DEFCON

AppleStorm:

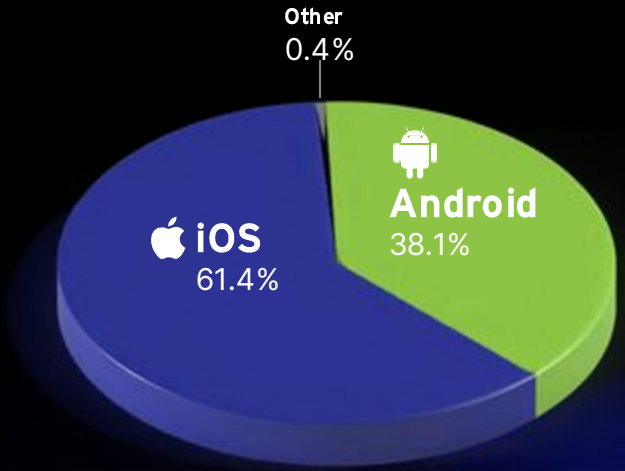
Unmasking the Privacy Risks of Apple Intelligence

Speaker: Yoav Magid

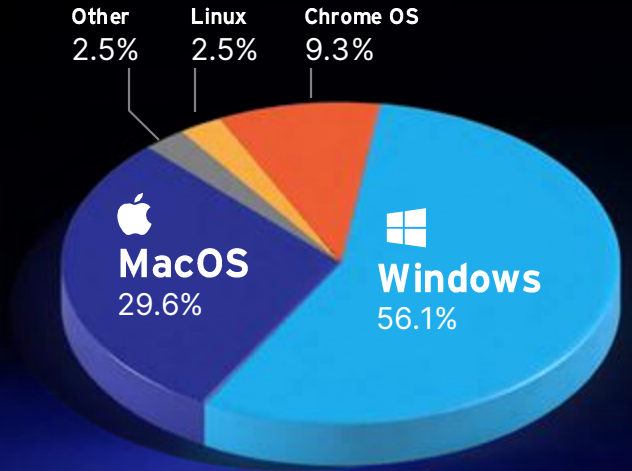


How many of you own an Apple device?

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



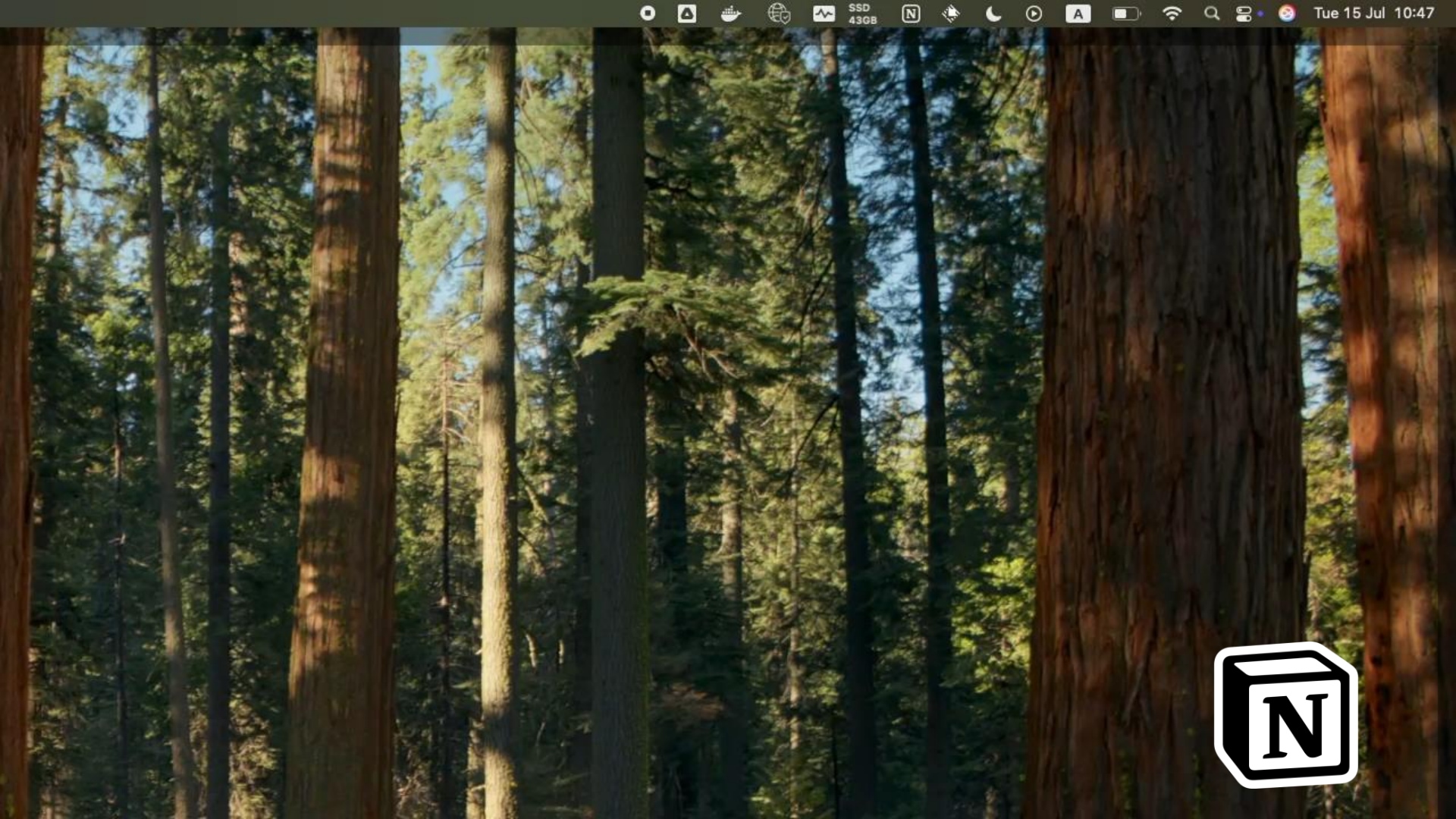
Siri



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

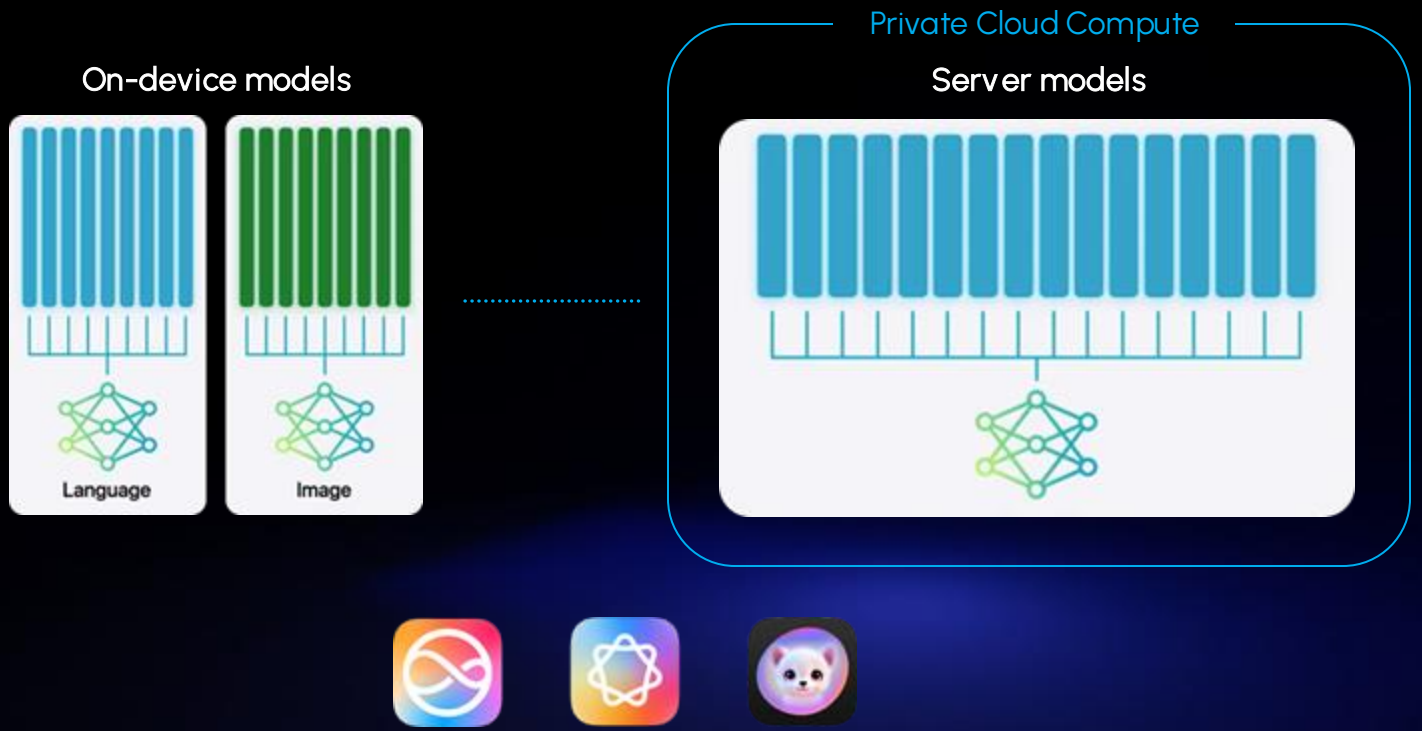
"Hey Siri, What can you do?"

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,
apple-r	d Music
apple-r	
cp4.clou	
apple-relay.ap	

```
TCP_MISS/200 4931 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.253 -
TCP_MISS/200 4656 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.253 -
TCP_MISS/200 4656 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.253 -
TCP_MISS/200 4931 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.253 -
TCP_MISS/200 4629 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.253 -
TCP_MISS/200 4656 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.250 -
TCP_MISS/200 4930 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.250 -
TCP_MISS/200 4656 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.250 -
TCP_MISS/200 4931 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.250 -
TCP_MISS/200 4656 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.248 -
TCP_MISS/200 5206 CONNECT api.smoot.apple.com:443 - HIER_DIRECT/17.252.11.248 -
TCP_MISS/200 6959 CONNECT bookkeeper.itunes.apple.com:443 - HIER_DIRECT/23.217.226
TCP_MISS/200 6959 CONNECT bookkeeper.itunes.apple.com:443 - HIER_DIRECT/23.217.226
TCP_MISS/200 1041 CONNECT bookkeeper.itunes.apple.com:443 - HIER_DIRECT/23.217.226
TCP_MISS/200 6959 CONNECT bookkeeper.itunes.apple.com:443 - HIER_DIRECT/23.217.226
TCP_MISS/200 1057 CONNECT bookkeeper.itunes.apple.com:443 - HIER_DIRECT/23.217.226
TCP_MISS/200 22836 CONNECT init.itunes.apple.com:443 - HIER_DIRECT/23.217.226.217
TCP_MISS/200 22868 CONNECT init.itunes.apple.com:443 - HIER_DIRECT/23.217.226.217
TCP_MISS/200 5155 CONNECT xp.apple.com:443 - HIER_DIRECT/17.154.66.107 -
TCP_MISS/200 5155 CONNECT xp.apple.com:443 - HIER_DIRECT/17.154.66.107 -
```

Risks & Methodology



What?

- On-device vs. PCC
- Which data?

How?

- Network Inspection



Siri Search

Dictation

HTTPS Connection

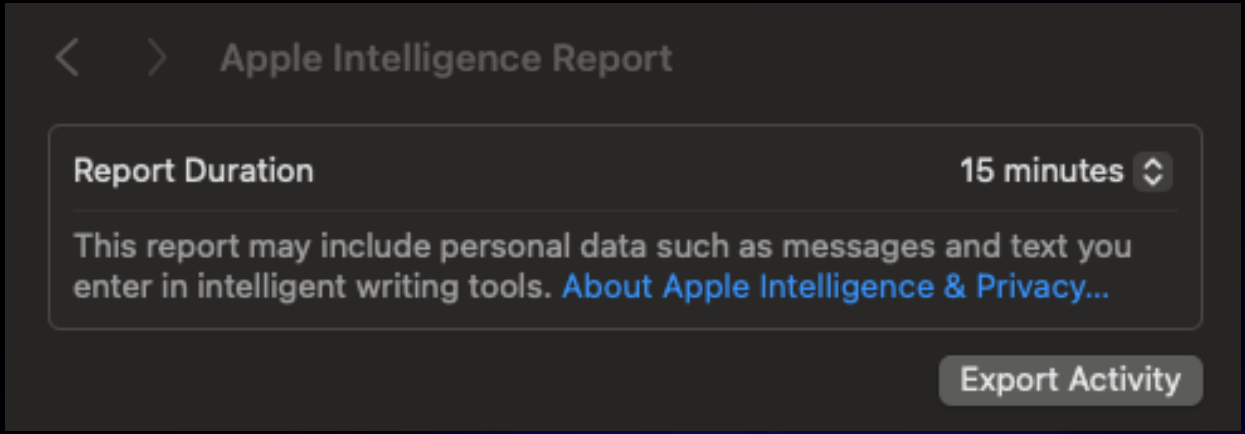


Cloud Models

Extensions

QUIC Connection

Private Cloud Compute



System Settings -> Privacy & Security -> Apple Intelligence Report

Siri's Services



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.

Tools





assitantd

```
assistantd.1983
    tcp4 127.0.0.1:64523
```

```
     ____
    / _  |   Frida 15.0.18 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .     object?   -> Display information about 'object'
   . . . .     exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
Failed to attach: process with pid 61244 either refused to load frida-agent, or terminated during injection
```

System Integrity Protection

System Integrity Protection is a security technology designed to help prevent potentially malicious software from modifying protected files and folders on your Mac. System Integrity Protection restricts the root user account and limits the actions that the root user can perform on protected parts of the Mac operating system.

Disable System Integrity Protection Temporarily

To disable SIP, do the following:

1. Restart your computer in Recovery mode.
2. Launch Terminal from the Utilities menu.
3. Run the command `csrutil disable`.
4. Restart your computer.

Breaking the Certificate Pinning

```
// SSL_CTX_set_custom_verify configures certificate verification. |mode| is one
// of the |SSL_VERIFY_*| values defined above. |callback| performs the
// certificate verification.
//
// The callback may call |SSL_get0_peer_certificates| for the certificate chain
// to validate. The callback should return |ssl_verify_ok| if the certificate is
// valid. If the certificate is invalid, the callback should return
// |ssl_verify_invalid| and optionally set |*out_alert| to an alert to send to
// the peer. Some useful alerts include |SSL_AD_CERTIFICATE_EXPIRED|,
// |SSL_AD_CERTIFICATE_REVOKED|, |SSL_AD_UNKNOWN_CA|, |SSL_AD_BAD_CERTIFICATE|,
// |SSL_AD_CERTIFICATE_UNKNOWN|, and |SSL_AD_INTERNAL_ERROR|. See RFC 5246
// section 7.2.2 for their precise meanings. If unspecified,
// |SSL_AD_CERTIFICATE_UNKNOWN| will be sent by default.
//
// To verify a certificate asynchronously, the callback may return
// |ssl_verify_retry|. The handshake will then pause with |SSL_get_error|
// returning |SSL_ERROR_WANT_CERTIFICATE_VERIFY|.
OPENSSL_EXPORT void SSL_CTX_set_custom_verify(
    SSL_CTX *ctx, int mode,
    enum ssl_verify_result_t (*callback)(SSL *ssl, uint8_t *out_alert));
```

```
// SSL_VERIFY_NONE, on a client, verifies the server certificate but does not
// make errors fatal. The result may be checked with |SSL_get_verify_result|. On
// a server it does not request a client certificate. This is the default.
#define SSL_VERIFY_NONE 0x00

// SSL_VERIFY_PEER, on a client, makes server certificate errors fatal. On a
// server it requests a client certificate and makes errors fatal. However,
// anonymous clients are still allowed. See
// |SSL_VERIFY_FAIL_IF_NO_PEER_CERT|.
#define SSL_VERIFY_PEER 0x01

// SSL_VERIFY_FAIL_IF_NO_PEER_CERT configures a server to reject connections if
// the client declines to send a certificate. This flag must be used together
// with |SSL_VERIFY_PEER|, otherwise it won't work.
#define SSL_VERIFY_FAIL_IF_NO_PEER_CERT 0x02
```

```
Called boringssl_context_set_verify_mode: 0xb45c43800 0x3
```

ACE What?

```
ACE https://guzzoni.apple.com/ace HTTP/1.0
Host: guzzoni.apple.com
X-Ace-Host: ml11sa
X-Client-Connection-Id: 6D2FDE4F-2585-4629-9C4D-895FFCE81E9A
X-Sync-Owner-Assistant-ID: 85534DF3-C83C-4202-B486-37D3F99AC346
User-Agent: Assistant(macOS/Mac15,6; macOS/15.2/24C101) Ace/13.0-20A
Accept-Language: en-US
Content-Length: 2000000000
```

Edit | Replace | View: auto

```
content missing
```

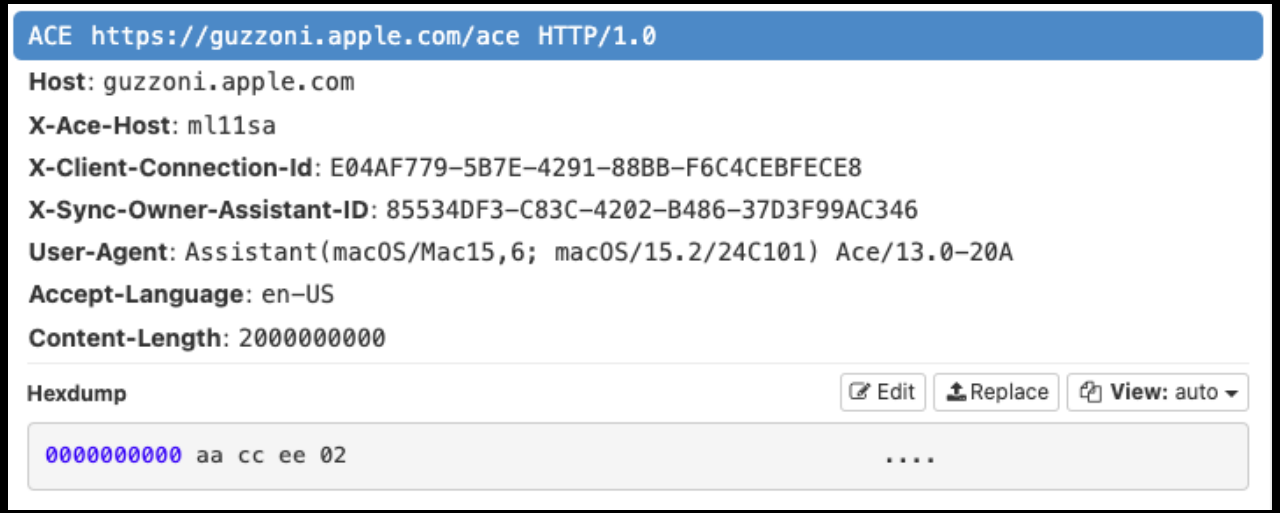
HTTP/1 protocol error: peer closed connection without sending complete message body (received 4 bytes, expected 2000000000)

Patching Mitmproxy

```
#    5.  If a valid Content-Length header field is present without
#        Transfer-Encoding, its decimal value defines the expected message
#        body length in octets.  If the sender closes the connection or
```

```
#    5.  If a valid Content-Length header field is present without
#        Transfer-Encoding, its decimal value defines the expected message
#        body length in octets.  If the sender closes the connection or
#        the recipient times out before the indicated number of octets are
#        received, the recipient MUST consider the message to be
#        incomplete and close the connection.
if cl := headers.get("content-length"):
    parsed_content_length = validate.parse_content_length(cl)
    if parsed_content_length == 2000000000: ⇥ tab
        return -1
    return parsed_content_length
```

AA CC EE


ACE https://guzzoni.apple.com/ace HTTP/1.0
Host: guzzoni.apple.com
X-Ace-Host: ml11sa
X-Client-Connection-Id: E04AF779-5B7E-4291-88BB-F6C4CEBFECE8
X-Sync-Owner-Assistant-ID: 85534DF3-C83C-4202-B486-37D3F99AC346
User-Agent: Assistant(macOS/Mac15,6; macOS/15.2/24C101) Ace/13.0-20A
Accept-Language: en-US
Content-Length: 2000000000
Hexdump
Edit
Replace
View: auto
0000000000 aa cc ee 02 ....

Decoding ACE Protocol

Step 1

Magic

AA BB CC 02

Step 2

Zlib

0x78DA

Step 3

Commands

"bplist"

"Keep-Alive"

Step 4

ProtoBuf

"baes64Proto"

Dealing with Siri Communications

Step 1

Proxy

Step 2

Protobuf Decoder

Step 3

Analyze

Step 1

Disable certificate pinning

Step 2

Proxy

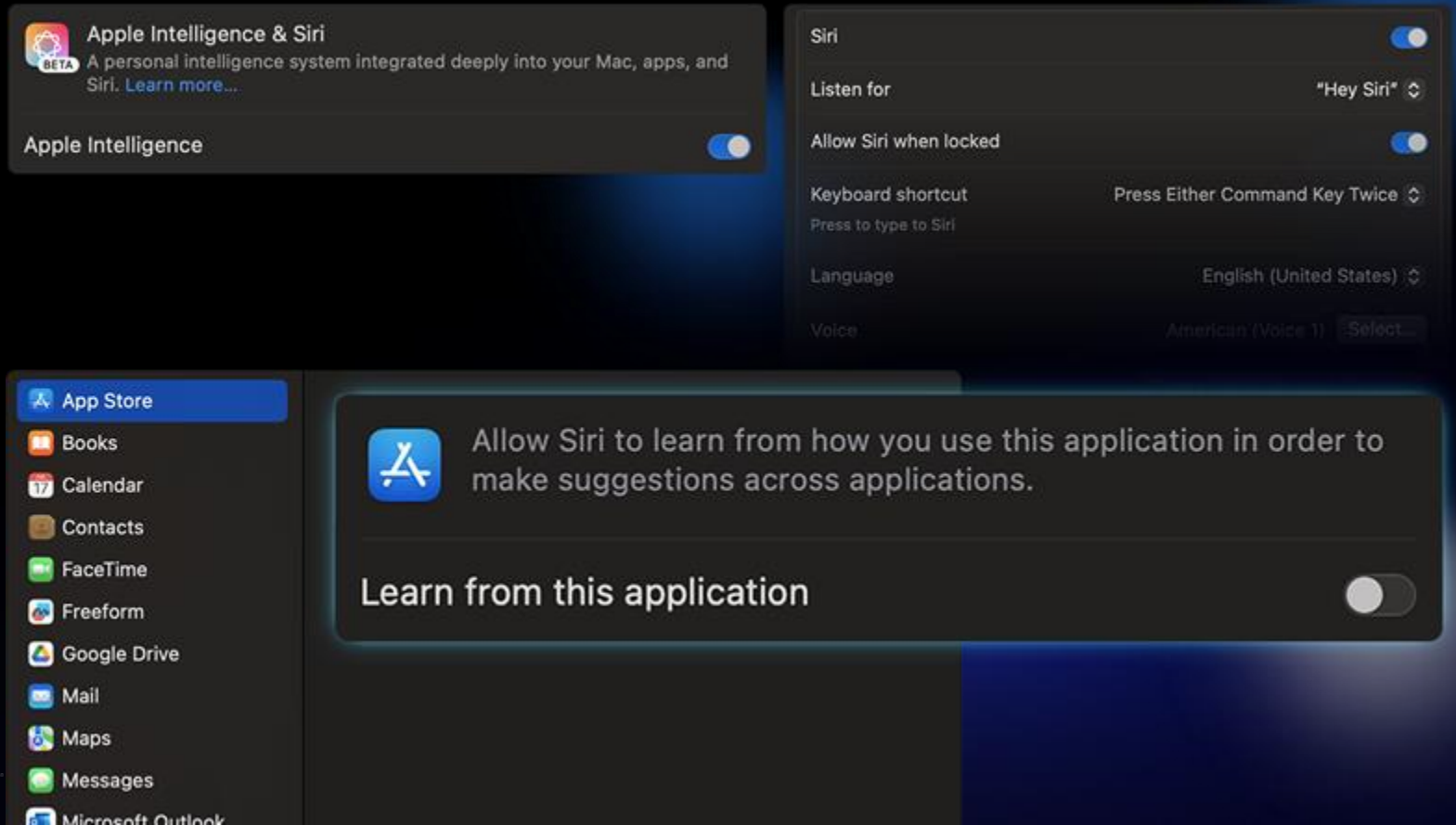
Step 3

ACE Parser

Step 4

Analyze

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



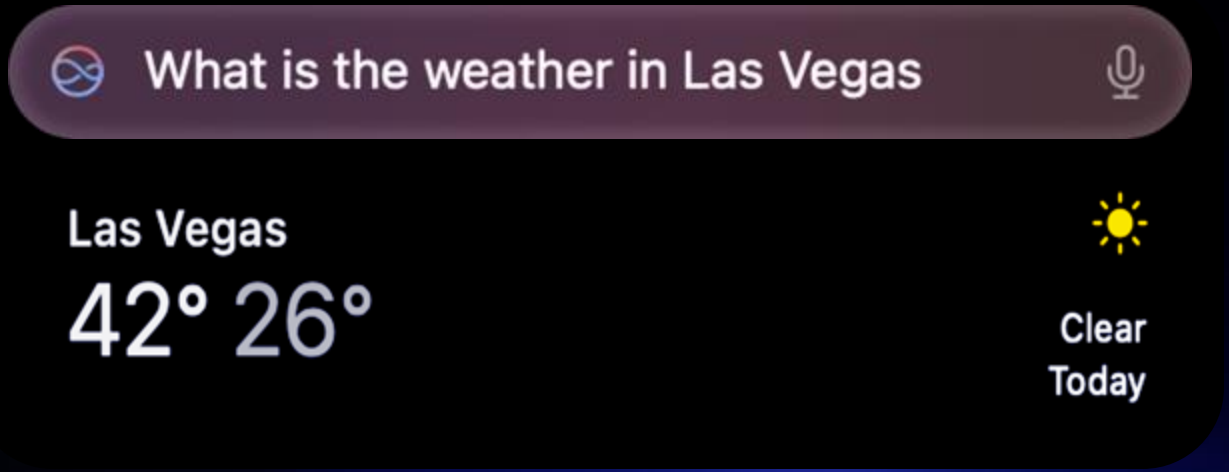
Siri



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
```

NowPlaying 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...

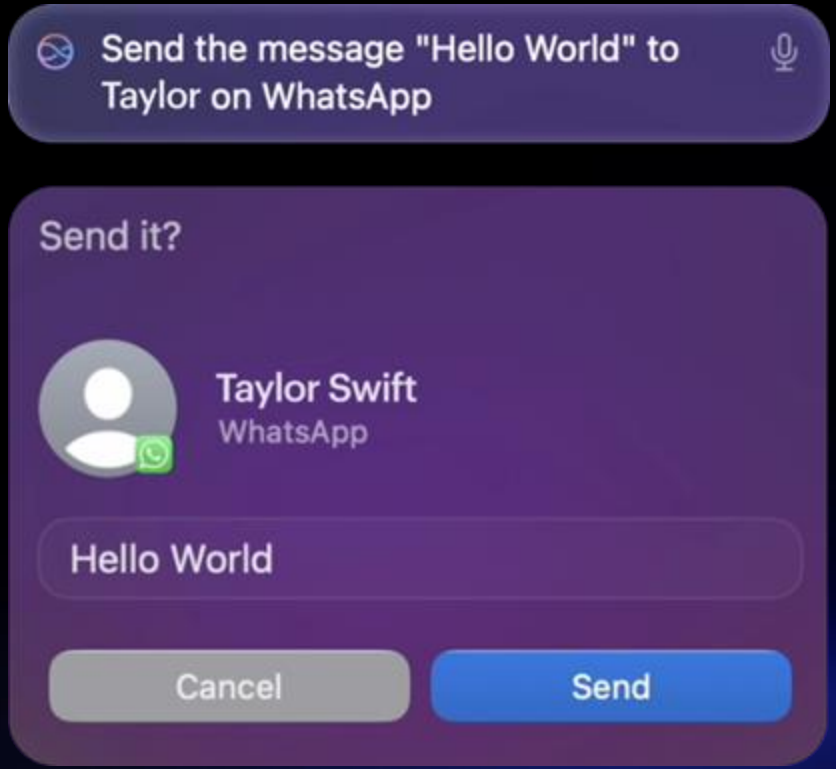


I just wanted to ask AI:

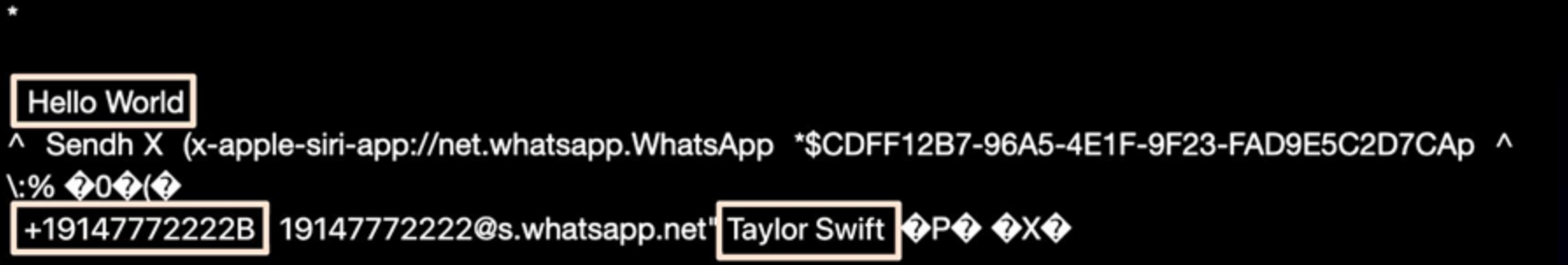
"What is the weather today in Las Vegas?"

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

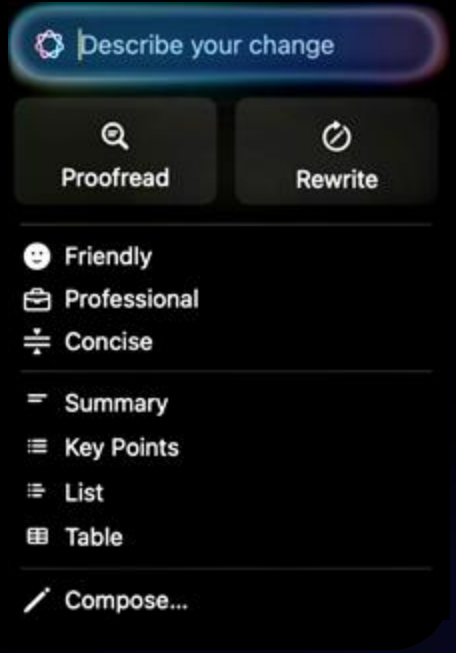


Siri Cases

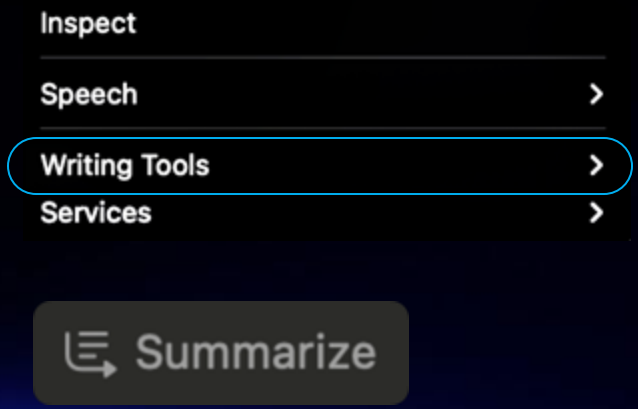
CASE	ON-DEVICE/CLOUD	DATA SENT	WHERE?
Calculator	Cloud	Active Apps Speakers' Audio Apps by Topic Location	Smoot guzzoni
Weather	Cloud		
Online Search	Cloud		
Article Search	Cloud		
Message Service	On-Device	Active Apps Speakers' Audio Message Data	guzzoni
Email Service	On-Device	Active Apps Speakers'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

Writing Tools

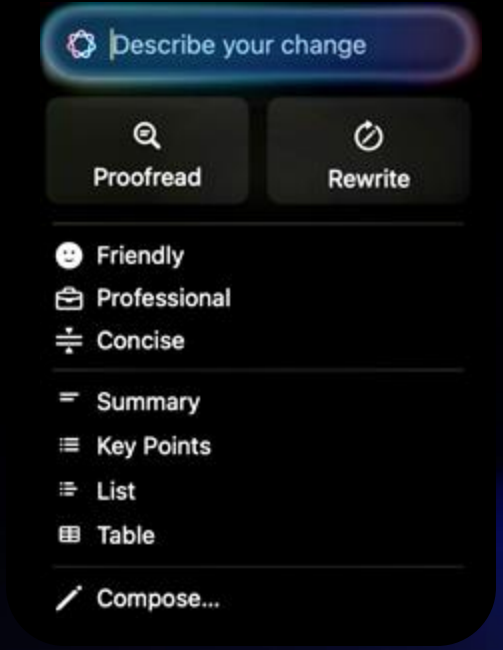
Writing Tools



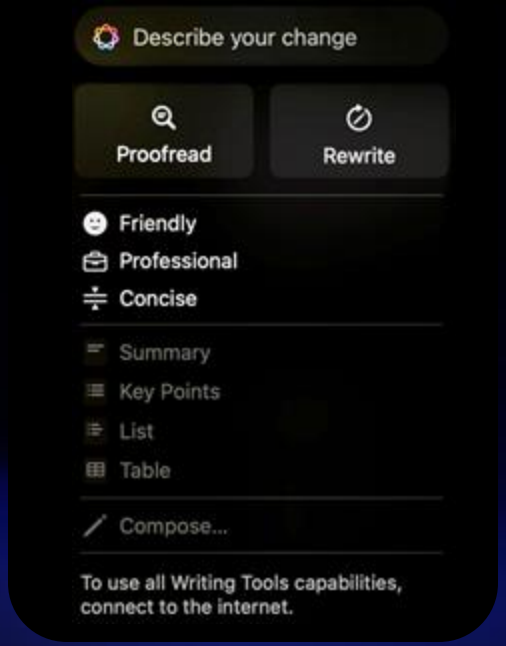




On-Device or Not?



Online



Offline

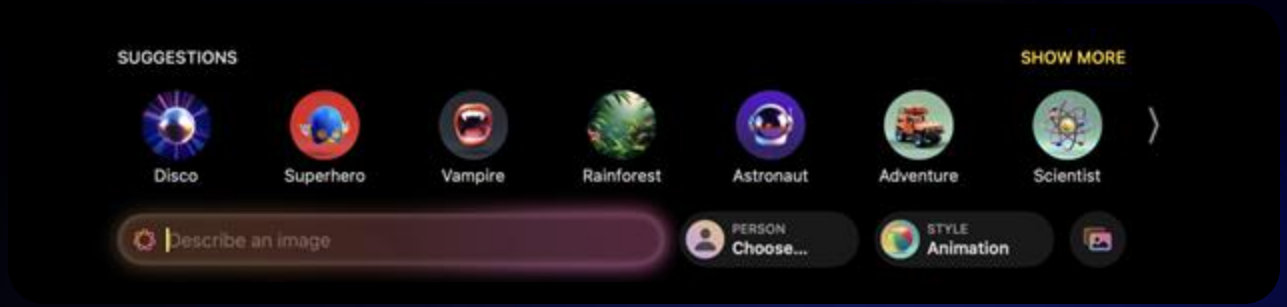
Image Playground

Image Playground



Genmoji

Describe an image or add a suggestion from the list.



Extensions

ChatGPT

The only extension of Apple Intelligence



Accessible via Siri & Writing Tools (Show Images)

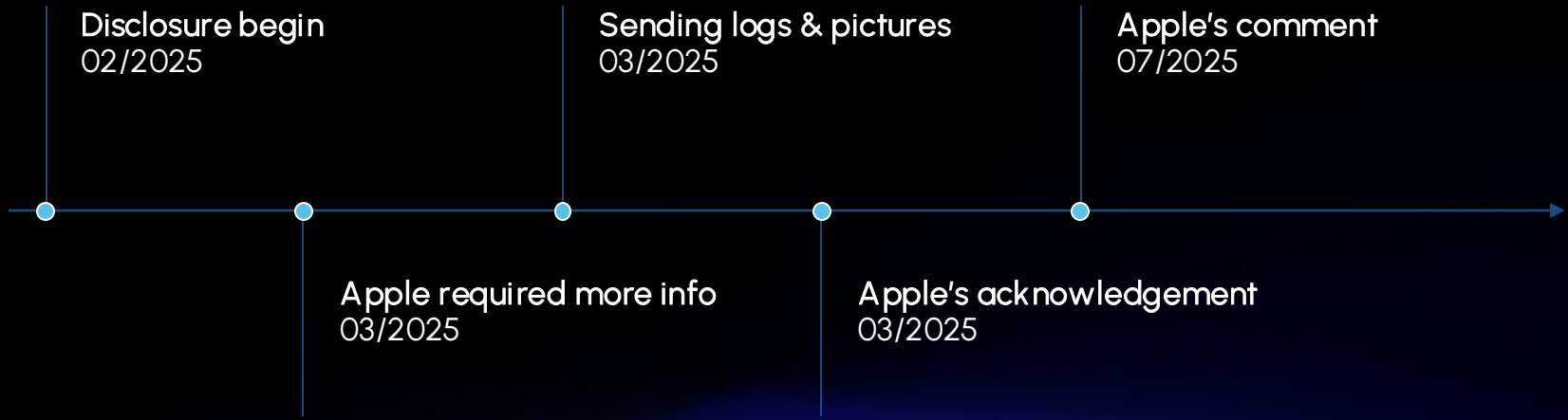


Proxy through Apple Servers and not directly with OpenAI

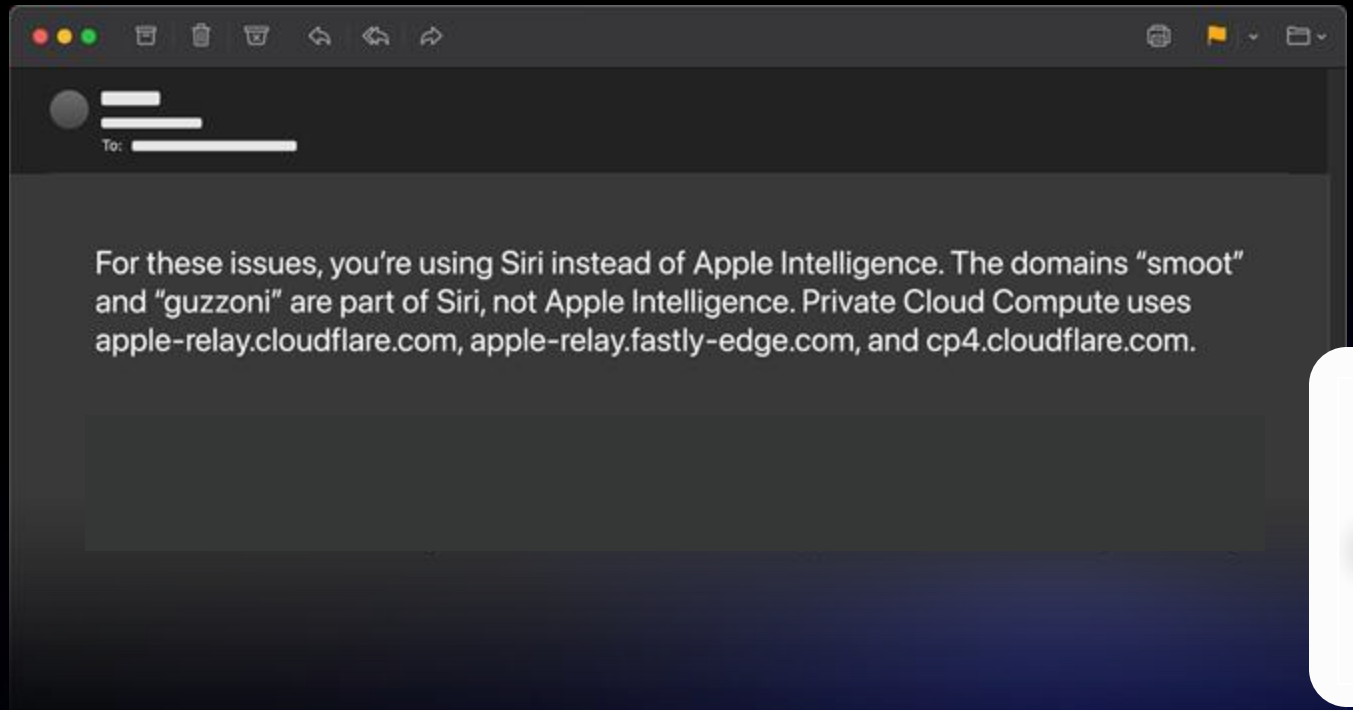
Some requests are duplicated to Siri Search



Disclosure Timeline



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

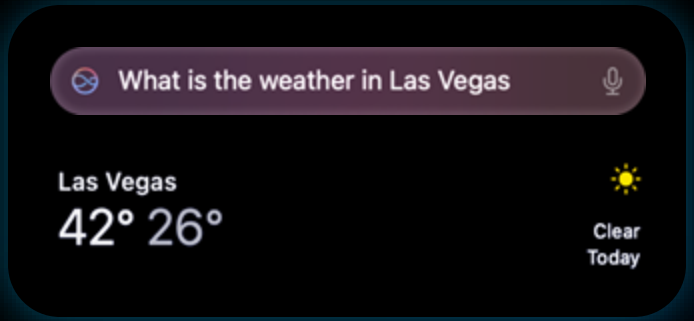
APP	DOMAINS	DATA SENT
Siri	guzzoni.apple.com	Active Apps Messaging Data Speakers' Audio
	*.smoot.apple.com	Apps by Topic Location Speakers' Audio
Writing Tools	apple-relay.cloudflare.com apple-relay.fastly-edge.com cp4.cloudflare.com (Private Cloud Compute)	Relevant Data
Image Playground	-	-
Extensions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

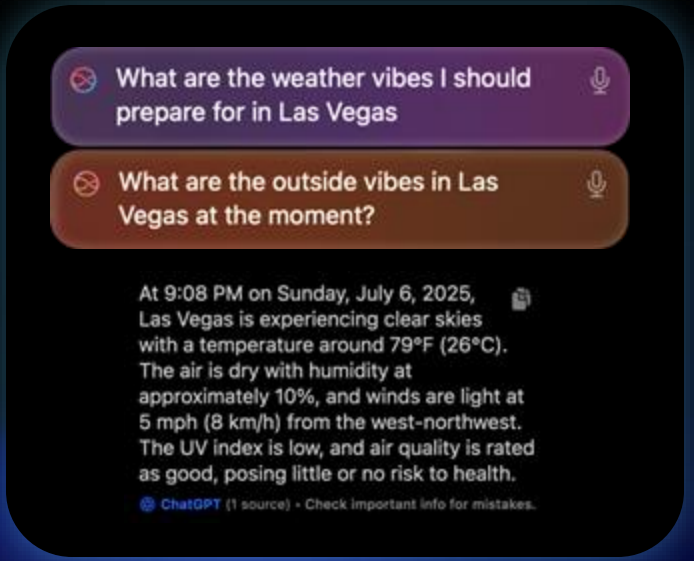
Takeaways

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

Can you tell the difference?

Thank you for listening!

Q&A