April 2025
Vol. XLIV, No 4

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral
April 15th Meeting

Please see your membership email for the links to this month's Zoom meeting or email us at KeystoneMacCentral@mac.com.

During our program this month we plan to discuss

☞ Personalize Your iPhone's Control Center

☞ How to Use Waze

We have virtual meetings via Zoom
on the third Tuesday of each month.

Emails will be sent out prior to each meeting.
Follow the directions/invitation each month
on our email — that is, just click on the link
to join our meeting.

Contents

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer
systems. Meetings are free and open to the public. **The *Keystone MacCentral printout*** is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2025, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles form the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors

By Adam Engst

How to Identify iPhone Apps That May Contain Location-Tracking Ads

Earlier this year, 404 Media published another article about the location-tracking industry that surreptitiously gathers and resells our location data (for earlier coverage, see "Exposé Reveals Ongoing Smartphone Location Tracking Threats," 23 October 2024). This piece highlighted another reason why allowing private companies to collect such information is concerning—one of the major players in the field was hacked. Gravy Analytics, the parent company of Venntel, which sold smartphone location data to the US government, reportedly lost "a massive amount of data, including customer lists, information on the broader industry, and even location data harvested from smartphones which show peoples' precise movements."

Despite the FTC later prohibiting both companies from collecting, using, and selling sensitive location data of Americans, all that data is reportedly now available for purchase. Among those compromised files was a list of over 12,000 iOS and Android apps that may have been—and may still be—exploited by data brokers to collect users' location data. These apps do not contain malicious code; instead, they are part of the real-time bidding advertising ecosystem. When advertisers bid to place ads within apps, all firms participating in the bidding—including data brokers—are granted access to information about your device, including data that can be used to infer location.

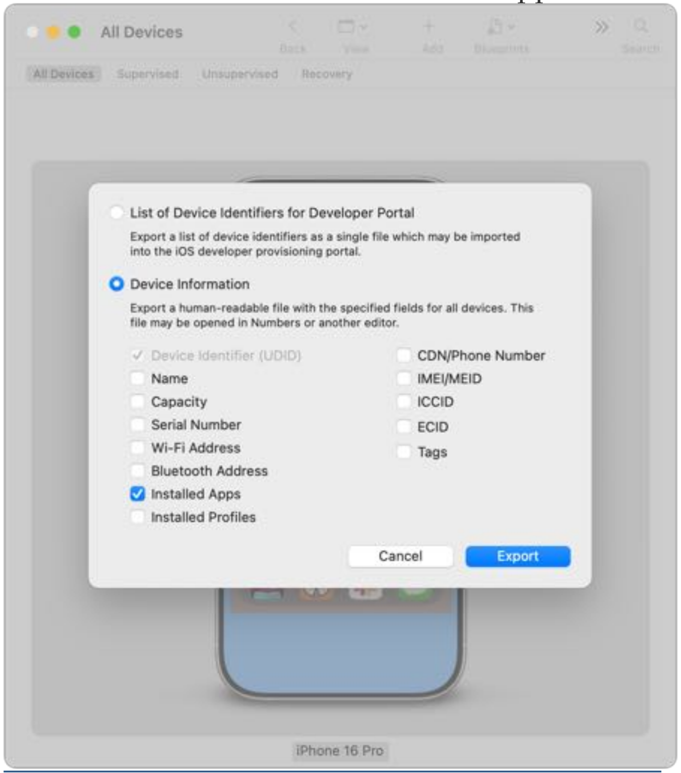
Even browsing through a list of over 12,000 apps, many of which are for Android, feels overwhelming, let alone manually comparing all the apps on your iPhone to the master list. Fortunately, there is an automated way to determine which apps on our iPhones were involved, knowingly or not, in this location data collection scheme.

1. Download Apple Configurator from the Mac App Store.

2. If prompted, allow the iPhone to connect and install a driver update.

3. Open Apple Configurator and select your iPhone.

4. Choose Actions > Export > Info, select Device Information, and then select Installed Apps.



○ List of Device Identifiers for Developer Portal

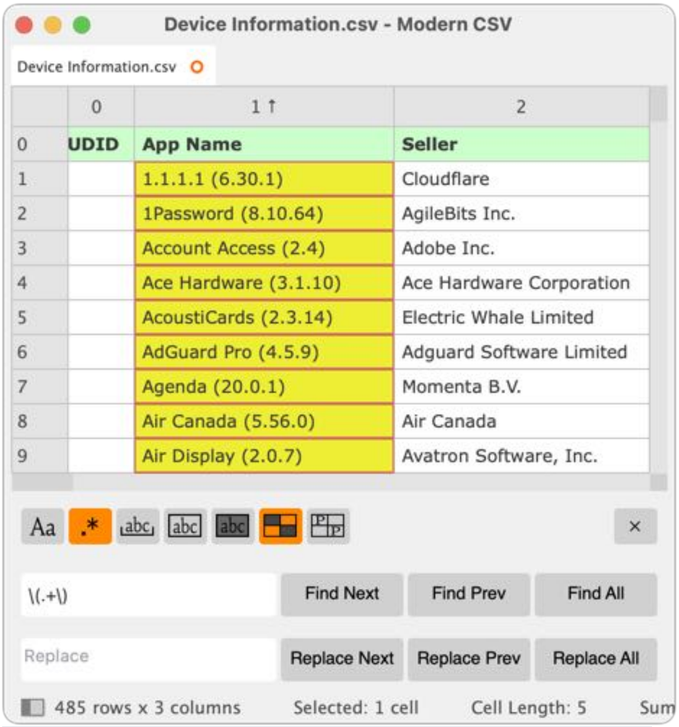
Export a list of device identifiers as a single file which may be imported into the iOS developer provisioning portal.

● Device Information

Export a human-readable file with the specified fields for all devices. This file may be opened in Numbers or another editor.

✓ Device Identifier (UDID)
□ Name
□ Capacity
□ Serial Number
□ Wi-Fi Address
□ Bluetooth Address
☑ Installed Apps
□ Installed Profiles
□ CDN/Phone Number
□ IMEI/MEID
□ ICCID
□ ECID
□ Tags

5. Apple Configurator then lets you save a three-column CSV file. I'll leave it as an exercise for the reader to delete the UDID and Seller columns and remove each app's parenthetical version number. I used Modern CSV with a grep search to find and delete a string consisting of a space and any text in parentheses, but you could also do that in BBEdit or other apps. (Yes, I really do have 484 apps on my iPhone.)

6. 

Device Information.csv - Modern CSV

	0	1 ↑	2
0	UDID	App Name	Seller
1		1.1.1.1 (6.30.1)	Cloudflare
2		1Password (8.10.64)	AgileBits Inc.
3		Account Access (2.4)	Adobe Inc.
4		Ace Hardware (3.1.10)	Ace Hardware Corporation
5		AcoustiCards (2.3.14)	Electric Whale Limited
6		AdGuard Pro (4.5.9)	Adguard Software Limited
7		Agenda (20.0.1)	Momenta B.V.
8		Air Canada (5.56.0)	Air Canada
9		Air Display (2.0.7)	Avatron Software, Inc.

\(.+\)

485 rows x 3 columns Selected: 1 cell Cell Length: 5

7. Download this [text file with all 12,325 apps](#) identified in the data breach to spare you the effort of copying data from the [public Google Sheet shared by 404 Media](#).

8. Once you have the list of apps on your iPhone and the text file of all the apps in the Gravy Analytics breach, run this command in Terminal to identify the apps that appear in both. To customize it with your filenames, use the arrow keys and delete key to remove `file1.txt` and then drag one of the files in; repeat the navigation with the arrow keys and character deletion for `file2.txt` before dragging in the second file. Press Return when you're ready.

```
comm -12 <(sort
file1.txt | uniq) <(sort
file2.txt | uniq)
```

9. The results appear instantly. Only three of my 484 apps appear in the Gravy Analytics list: Citymapper, Tumblr, and Wattpad. I must have downloaded Citymapper long ago for some trip, I don't use the Tumblr app, and I don't even remember what Wattpad is. It was an easy decision to delete them.

Given that I hadn't launched any of those apps in years, I don't think I was particularly vulnerable to having my location data sucked up as part of the real-time bidding process. Nevertheless, this experience will make me even more cautious about downloading apps that display ads.

If you go through this process, please share the apps it identifies. Some people have come up with alternative approaches that include Apple apps, which Configurator does not, and then match those apps against what I believe are Android apps in the full list. There's no reason to worry about Apple apps in this regard.

By Adam Engst

Apple Updates Keep Malicious Web Content in the Sandbox

Apple has released several updates with a supplementary fix for an attack that the company says was blocked in iOS 17.2. These include [iOS 18.3.2 and iPadOS 18.3.2](#), [macOS 15.3.2 Sequoia](#), [visionOS 2.3.2](#), and [Safari 18.3.1](#) for macOS 13 Ventura and macOS 14 Sonoma. (Apple also released [tvOS 18.3.1](#) to fix a bug that may prevent playback of some streaming content on the 3rd-generation Apple TV 4K. It has no security release notes and may not have needed the supplementary fix.)

The updates prevent maliciously crafted Web content from breaking out of the Web Content sandbox and kicking sand in the faces of Apple users everywhere. The original vulnerability was exploited in what Apple describes as an "extremely sophisticated" attack against specific targeted individuals on versions of iOS before iOS 17.2.

Apple identifies this latest vulnerability as CVE-2025-24201. Apple filing a CVE is unusual, as the company typically only acknowledges external researchers and organizations while remaining silent about vulnerabilities discovered internally.

Given Apple's reference to the atta201 exists in the wild."

In other words, despite Apple's statement, I don't think iOS 17.2 blocks the "extremely sophisticated attack against specific targeted individuals." When I combine the lack of release notes for iOS 17.2.1 with the release of Safari 17.2.1 (suggesting a WebKit vulnerability) and the late December release date, I believe that this second set of releases was aimed at rebuilding the Web Content sandbox, but Apple could stay quiet about the details because it discovered the problem internally. Perhaps Apple was speaking loosely by including iOS 17.2.1 when it said that versions of iOS before iOS 17.2 were affected.

I suspect that Apple would have quietly integrated this fix into its next set of updates, except that it also affected Google Chrome. That required going public and filing a CVE, and once that had happened, Apple had no choice but to release these updates immediately to ensure that its current operating systems weren't vulnerable.

Practically speaking, I think it's important to update, but not in panic mode. Although this supplementary fix is associated with a zero-day exploit, it occurred over a year ago and was used against "specific targeted individuals," so the vulnerability is probably not the sort of thing that would be leveraged in malware against everyday Apple users in the next few days. Install the updates as soon as it's convenient, and stay safe out there.

Bu Glenn Fleishman

Apple Aims to Boost Child Privacy with New Age-Related Controls

In an era marked by competing desires for online child safety, parental control, and the need to abide by evolving government regulation, Apple hopes that changes it plans to roll out over the rest of 2025 will thread the needle on issues related to personal data disclosure for children. In a new white paper, "Helping Protect Kids Online," the company has outlined its plans for how children's ages will be indicated by parents and passed to developers to provide access to age-appropriate apps and features.

Apple's approach tries to balance three different impinging needs: more invasive age-verification requirements being imposed by some US states and countries, parents' interest in protecting their children's personal data and blocking access to materials they deem inappropriate, and the company's goal of releasing to developers the least amount of information necessary to comply with privacy-impacting regulations. It's a hard row to hoe.

While the white paper focuses on parents' oversight of children's access to apps and the content within them, Apple isn't shy about criticizing requests for government-issued IDs—whether instigated by developers or required by legislation—when nothing within an app should require such disclosure.

Apple outlines four areas of change:

- Child Account setup: A new setup process will simplify setting up a Child Account. Separately, Apple will enable parents to correct the age associated with a child's Apple Account and turn it into a Child Account within a Family Sharing group.
- Safe sharing of broad age ranges: Parents will be able to share an age range instead of being forced to share a birthdate or even an exact age to access age-appropriate content in apps. Developers will have to update their apps to use a new API.
- Defining age ranges for apps: Apple currently has just two global age ranges: 12+ and 17+. Other age ranges exist in particular countries that already require different ages or more granularity. The update will define two ranges for younger children and three for teenagers.
- App Store disclosures and browsing: Apple will require that developers disclose features within apps that could show material inappropriate for a declared age range, the use of in-app parental controls, and any requirement for proof of age. Further, users with Child Accounts searching in any App Store will only see matches available within their age range.

A full-page sidebar also explains Apple's stance on limiting age disclosure from information Apple or its users possess to developers. (The company categorizes this under the new term Age Assurance.) This explanation is targeted at the many rules imposed by various governments, most recently across the United States, that require age verification to access social media or adult media content. There's quite a lot of subtext on this page, such as:

Some apps may find it appropriate or even legally required to use age verification, which confirms user age with a high level of certainty—often through collecting a user's sensitive personal information (like a government-issued ID)—to keep kids away from inappropriate content. But most apps don't.

Apple states its position clearly without calling out any particular state, political party, or nation:

Requiring users to overshare their sensitive personal data would also undermine the vibrant online ecosystem that benefits developers and users.

As a result, Apple says it won't allow apps to request IDs or other proof of age arbitrarily. Instead, the company will rely on age ranges for people under 18. Regardless of age, Apple implies that a developer will have to justify the need to collect explicit proof of age during app review.

The new global age ratings Apple plans to roll out are:

- 4+: Apps have no objectionable content.
- 9+: Apps might contain infrequent uses of fantasy or cartoon violence, mild horror elements, or crude humor.
- 13+: Apps might increase the frequency of those 9+ items. They could also contain "medical or treatment-focused content" (a disturbing set of terms) and reference a range of things, like drugs, alcohol, nudity, or realistic violence. It's unclear what "reference" means compared to "includes."
- 16+: Apps could include "frequent or intense" use of "mature or suggestive" content, as well as medical and treatment-focused material and unrestricted Web access.
- 18+: Apps could contain actual nudity and gambling, plus frequent or intense instances of adult stuff like drinking, sexual activity, smoking, and realistic violence. It's hard to imagine Apple approving even apps rated 18+ that contain nudity or sexual activity, given the company's past opinions about such content.

Apple says most of these features are "coming later this year," "this year," or "by the end of the year." Some changes will be straightforward and entirely within Apple's control, such as streamlining Child Account sign-up or enabling migration from a regular Apple Account. Others will require Apple to deploy new APIs and developers to upgrade their apps and disclose new age-range requirements in the Privacy Nutrition Labels in their App Store listings.