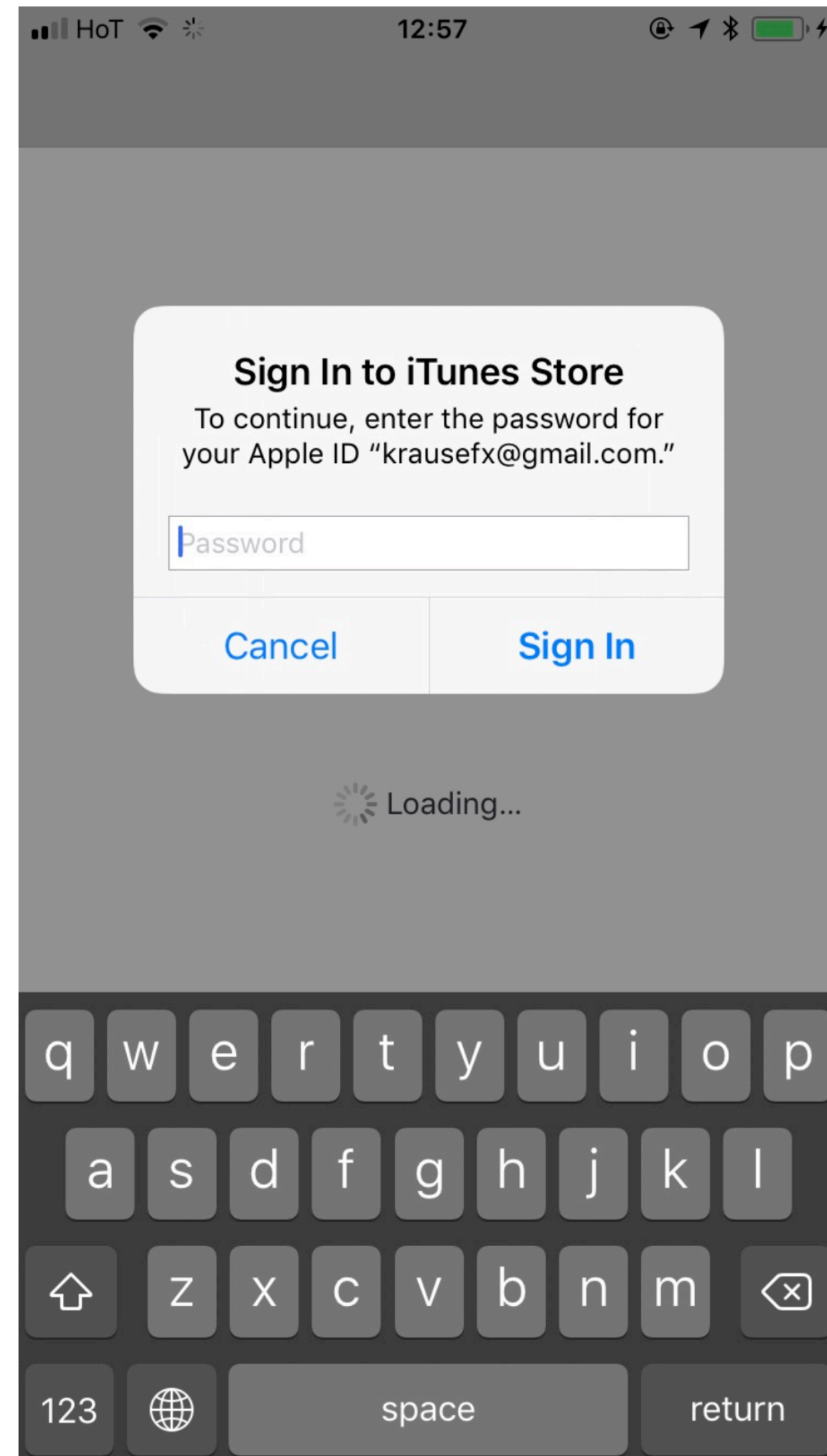


Taken with iPhone 6s back camera

Camera Permissions



Official iOS Popup



This image shows an official iOS system popup for signing into the iTunes Store. The popup is centered on a gray background. It has a title "Sign In to iTunes Store" and a subtitle "To continue, enter the password for your Apple ID 'krausefx@gmail.com.'" Below the text is a password input field with the placeholder text "Password". At the bottom of the popup are two buttons: "Cancel" and "Sign In". Below the popup, there is a "Loading..." indicator with a circular progress icon. At the very bottom of the screen is a standard iOS keyboard with keys for letters, numbers, space, and return.

Sign In to iTunes Store

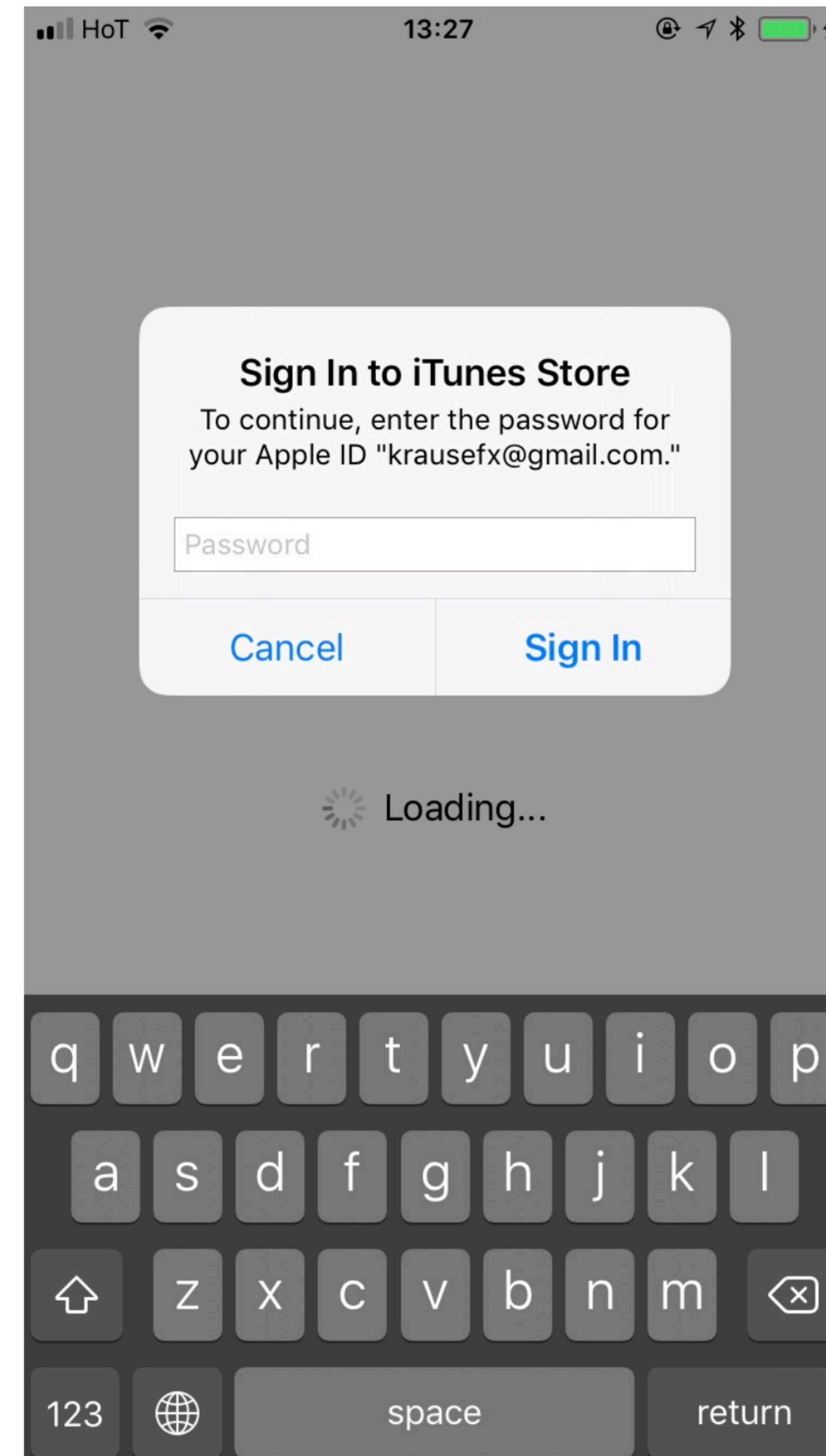
To continue, enter the password for your Apple ID "krausefx@gmail.com."

Password

Cancel Sign In

Loading...

Phishing Popup



This image shows a phishing version of the iOS Sign In to iTunes Store popup. It is visually identical to the official version, with the same title, subtitle, password input field, and buttons. However, the background is a solid gray, and the keyboard at the bottom is a standard iOS keyboard. The time in the status bar is 13:27, and the carrier is HoT.

Sign In to iTunes Store

To continue, enter the password for your Apple ID "krausefx@gmail.com."

Password

Cancel Sign In

Loading...

S 1Password 6 File Edit View Account Item Window Help

411 a 3m ••• 10.2 - 11:00

FOLDERS • fastlane

► • .assets ► r .circleci ► .github ► ll bin ► ME cert ► • credentials_manag ► r deliver ► • fastlane ► • fastlane_core ► r frameit ► ll gym ► ll
match ► r pem ► p pilot ► hi pkg ► precheck ► Pr produce ► ▪ rakelib ► ▪ rubocop ► ME scan ► r screengrab ► ll sigh ► ll snapshot ► ll
spaceship ► ll supply D .gitignore /* .hound.yml /* .keys n .rspec /* .rubocop.yml n .ruby-version /* appveyor.yml /* Brewfile <> CODE_OF_CONDU
<> CONTRIBUTING.md <> CORE_CONTRIBUT /* Dangerfile /* fastlane.gemspec /* Gemfile n Gemfile.lock D LICENSE

export GITHUB_API_TOKEN "64eb522d54e54484b91fa58d9a02c0fc" 2 export FL_GITHUB_RELEASE_API_TOKEN
"23b67efc916471abf9a25796c53669b" 3 export GITHUB_USER_NAME "KrauseFx" 4 export FASTLANE_PLUGIN_DIRECTORY_GITHUB_USER
"KrauseFx" 5

Spaces: 2

Shell Script (Bash)

All Vaults o

Favorites Categories Tags

Security Audit I? Watchtower eWeak Passwords Duplicate Passwords (180) 0 3+ years old 0 1-3 years old (273) 0 6-12 months old
(571.)

Q'Search 1Password

571 items sorted by Date Modified N.1

Dec 2017

Fake Login Data

Vault Primary

username myuser@gmail.com

password 1MyTopSecretPassword copy strength

show web form details

last modified Today at 11:00 AM

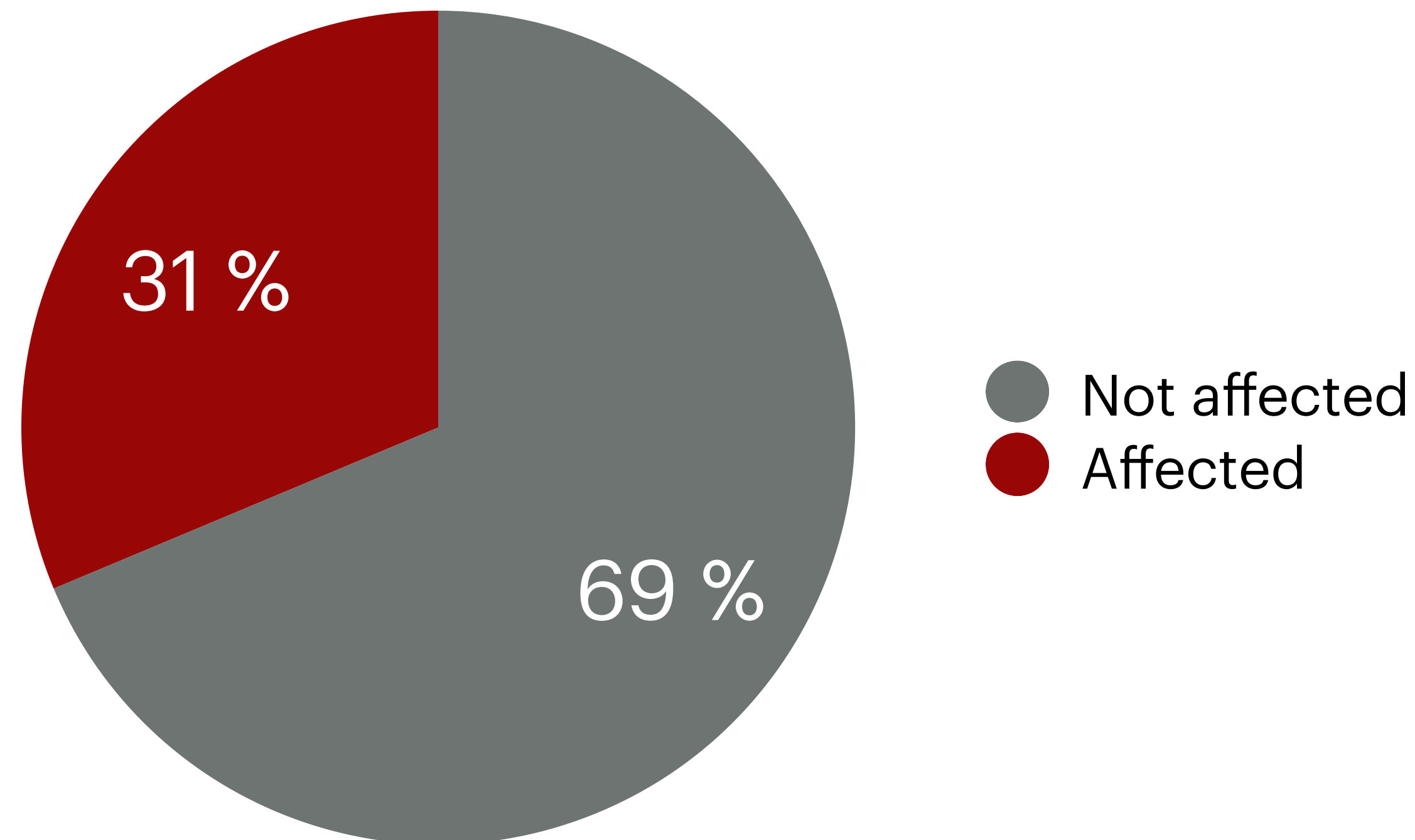
created Today at 11:00 AM

Edit

Hijacking SDKs

Analysed 41 of the most used SDKs

Vulnerable to a human-
in-the-middle attack



- 🏠 Welcome to buddybuild!
- 🔧 Quickstart
- Sign up with GitHub
- Sign up with GitLab
- Sign up with SSH
- Sign up with Bitbucket
- Connect with Bitbucket Server
- Connect with GitHub Enterprise
- Connect your privately-hosted GitLab instance
- Single sign on (SSO)
- Require SSO
- Disconnect SSO
- Okta
- iOS
- Selecting an app
- Inviting testers
- Integrate the SDK for iOS
- Auto-syncing provisioning profiles
- Auto versioning
- Android



🔍

Type to search



Prefer to manually integrate the SDK?

Follow the [Manual SDK Integration Guide](#).

Update the SDK

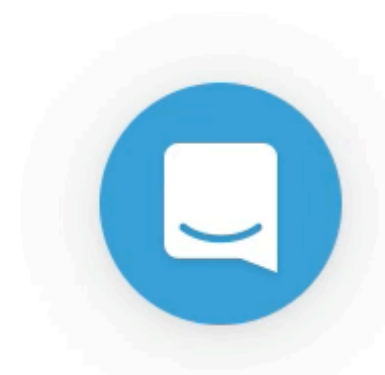
- 1
- Open the Terminal and `cd` to your root directory of your repo.
- 2
- Run the following command:

```
curl -Ls tools.buddybuild.com.s3-website-us-west-2.amazonaws.com/UpdateSDK | sh
```

- 3
- Commit and push the changes.

Uninstall the SDK

If for some reason, you wish to uninstall the SDK, you simply need to revert the commit which installed it in the first place.

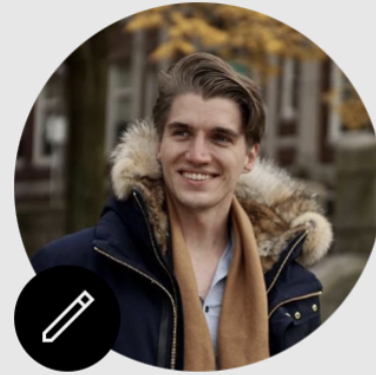


“Yah obviously”

- **“Giving an app camera permission lets them record you”**
- **“Of course photos have GPS location”**



Edit Account



First Name

Felix



Last Name

Krause



Phone Number



Verified >

Select a photo

Take photo

Choose from library

Cancel

“Just don’t use the app”

It's our job to protect the user

**We need to improve the underlying
platform to protect the user**

You already know of something!

Think about the Worst Case

Build it out

Responsible Disclosure

How to go public?

Why your report might get ignored

Why going public is important

Go for it

Don't forget to
rate this session
in the **GOTO Guide app**