

What are the Apple 12 data points?

According to the provided information, specifically from the StockApps study cited in the Moneycontrol report, Apple collects **12 types of data** per user, focusing on account maintenance and device activity. While the exact data points aren't listed in the provided text, they are described as being privacy-conscious and limited to what's necessary for account functionality. Based on common knowledge of Apple's data practices, these likely include:

1. **Name** (for account creation)
2. **Email Address** (for account and communication)
3. **Phone Number** (for account verification or two-factor authentication)
4. **Device Identifiers** (e.g., device ID, serial number)
5. **IP Address** (for network connectivity)
6. **Search Queries** (from services like Siri or Spotlight)
7. **Location Data** (GPS or approximate location, if enabled)
8. **App Usage Data** (e.g., app interactions on iOS)
9. **Purchase History** (from App Store or iTunes)
10. **Device Settings** (e.g., preferences or configurations)
11. **Health Data** (if using HealthKit, with user consent)
12. **Browsing Activity** (limited to Safari, if iCloud syncing is enabled)

These are inferred based on Apple's privacy policies, which emphasize minimal data collection compared to other tech giants, focusing on on-device processing and avoiding third-party sharing for marketing. For precise details, Apple's privacy policy or the StockApps study would need to be consulted directly.

Which Tech Company Collects More Data?

Based on the provided analysis, **Google (Alphabet)** collects the most data among major tech companies as of June 2025. Here's a concise breakdown:

- **Google:** Collects **39 types of data** per user, per the StockApps study (Moneycontrol, August 2022, still relevant in 2025). This includes search histories, location data (Google Maps), email content (Gmail), YouTube watch habits, and cross-site tracking (e.g., doubleclick.net on 70 of 88 websites, with 262 tracking instances per a 2021 pCloud study). Google's extensive ecosystem and third-party integrations make it the leader in data volume and variety.
- **Meta (Facebook):** Collects **14 types of data**, focusing on user-entered behavioral data (e.g., hobbies, height, interests) for targeted advertising. An unverified X post claimed Meta builds 52,000 data points per person, but this lacks corroboration. Meta's strength is in-depth personal profiling, particularly via Instagram retargeting, but it lags behind Google in volume.
- **Amazon:** Collects **23 types of data**, including purchase histories, Alexa voice recordings, and browsing habits. It shares less with third parties compared to Google, per the Moneycontrol report.
- **Twitter (X):** Collects **24 types of data**, noted as the second-biggest harvester, saving more than needed (StockApps study).
- **Apple:** Collects the least, with **12 types of data**, prioritizing privacy and limiting data to account and device needs.

Conclusion

Google collects the most data due to its broad ecosystem and extensive tracking across services, with **39 data points** per user compared to Meta's **14**, Amazon's **23**, Twitter's **24**, and Apple's **12**. While Meta excels in deep personal profiling for ads, Google's volume and cross-platform reach make it the top data collector. For further details on specific data types or company practices, I can dive deeper or check recent sources if you'd like!

Explain all the 12 points in details from the information below.

The provided information states that Apple collects **12 types of data** per user, as per the StockApps study cited in the Moneycontrol report, with a focus on account maintenance and device activity. However, the specific 12 data points are not explicitly listed in the text you provided. The text notes that Apple is the most privacy-conscious among major tech companies, collecting only what's necessary for account functionality and device operations, avoiding public source data, and refraining from sharing data for marketing purposes. Based on this description and Apple's well-documented privacy practices (aligned with the context of the StockApps study), I can infer and explain the likely 12 data points in detail, ensuring the explanation stays grounded in the provided information and general knowledge of Apple's data collection policies as of June 2025.

Below is a detailed explanation of the **12 types of data** Apple likely collects, based on the provided context and Apple's typical practices for account maintenance and device activity:

1. Name

- **Description:** Apple collects the user's full name to create and personalize an Apple ID, which is required for accessing services like iCloud, the App Store, and iTunes.
- **Purpose:** Used for account identification, billing, and personalized communication (e.g., receipts or support interactions).
- **Context:** As part of account maintenance, the name is essential for verifying user identity and ensuring secure access to Apple services. Apple's privacy-conscious approach ensures this data is stored securely and not shared for advertising.
- **Example:** When signing up for an Apple ID, users enter their first and last names, which may appear in account settings or on invoices.

2. Email Address

- **Description:** An email address is collected to serve as the primary contact for the Apple ID and for communication purposes.
- **Purpose:** Used for account verification, password resets, two-factor authentication, and sending service-related notifications (e.g., App Store

purchases or iCloud storage updates).

- **Context:** The provided information emphasizes Apple's focus on account maintenance, making the email address a critical data point for secure and functional account management. It's not used for marketing unless users opt in.
- **Example:** Users receive emails about account activity, such as login alerts or subscription renewals, tied to their Apple ID email.

3. Phone Number

- **Description:** Apple collects a phone number, often required for account security and verification processes.
- **Purpose:** Enables two-factor authentication, account recovery, and contact for support or billing issues. It may also be used for iMessage or FaceTime activation.
- **Context:** As part of Apple's privacy-focused data collection, the phone number is used solely for account and device functionality, not for third-party sharing or ads, aligning with the StockApps study's findings.
- **Example:** A phone number is requested during Apple ID setup or when enabling two-factor authentication to receive verification codes.

4. Device Identifiers

- **Description:** Unique identifiers such as device serial numbers, UDID (Unique Device Identifier), or IMEI numbers are collected for each Apple device.
- **Purpose:** Used to track device activity, manage warranties, provide support, and ensure services like Find My iPhone work correctly.
- **Context:** The provided text mentions Apple's collection of "device activity" data, making device identifiers a key component for maintaining functionality across hardware and software ecosystems.
- **Example:** When registering a new iPhone with iCloud, Apple links the device's serial number to the user's account for features like device tracking or repair services.

5. IP Address

- **Description:** The IP address of the user's device is collected when connecting to Apple's servers or services.
- **Purpose:** Facilitates network connectivity, security monitoring, and region-based service customization (e.g., App Store content availability).
- **Context:** As part of device activity, IP addresses are necessary for operational purposes but are anonymized or minimally processed to align with Apple's privacy stance, per the provided information.
- **Example:** When downloading an app, Apple's servers log the IP address to deliver content and detect potential security threats.

6. Search Queries

- **Description:** Search terms entered in Apple services like Siri, Spotlight Search, or the App Store are collected.
- **Purpose:** Improves search functionality, personalizes results, and enhances user experience across Apple's ecosystem.
- **Context:** The provided text explicitly mentions Apple collecting "search terms," indicating this as one of the 12 data points. Apple processes these queries on-device or anonymizes them to protect privacy, avoiding marketing use.
- **Example:** Typing "weather" in Spotlight Search may be logged to refine future suggestions, but Apple strips personal identifiers from such data.

7. Location Data

- **Description:** GPS or approximate location data is collected when location services are enabled on Apple devices.
- **Purpose:** Powers features like Find My iPhone, Maps navigation, location-based app recommendations, or weather updates.
- **Context:** The text notes Apple collects "GPS" data, which is part of the 12 data points. Apple emphasizes user control, allowing users to toggle location

services and limiting data sharing, consistent with its privacy-conscious approach.

- **Example:** Enabling location for Maps records your position to provide directions, but Apple obfuscates precise data when sharing with apps.

8. App Usage Data

- **Description:** Data on how users interact with apps on iOS, iPadOS, or macOS, such as app launches or feature usage, is collected.
- **Purpose:** Optimizes system performance, informs app recommendations, and supports developers with anonymized analytics.
- **Context:** As part of “device activity” in the provided text, app usage data helps Apple maintain and improve its ecosystem while keeping data on-device or anonymized.
- **Example:** Apple may track how often you open the Notes app to prioritize it in Spotlight suggestions, but this data isn’t tied to your identity for ads.

9. Purchase History

- **Description:** Records of purchases made through the App Store, iTunes, or Apple services (e.g., subscriptions, in-app purchases) are collected.
- **Purpose:** Manages billing, provides receipts, and enables features like Family Sharing or purchase restoration.
- **Context:** Purchase history is a necessary part of account maintenance, as implied by the StockApps study’s focus on Apple’s minimal data needs for account functionality.
- **Example:** Buying a subscription to Apple Music generates a record in your Apple ID account, accessible in your purchase history.

10. Device Settings

- **Description:** User-configured settings on Apple devices, such as language, time zone, or notification preferences, are collected.
- **Purpose:** Ensures consistent user experience across devices via iCloud syncing and tailors services to user preferences.

- **Context:** Device activity, as mentioned in the text, includes settings data to support seamless operation of Apple's ecosystem, aligning with Apple's privacy focus.
- **Example:** Setting your iPhone to "Dark Mode" is synced to your iPad via iCloud, requiring Apple to store this preference.

11. Health Data (Optional)

- **Description:** Health and fitness data, such as step counts, heart rate, or workout details, collected via Apple Watch or HealthKit-enabled apps, if users opt in.
- **Purpose:** Powers the Health app, provides personalized fitness insights, and supports medical research (if users consent).
- **Context:** While not explicitly mentioned in the provided text, health data is a known Apple data type for users engaging with HealthKit. It's included as a likely data point since Apple collects it with strict user consent, fitting the 12-point framework.
- **Example:** An Apple Watch user's daily step count is stored in the Health app, but Apple encrypts this data and restricts access unless explicitly shared.

12. Browsing Activity (Limited)

- **Description:** Limited browsing data from Safari, such as URLs visited or iCloud tabs, if iCloud syncing is enabled.
- **Purpose:** Enables cross-device browsing continuity and improves Safari features like Intelligent Tracking Prevention.
- **Context:** The text notes Apple's focus on device activity, and browsing data is a minimal component when users opt into iCloud features. Apple anonymizes or encrypts this data to avoid marketing use, per the StockApps study.
- **Example:** Opening a webpage on Safari with iCloud enabled syncs the tab to your Mac, requiring Apple to store the URL temporarily.

Notes and Context

- **Privacy Focus:** The provided information emphasizes Apple's privacy-conscious approach, collecting only the **12 types of data** necessary for account maintenance and device activity, far fewer than Google (39), Meta (14), Amazon (23), or Twitter (24). Apple avoids pulling data from public sources and doesn't share it for marketing, unlike competitors.
- **Inference Basis:** Since the exact 12 data points aren't listed in the text, the above list is derived from the description of Apple's data practices (e.g., "search terms," "GPS," "device activity") and standard Apple privacy disclosures, ensuring alignment with the StockApps study's findings.
- **Limitations:** Without the original StockApps study, minor variations in the exact data points are possible. However, the above list is consistent with Apple's documented practices as of June 2025, focusing on minimal, functional data collection.
- **Verification:** For precise details, users can refer to Apple's privacy policy (available at apple.com/privacy) or the StockApps study cited in the Moneycontrol report.

If you need further clarification on any specific data point, want me to check Apple's current privacy policy for updates, or need a comparison with another company's data practices, let me know!