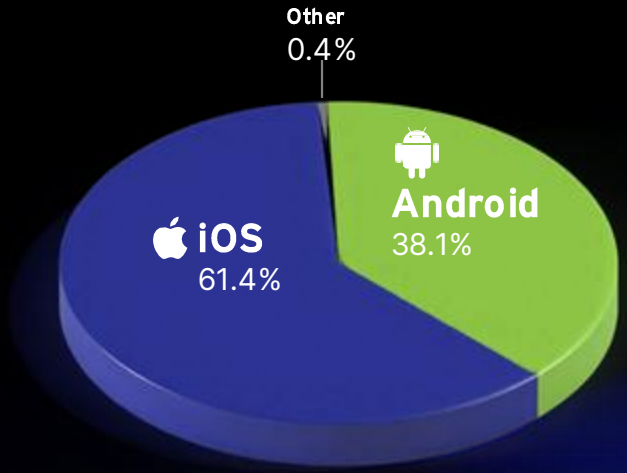
AppleStorm:

Unmasking the Privacy Risks of Apple Intelligence

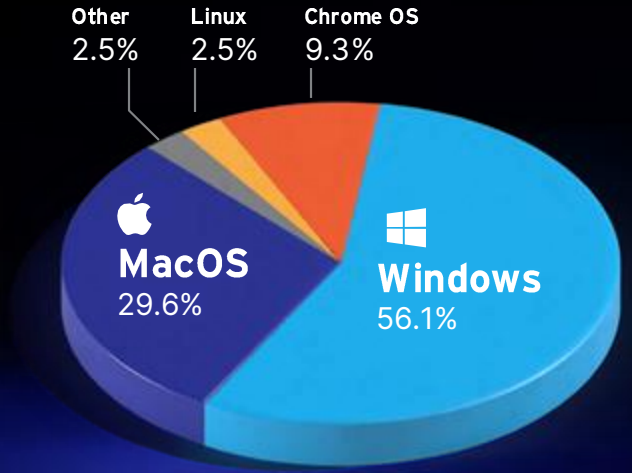
Speaker: Yoav Magid

How many of you own an Apple device?

U.S. Mobile OS Usage Share
2025



U.S. Desktop OS Usage Share
2025



How many of you use Siri?


BBC
Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live
Apple to pay $95m to settle Siri 'listening' lawsuit
7 January 2025
Share
Save
Imran Rahman-Jones
Technology reporter

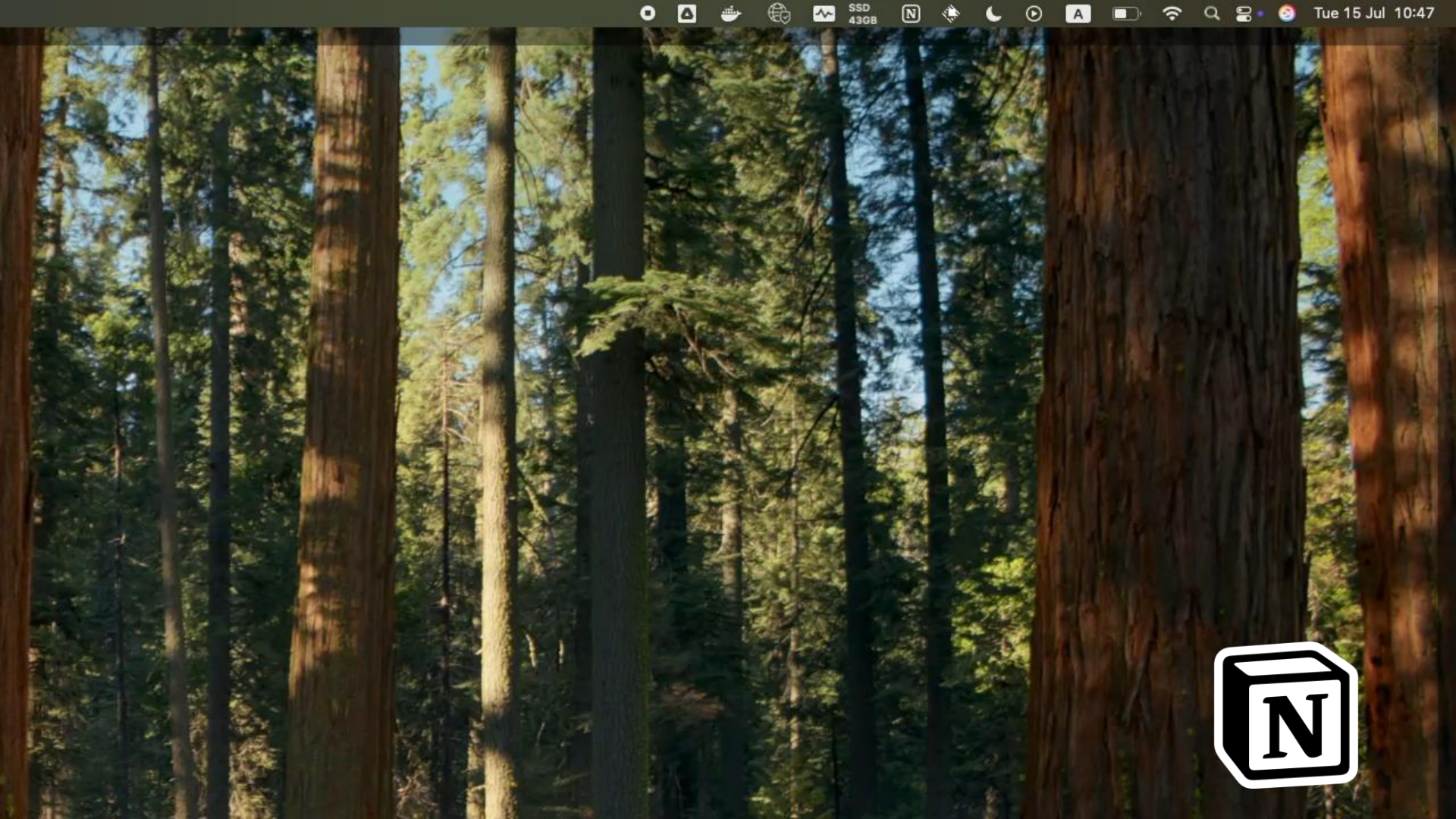
How many of you use Apple Intelligence?

Apple Intelligence

Siri

Writing Tools

Image Playground


SSD
43GB
Tue 15 Jul 10:47

Is Your Data Private? By: Yoav Magid Private Edited 2d ago Share

Is Your Data Private? By: Yoav Magid

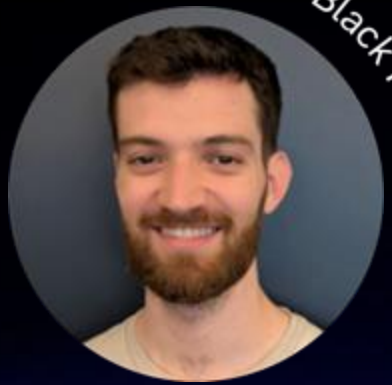
The Secret

The Secret

Yoav Magid

Team Lead & AI Researcher

lumia



Agenda

Behind Apple Intelligence's Curtains

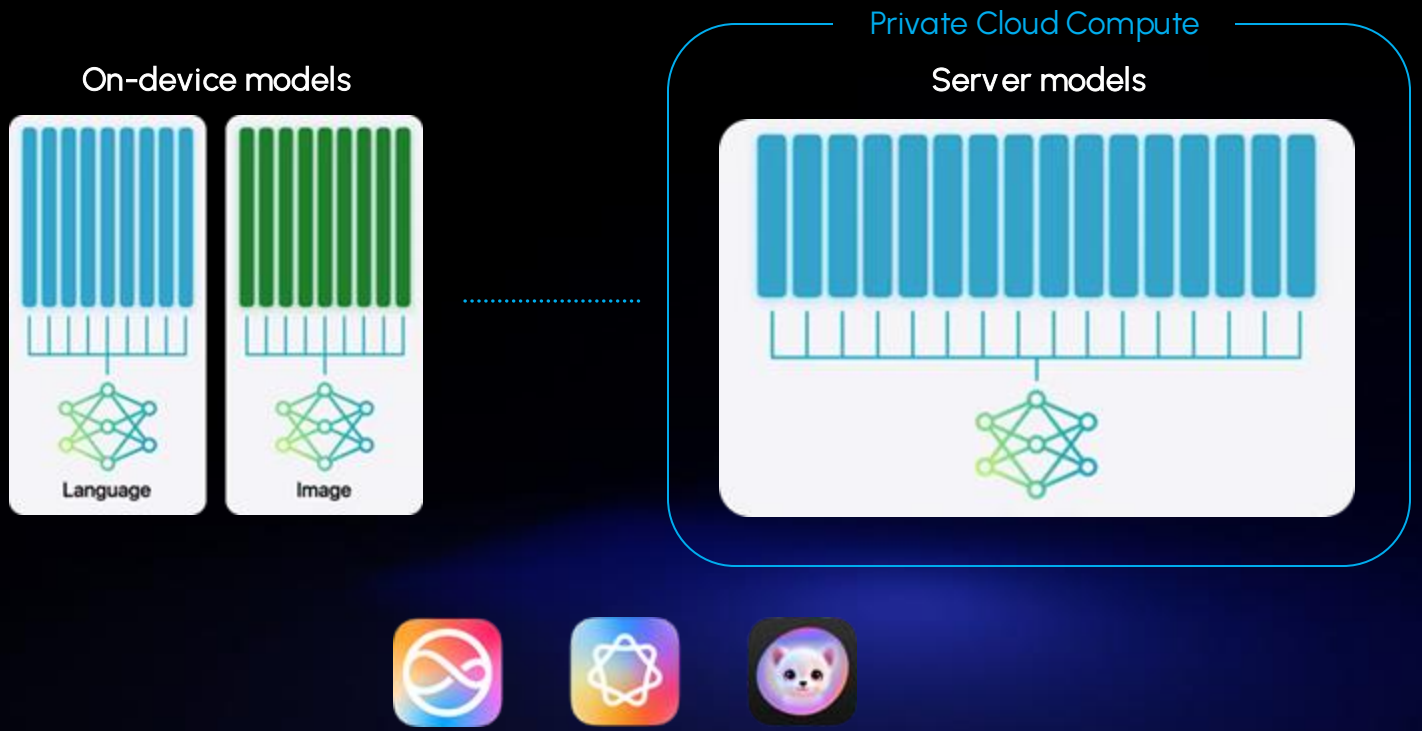
Risks & Methodology

"Hey Siri, What can you do?"

What can we do?

Apple Intelligence's Infrastructure

Enhance Productivity While Protecting Your Data!



Apple Intelligence & Privacy

Apple Intelligence is designed to protect your information.

When possible, Apple Intelligence models run entirely on device so that a task can be completed without data leaving your device. For example, when Apple Intelligence provides you with preview summaries of your emails, messages, and notifications, these summaries are generated by on-device models. There are

When you initiate an Apple Intelligence task, a model running on your device analyzes whether the task can be completed on device. If a larger, server-based model is required, Apple Intelligence uses Private Cloud Compute to send only data relevant to your request to be processed on Apple silicon servers.

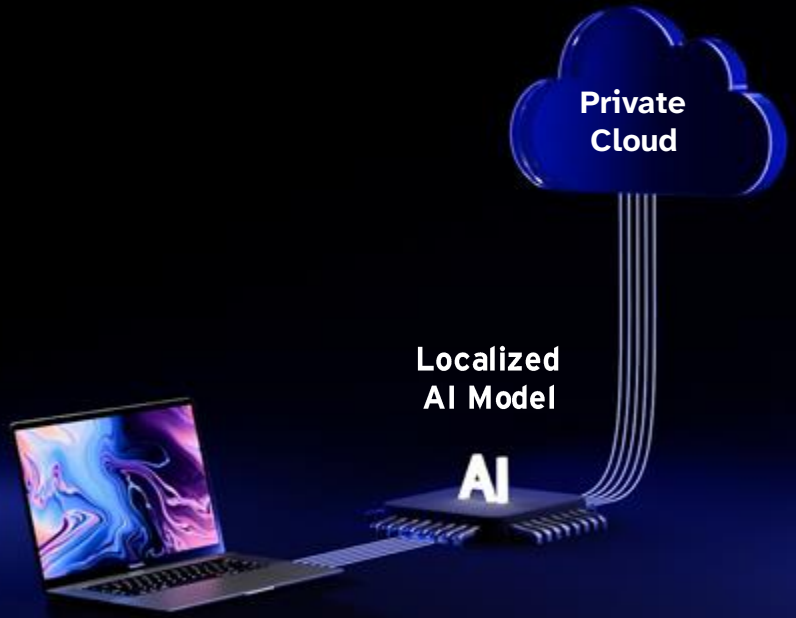
When you initiate an Apple Intelligence task, a model running on your device analyzes whether the task can be completed on device. If a larger, server-based model is required, Apple Intelligence uses Private Cloud Compute to send only data relevant to your request to be processed on Apple silicon servers. The data sent to and returned by Private Cloud Compute is not stored or made accessible to Apple. The data is processed only to fulfill your request, after which point the results are returned securely to your device and are not retained by Private Cloud Compute. When your device sends a request to Private Cloud Compute, Apple only collects limited information about the request, such as the approximate size of the request and response, which features are used for the request, and how long the request takes to complete. This data does not include any information about the content of your request or the returned result. It is not identifiable or linked to your Apple Account or other data Apple may have from your use of other Apple

Apple Intelligence, Siri, and Search

Apple devices must be able to connect to the following hosts to process Apple Intelligence requests that use Private Cloud Compute and to process Siri requests, including dictation and searching in Apple apps.

Hosts	Description
guzzoni.apple.com	Siri and dictation requests
*.smoot.apple.com	Search services, including Siri, Spotlight, Lookup, Safari, News, Messages, and Music
apple-relay.cloudflare.com	Private Cloud Compute
apple-relay.fastly-edge.com	Private Cloud Compute
cp4.cloudflare.com	Private Cloud Compute
apple-relay.apple.com	Apple Intelligence Extensions

Risks & Methodology



What?

- On-device vs. PCC
- Which data?

How?

- Network Inspection

SSL

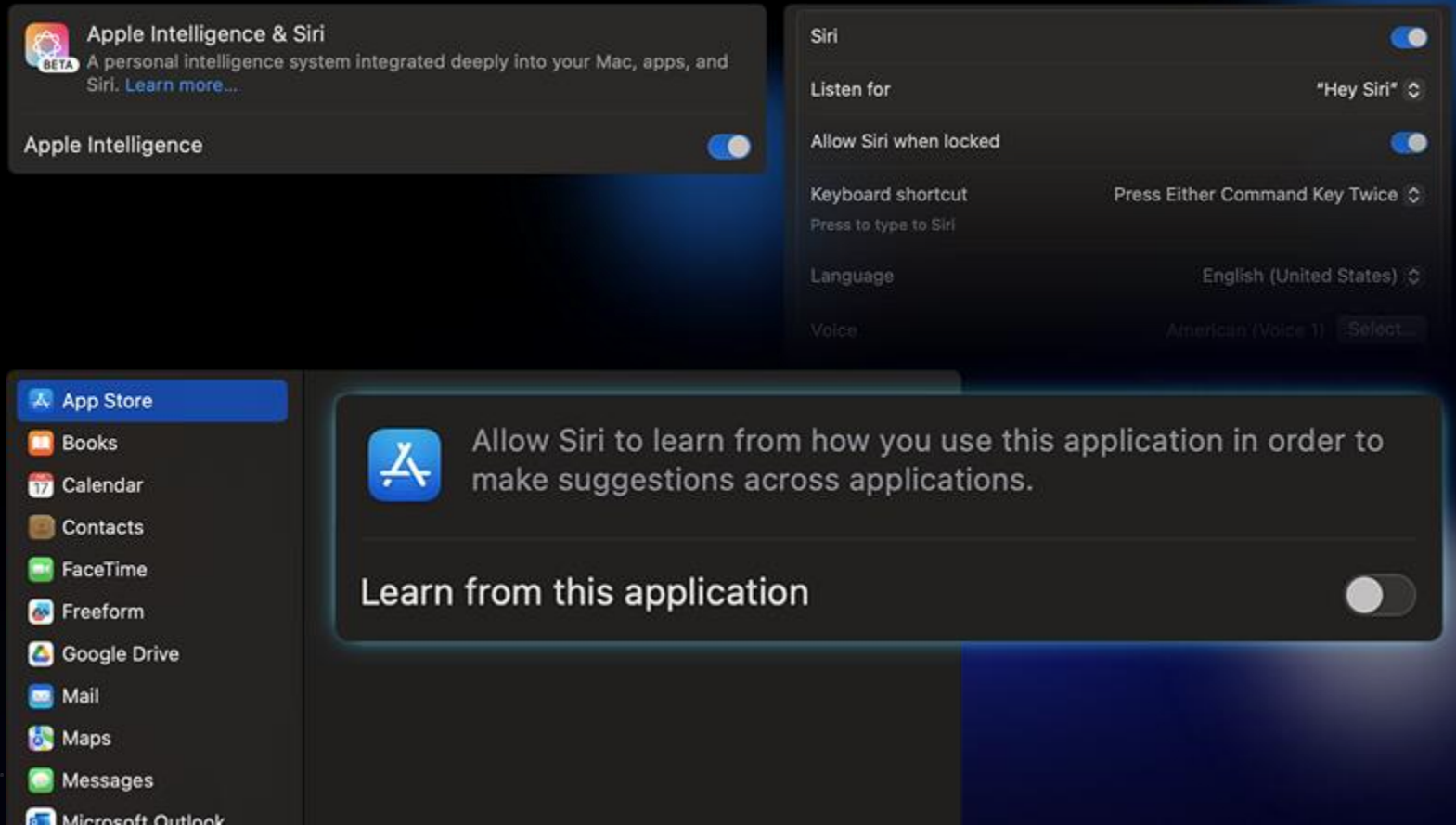
Enabled via SSL/TLS certificates issued by trusted **Certificate** Authorities.

Certificate Pinning

A technique to **"pin"** a specific certificate or public key to an **app.**

The app **rejects** all certificates not matching the pinned one to prevent Adversary-in-the-Middle.

Scenarios

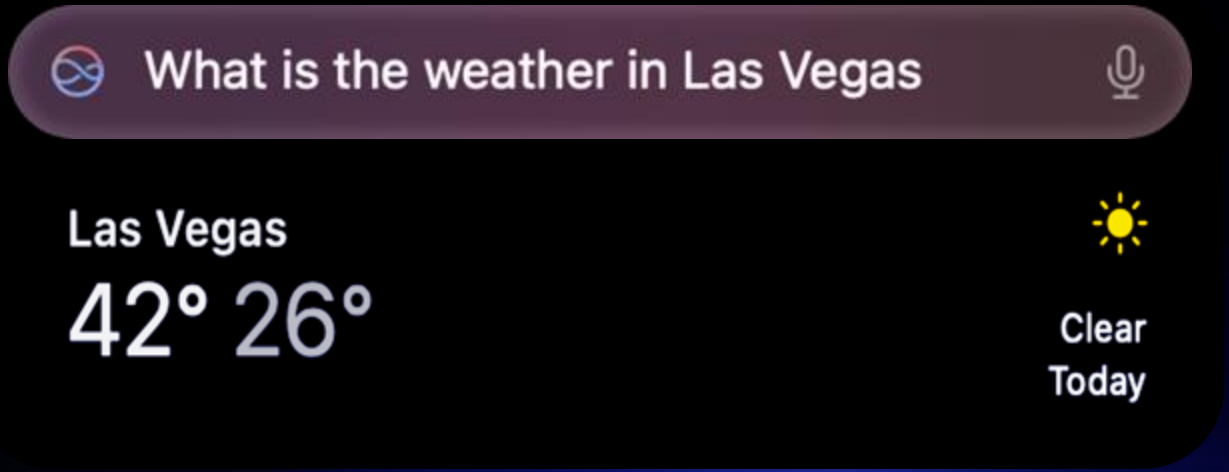

Apple Intelligence & Siri
BETA
A personal intelligence system integrated deeply into your Mac, apps, and Siri. Learn more...
Apple Intelligence
Siri
Listen for
"Hey Siri"
Allow Siri when locked
Keyboard shortcut
Press Either Command Key Twice
Press to type to Siri
Language
English (United States)
Voice
American (Voice 1)
Select...
App Store
Books
Calendar
Contacts
FaceTime
Freeform
Google Drive
Mail
Maps
Messages
Microsoft Outlook
Allow Siri to learn from how you use this application in order to make suggestions across applications.
Learn from this application

Siri

The start of a new era for Siri

"Siri draws on Apple Intelligence for new superpowers... the ability to type to Siri whenever it's convenient for you.... And with extensive product knowledge and the ability to tap into ChatGPT..."

The Prompt



Quick look – Data Frame

```
Intercepted request to api-glb-ause1c.smoot.apple.com
root:
    1 <chunk> = message:
        1 <chunk> = "What is the weather in Las Vegas"
```

Location (Latitude, Longitude)

```
1 <32bit>= 0x4214f200 / 1108668928 / 37.23633
2 <32bit>= 0xc2e79c36 / 3269958710 / -115.805098
```

```
Intercepted request to api-glb-ause1c.smoot.apple.com
```

Precise Location

If you have Location Services turned on for Siri, the location of your device at the time you make a request will be sent to Apple to help Siri and Dictation improve the accuracy of its response to your requests. To deliver relevant responses and suggestions, Apple may use the IP address of your internet connection to approximate your location by matching it to a geographic region.

If you have enabled Location Services, you can turn off Location Services for Siri by going to Settings > Privacy & Security > Location Services > Siri and tapping Never.

If you have enabled Location Services, you can turn off Location Services for Siri Suggestions by going to Settings > Privacy & Security > Location Services > System Services and tapping to turn off Suggestions & Search.

Apple's Weather App

```
1 <varint> = 9
2 <chunk> = message:
    1 <chunk> = "type.googleapis.com/apple.parsec.siri.v2alpha.AppInfo"
    2 <chunk> = message:
        1 <chunk> = "weather"
        2 <chunk> = "com.apple.weather"
        3 <varint> = 1
        4 <chunk> = "WeatherIntent"
```

```
Intercepted request to api-glb-ause1c.smoot.apple.com
```

Weather App?

```
2 <chunk> = message:
    1 <chunk> = "weather"
    2 <chunk> = "com.parallels.winapp.1441df6b1c10f910ccdc400e40b5fce9
```

```
<string>com.parallels.winapp.1441df6b1c10f910ccdc400e40b5fce9
<string>Weather</string>
```

```
Intercepted request to api-glb-ause1c.smoot.apple.com
```

Applications lists by topic

```
2 <chunk> = message:
    1 <chunk> = "type.googleapis.com/apple.parsec.siri.v2alpha.AppInfo"
    2 <chunk> = message:
        1 <chunk> = "Outlook"
        2 <chunk> = "com.microsoft.Outlook"
```

OUTLOOK

```
    1 <chunk> = "type.googleapis.com/apple.parsec.siri.v2alpha.AppInfo"
    2 <chunk> = message:
        1 <chunk> = "Vlc"
        2 <chunk> = "org.videolan.vlc"
```

VLC

```
2 <chunk> = message:
    1 <chunk> = "type.googleapis.com/apple.parsec.siri.v2alpha.AppInfo"
    2 <chunk> = message:
        1 <chunk> = "code"
        2 <chunk> = "com.microsoft.VSCode"
```

CODE

```
Intercepted request to api-glb-ause1c.smoot.apple.com
```

Active Applications

```
[{'$class': 'AppInfo',
  '$group': 'com.apple.ace.system',
  'appIdentifyingInfo': {'$class': 'AppIdentifyingInfo',
                         '$group': 'com.apple.ace.sync',
                         'bundleId': 'com.tinyspeck.slackmacgap'}}],
[{'$class': 'AppInfo',
  '$group': 'com.apple.ace.system',
  'appIdentifyingInfo': {'$class': 'AppIdentifyingInfo',
                         '$group': 'com.apple.ace.sync',
                         'bundleId': 'com.apple.finder'}}],
[{'$class': 'AppInfo',
  '$group': 'com.apple.ace.system',
  'appIdentifyingInfo': {'$class': 'AppIdentifyingInfo',
                         '$group': 'com.apple.ace.sync',
                         'bundleId': 'notion.id'}}]],
```

```
Intercepted request to guzzoni.apple.com
```

Taylor Swift?!

```
1 <chunk> = "type.googleapis.com/apple.parsec.siri.v2alpha.AudioQueueStateInfo"
2 <chunk> = message:
    1 <varint> = 2
    2 <varint> = 3
    3 <chunk> = "company.thebrowser.Browser"
    6 <chunk> = message:
        1 <chunk> = "TaylorSwiftVEVO"
        2 <chunk> = "Taylor Swift - no body, no crime (Official Lyric Video) ft.
```

```
Intercepted request to api-glb-ause1c.smoot.apple.com
```

Now Playing Queue

Metadata Query

song	Never Gonna Give You Up
artist	Rick Astley
album	Greatest Hits
album artist	Rick Astley
composer	Mike Stock, Matt Aitken & Peter Waterman
	☐ Show composer in all views
grouping	
genre	Pop
year	1987
track	1 of 17
disc number	1 of 1
compilation	☐ Album is a compilation of songs by various artists

Remember?


Your Data is not Private, By: Yoav Magid
The Secret
The Secret
0:00 / 0:30

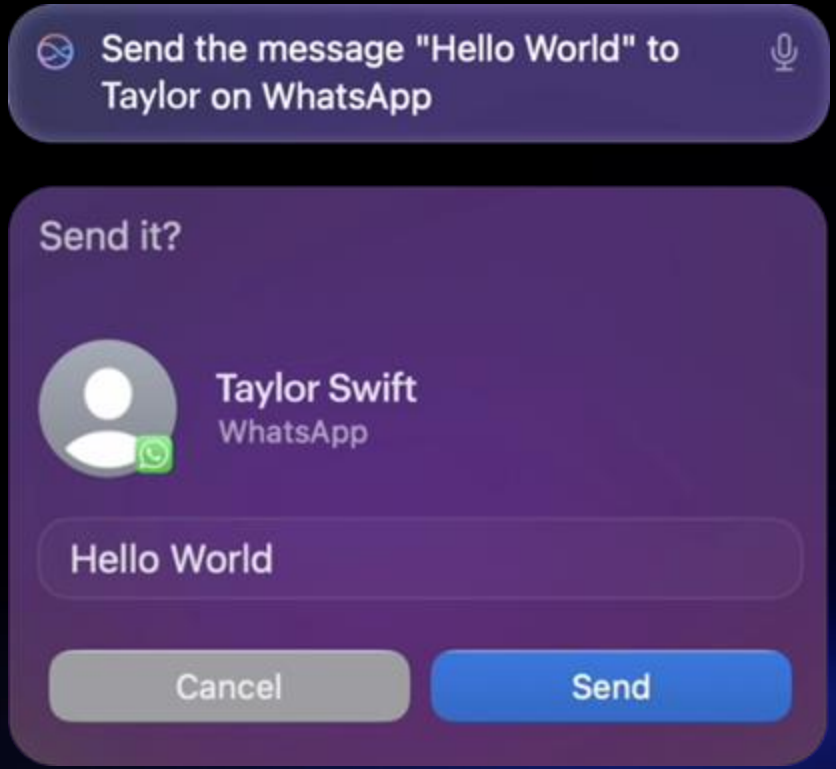
When TMI meets AI…

I just wanted to ask AI:

"What is the weather today in Las Vegas?"

However, Siri interpreted it as…

- What's the weather today in Las Vegas
- Check which weather apps I have installed
- What my favorite song is?
- BTW, do you know I have VMs on my device?


Send the message "Hello World" to Taylor on WhatsApp
Send it?
Taylor Swift
WhatsApp
Hello World
Cancel
Send

Messaging Data

*

Hello World

^ Sendh X (x-apple-siri-app://net.whatsapp.WhatsApp *$CDFF12B7-96A5-4E1F-9F23-FAD9E5C2D7CAp ^

\:% ⍰0⍰(⍰

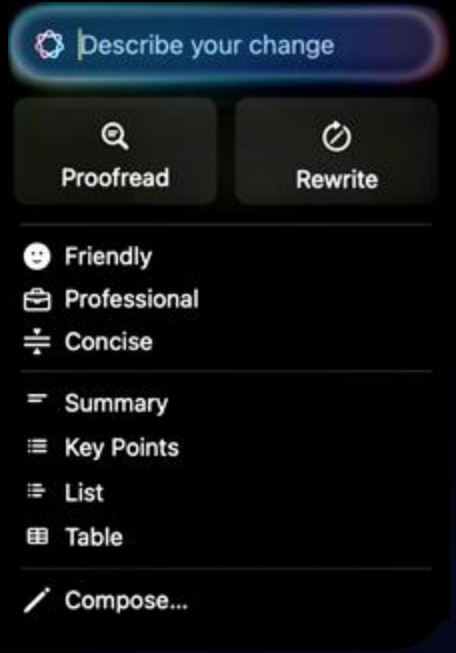
+19147772222B 19147772222@s.whatsapp.net" Taylor Swift ⍰P⍰ ⍰X⍰

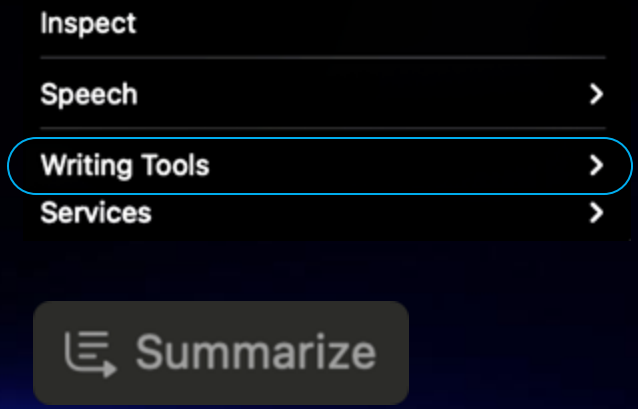
Siri Cases

CASE	ON-DEVICE/CLOUD	DATA SENT	WHERE?
Calculator	Cloud	Active Apps Speakers' Audio Apps by Topic Location	Smoot guzzoni
Weather	Cloud		
Online Search	Cloud		
Article Search	Cloud		
Message Service	On-Device	Active Apps Speakers' Audio Message Data	guzzoni
Email Service	On-Device	Active Apps Speakers' Audio	
Calendar	On-Device		

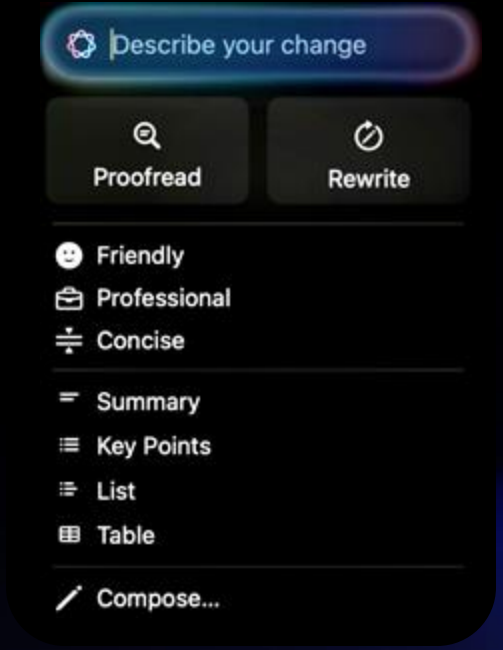
Writing Tools

Writing Tools

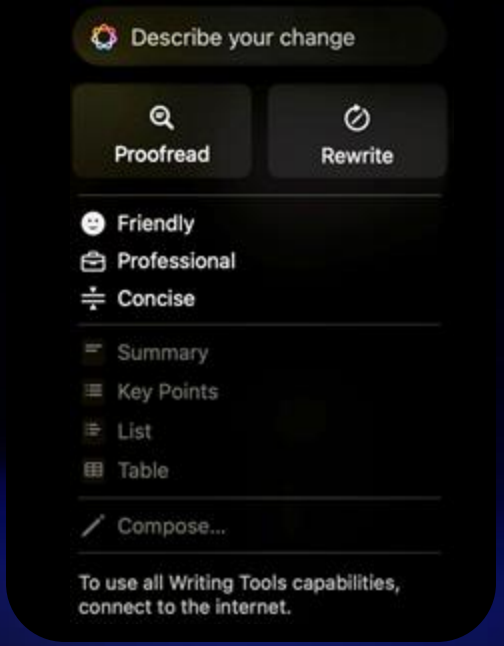




On-Device or Not?



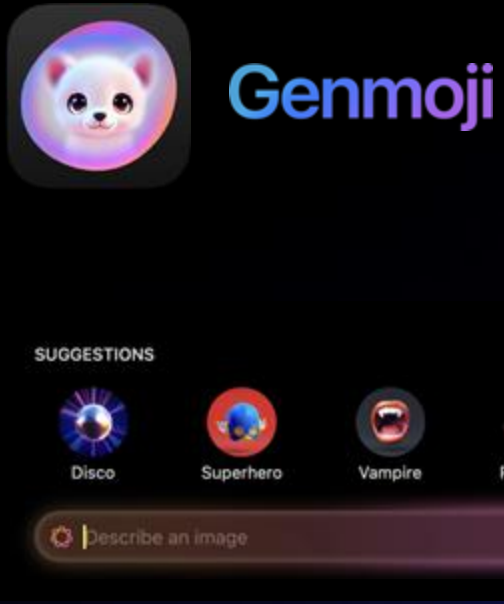
Online



Offline

Image Playground

Image Playground



Extensions

ChatGPT

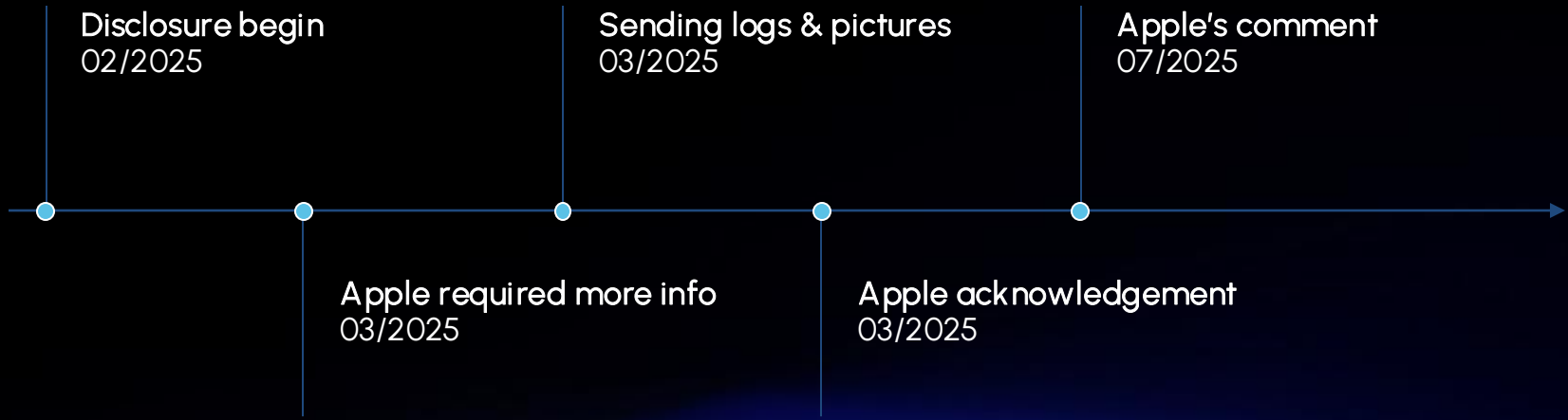
The only extension of Apple Intelligence

Accessible via Siri & Writing Tools (Show Images)

Proxy through Apple Servers and not directly with OpenAI

Some requests are duplicated to Siri Search

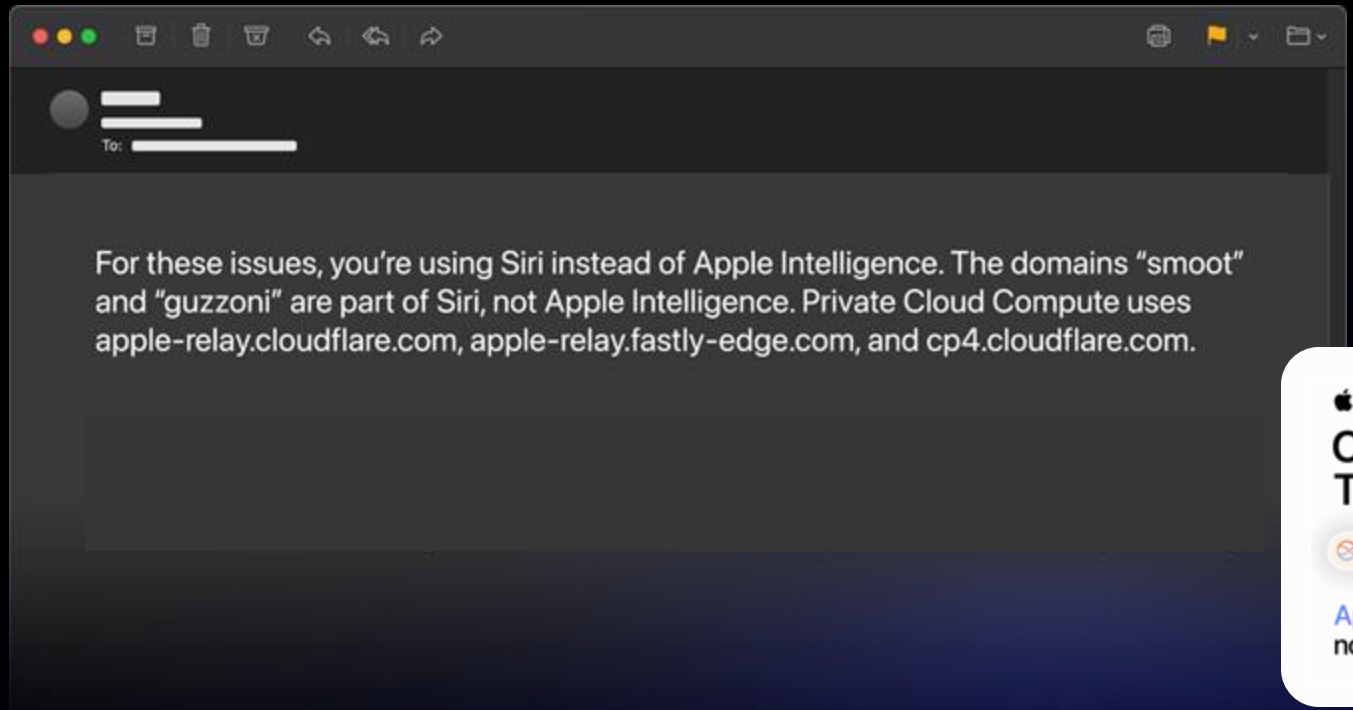
Disclosure Timeline



We're planning to address the issue you reported.

We're working with our engineering teams and have an initial plan to resolve the issue.

Apple Response



SiriKit Test

Developer

```
*
  See you soon
d  Sendh X  .x-apple-siri-app://Yoav-Lumia.TestMessagingAPP  *$756DB956-9C9A-45EB-8423-3ACFD5991249p
   John" John ▯P▯ ▯ ▯X▯
```

Mitigations

1. Block any network traffic to guzzoni.apple.com – does not hinder functionality
2. Disable any settings of apps that you are not willing to share

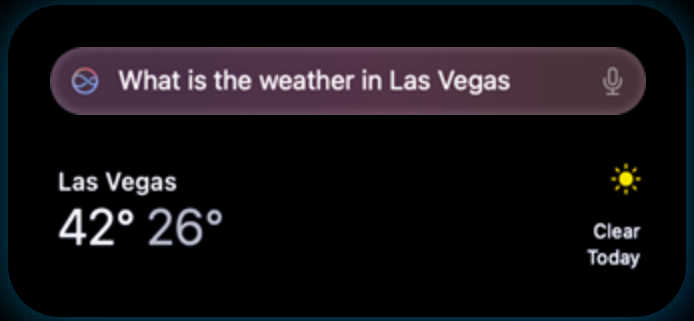
APP	DOMAINS	DATA SENT
Siri	guzzoni.apple.com	Active Apps Messaging Data Speakers' Audio
	*.smoot.apple.com	Apps by Topic Location Speakers' Audio
Writing Tools	apple-relay.cloudflare.com apple-relay.fastly-edge.com cp4.cloudflare.com (Private Cloud Compute)	Relevant Data
Image Playground	-	-
Extensions - ChatGPT	apple-relay.apple.com (PCC) *.smoot.apple.com (Siri)	Prompt Auth (only PCC)

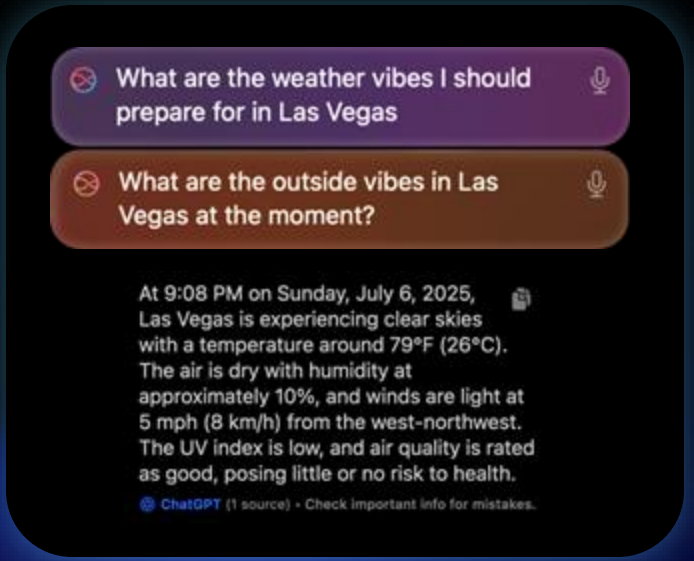
Takeaways

1. Privacy Policy - To Read or not to Read?
2. Implement Careful Network-Level Monitoring
3. Transparency from AI Vendors
   - Pinning should not be an obstacle

Retrospective

Apple Intelligence VS Siri





2 Terms of Use • 2 Privacy Policies

Same App

Can you tell the difference?

Thank you for listening!

Q&A