AllTrails as an OSINT Target: Methodology, Attack Surface, and Investigative Workflow

Maria Cattini | 16/04/2026 | OSINT

AllTrails is not primarily an outdoor app. From an OSINT perspective, it is a geospatial data platform with 65+ million registered users, default-public activity profiles, and GPS track records indexed by major search engines. The investigative value does not come from the app itself — it comes from what the platform exposes, how that data connects to external sources, and what a structured collection workflow can extract without any privileged access.

The Motherboard/Vice investigation published in July 2024 demonstrated this precisely: a security researcher reconstructed the physical movement patterns of a former senior Biden administration official using only public AllTrails data — probable home address included.

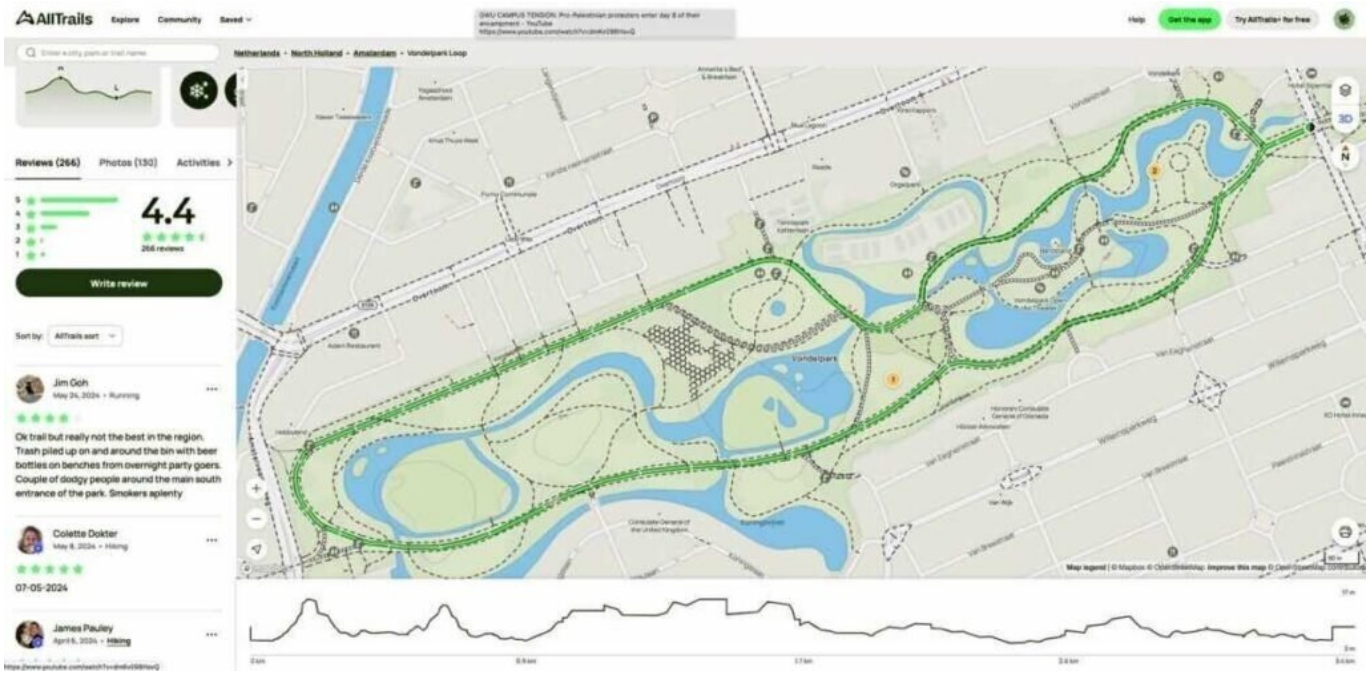
Context Framing

Three structural conditions make AllTrails a high-value OSINT target.

Default visibility. Every new account is set to public. Activity logs, completed trails, GPS tracks, and profile photos are visible to any authenticated user. The platform's own documentation confirms that adjusting privacy settings applies only to future content — past activities must be modified individually.

Search engine indexing. AllTrails profiles were, by default, indexed by Google. The query site:alltrails.com/members/ returns public account listings without requiring API access or scraping tools. This is passive reconnaissance with zero technical barrier.

Third-party sync exposure. Users importing activities from Garmin Connect, Apple Health, or similar platforms report that private activities on the originating platform become public on AllTrails unless manually reconfigured. This creates an exposure vector that bypasses the user's privacy intent entirely.



System Breakdown

Layer 1 — User-generated data (public surface)

• Profile: name, avatar, declared location
• Activity log: trails completed, timestamps, GPS coordinates
• Photos: geotagged images attached to trail reviews
• Reviews: text content linking activity to specific locations and dates

Layer 2 — Platform infrastructure

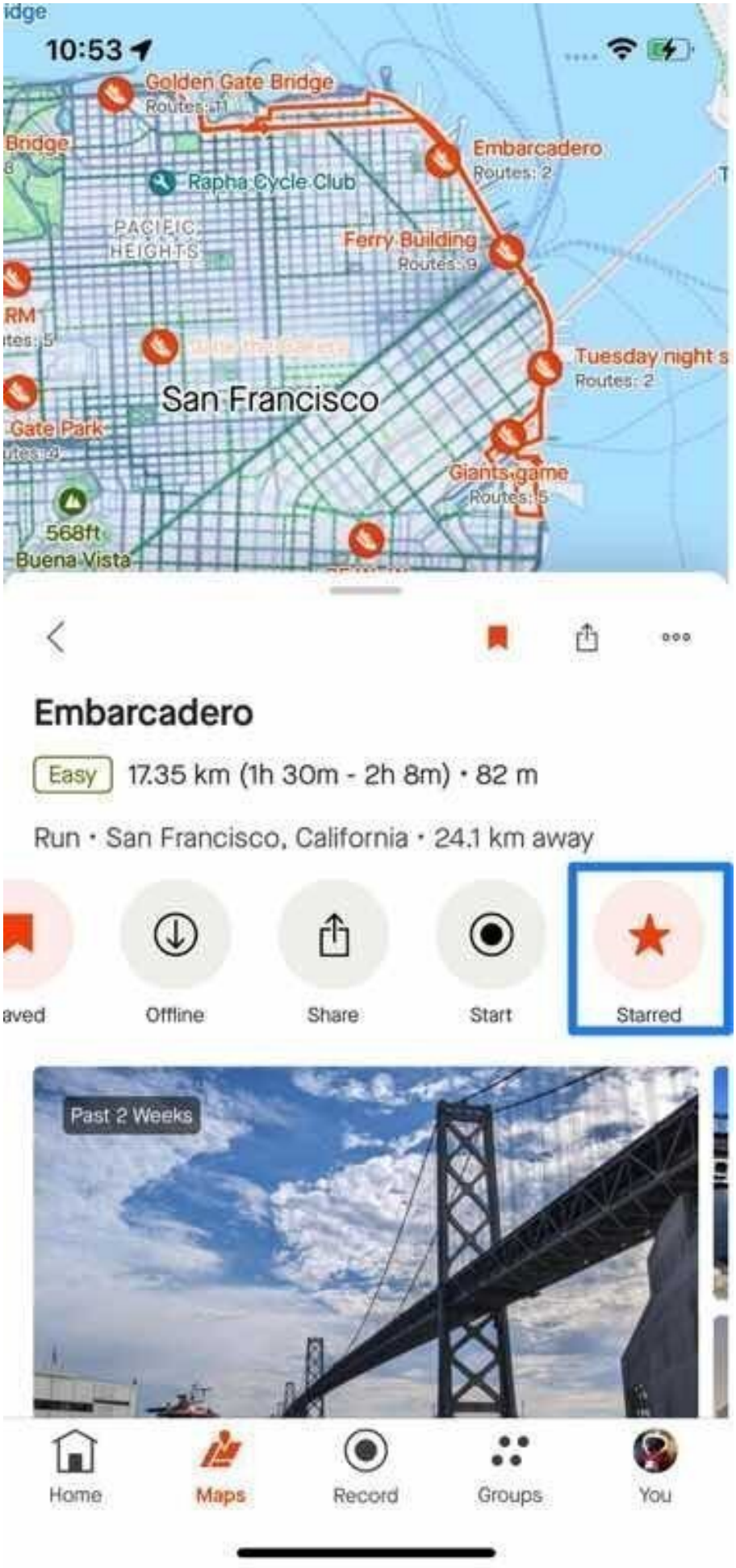
• Core domain: alltrails.com
• Observable subdomains: api.alltrails.com, support.alltrails.com, blog.alltrails.com
• Anti-bot protection: DataDome (deployed on app, web, and API)
• Technology stack (fingerprinting-derived): CDN via Cloudflare/Fastly, frontend React/Next.js, mobile API REST/GraphQL

Layer 3 — Corporate footprint

• Employee data: LinkedIn profiles under "AllTrails engineer" or similar queries reveal team structure, stack usage, and infrastructure decisions
• Job postings: historically disclosed AWS and Kubernetes usage
• GitHub: potential public repositories or accidental leaks
• Financial layer: Permira (lead investor, $150M round, 2021), Spectrum Equity (majority shareholder since 2018), total funding ~$151M across 6 rounds

Layer 4 — Third-party SDK exposure

AllTrails integrates 17 third-party SDKs including Facebook SDK, Google AdMob, and Firebase Analytics. The app requests 11 iOS permissions: camera, contacts, photo library, location (in-use and always-on), HealthKit read/write, Bluetooth. These integration points are not investigative targets in themselves, but they define the data collection surface when assessing platform risk.



Operational Methodology

Step 1 — Passive enumeration

Begin without authentication. Run Google dorking:

```
site:alltrails.com/members/
site:alltrails.com/members/ "[target name or username]"
```

Cross-reference usernames with Sherlock or Maigret for cross-platform identity correlation. A username active on AllTrails appearing on Instagram, Reddit, or Strava constitutes a confirmed identity pivot.

Step 2 — Account-level reconnaissance

Create an authenticated account. AllTrails requires login to view full profile content. Once authenticated, navigate to the target profile directly via URL pattern alltrails.com/members/[username]. Extract: completed trail list, activity timestamps, photo uploads, and geographic clustering.

Step 3 — GPS track analysis

Public GPS tracks on AllTrails display start/end coordinates. Repeated tracks starting from the same geographic cluster indicate home base or regular departure point. Cross-reference with Google Earth or OpenStreetMap to verify location type (residential, workplace, recurring venue).

Validation step: correlate start-point coordinates across multiple activities. If 3+ separate activities originate within a 200-meter radius, that point warrants geolocation verification.

Step 4 — Photo metadata extraction

Photos uploaded to trail galleries may retain EXIF data. Download using standard EXIF tools. Check for GPS coordinates embedded in image metadata. Even stripped images can be geolocated via background landmark analysis using Google Earth or Yandex reverse image search.

Step 5 — Cross-platform triangulation

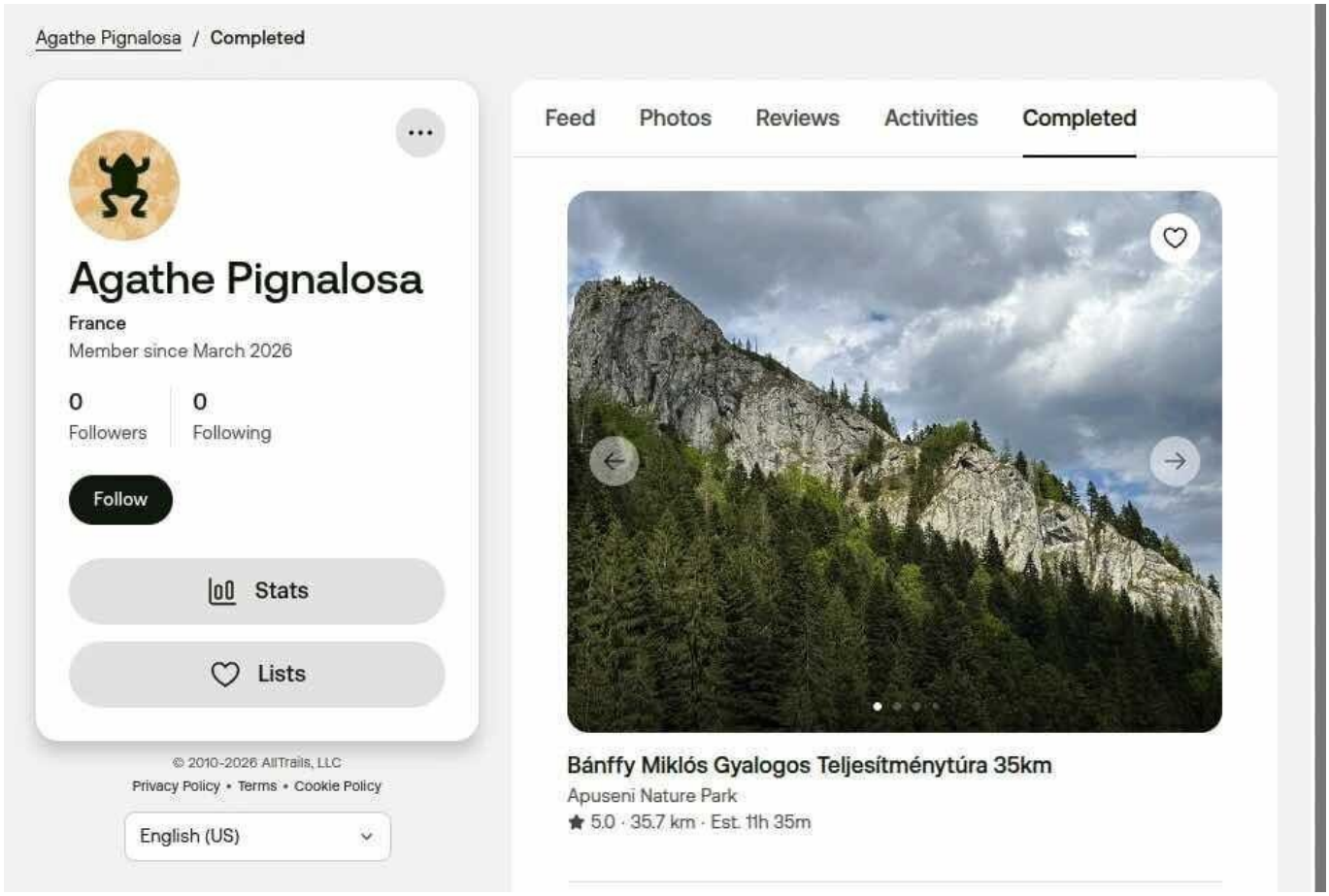
Username → Instagram/Reddit/Strava search confirms identity. Profile photo → reverse image search (Google Images, Yandex) identifies cross-platform accounts. Trail activity dates → cross-reference with public records, social posts, or news mentions for timeline correlation.

Step 6 — Infrastructure reconnaissance (corporate targets)

For corporate OSINT:

```
amass enum -d alltrails.com
subfinder -d alltrails.com
```

Supplement with SecurityTrails or RiskIQ for passive DNS and historical records. Use Shodan/Censys for exposed services. Job posting archives on LinkedIn and Wayback Machine reveal technology stack decisions and hiring patterns over time.



Risks and Limitations

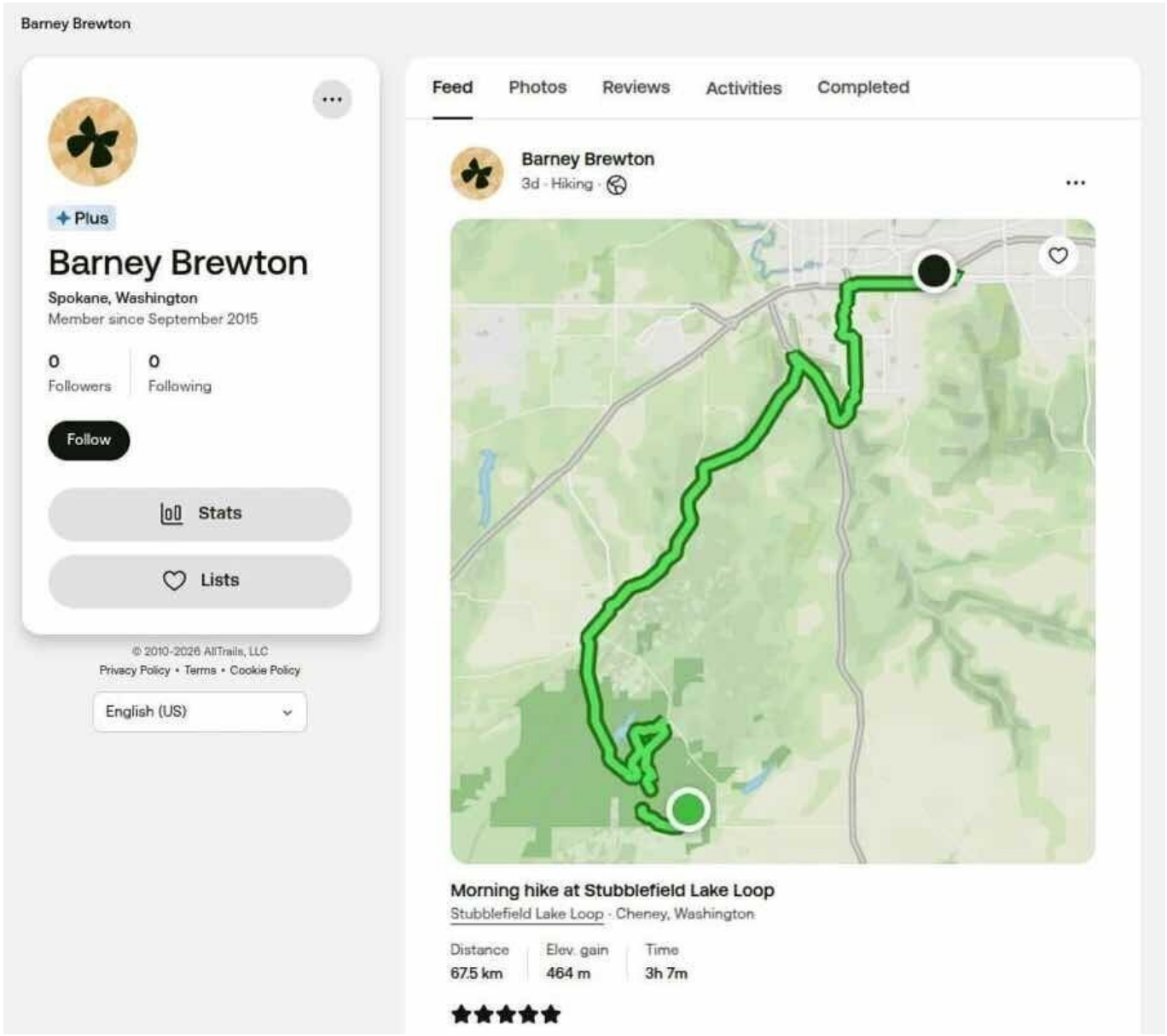
Data gaps. AllTrails records only explicitly tracked activities. A target using paper maps, a separate GPS device, or no tracking at all produces an empty or near-empty profile. Absence of data is not evidence of absence of movement.

Anti-scraping controls. DataDome deployment on AllTrails' API, web, and mobile app blocks automated collection at scale. Manual collection is still feasible but time-constrained.

Privacy setting changes. A privacy-aware target can retroactively restrict all activities. The change applies forward; existing public activities must be individually locked. However, if data was indexed before restriction, cached versions may persist in search engine archives or third-party databases.

Third-party sync inconsistencies. User reports on Reddit describe Garmin activities set as private becoming public on AllTrails after sync. This is a documented but unconfirmed platform behavior — treat synced-activity visibility as unreliable until tested directly.

Geolocation precision. GPS tracks in the platform are accurate to consumer device standards (~3–5 meters in open terrain). Urban canyons and forest cover degrade this. Verify coordinates independently before treating them as confirmed locations.



Analytical Layer

The structural pattern across AllTrails, Strava, and similar platforms is consistent: fitness apps are designed for sharing, not privacy. Default-public settings serve retention and network effect logic — more visible data drives more engagement, more engagement drives more users. Privacy controls exist but are buried, retroactively limited, and non-obvious for non-technical users.

The Biden official case is not an anomaly. It is a demonstration of the baseline risk present in any platform where movement data is user-generated, publicly accessible, and search-indexed. The same methodology applies to any target — corporate executive, government employee, activist, journalist — who uses a fitness tracking platform with default settings.

The cross-border implication is distinct: AllTrails operates in 191 countries. GDPR creates theoretical data subject rights in the EU, but the investigative surface is still exposed before any right-of-erasure request is processed. Data once indexed or archived is not recoverable through privacy requests alone.

The DataDome deployment signals that AllTrails treats its trail database as a strategic proprietary asset worth protecting at infrastructure level — not just user data. This distinction matters: bulk scraping is defended against; manual, authenticated, record-by-record access is not.

Closing Insight

The investigative value of AllTrails is not in any single data point. It lies in the correlation layer: GPS start points identify locations, timestamps establish patterns, cross-platform username pivots confirm identity, photo metadata provides independent verification. No individual element is conclusive. Combined across sources and validated against independent geographic data, the picture becomes operationally precise.

The platform's own architecture makes this possible — not through a vulnerability, but through design.

Join the community:

• Newsletter → https://projectosint.substack.com/
• Telegram → https://t.me/osintprojectgroup
AllTrails is not primarily an outdoor app. From an OSINT perspective, it is a geospatial data platform with 65+ million registered users, default-public activity profiles, and GPS track records indexed by major search engines. The investigative value does not come from the app itself — it comes from what the platform exposes, how that data connects to external sources, and what a structured collection workflow can extract without any privileged access.

The Motherboard/Vice investigation published in July 2024 demonstrated this precisely: a security researcher reconstructed the physical movement patterns of a former senior Biden administration official using only public AllTrails data — probable home address included.

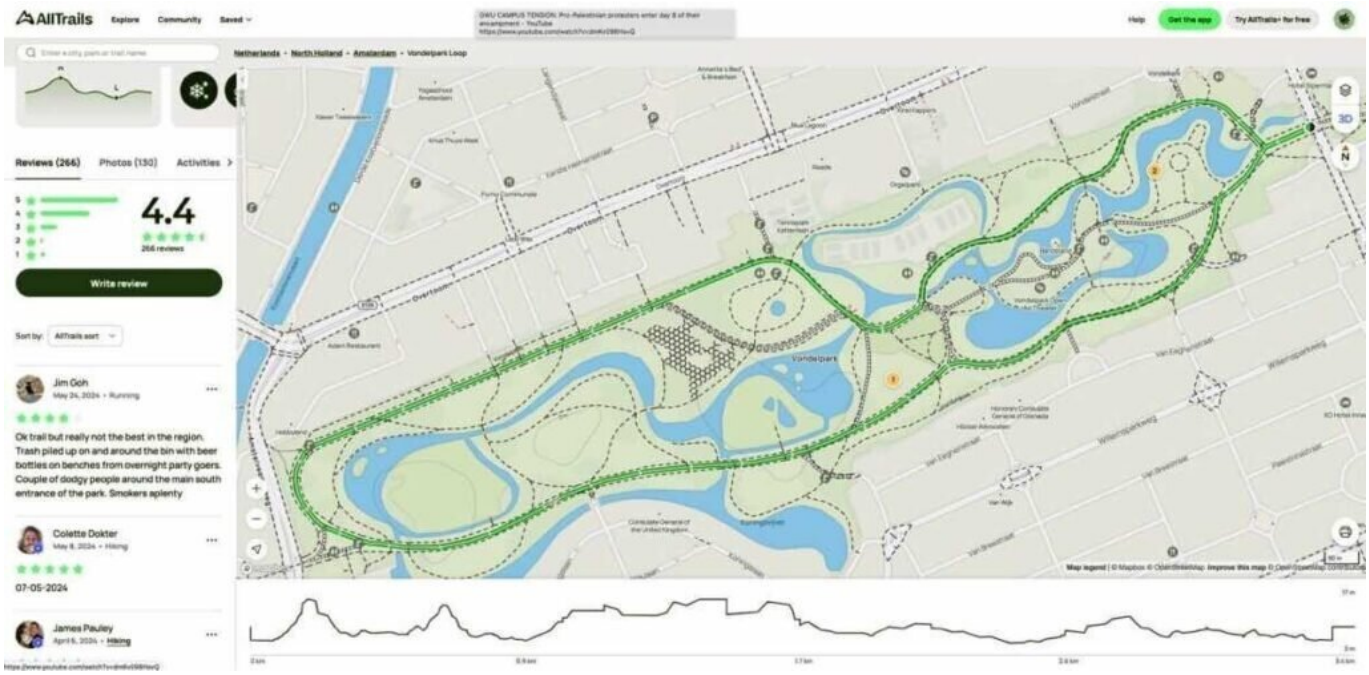
Context Framing

Three structural conditions make AllTrails a high-value OSINT target.

Default visibility. Every new account is set to public. Activity logs, completed trails, GPS tracks, and profile photos are visible to any authenticated user. The platform's own documentation confirms that adjusting privacy settings applies only to future content — past activities must be modified individually.

Search engine indexing. AllTrails profiles were, by default, indexed by Google. The query site:alltrails.com/members/ returns public account listings without requiring API access or scraping tools. This is passive reconnaissance with zero technical barrier.

Third-party sync exposure. Users importing activities from Garmin Connect, Apple Health, or similar platforms report that private activities on the originating platform become public on AllTrails unless manually reconfigured. This creates an exposure vector that bypasses the user's privacy intent entirely.



System Breakdown

Layer 1 — User-generated data (public surface)

• Profile: name, avatar, declared location
• Activity log: trails completed, timestamps, GPS coordinates
• Photos: geotagged images attached to trail reviews
• Reviews: text content linking activity to specific locations and dates

Layer 2 — Platform infrastructure

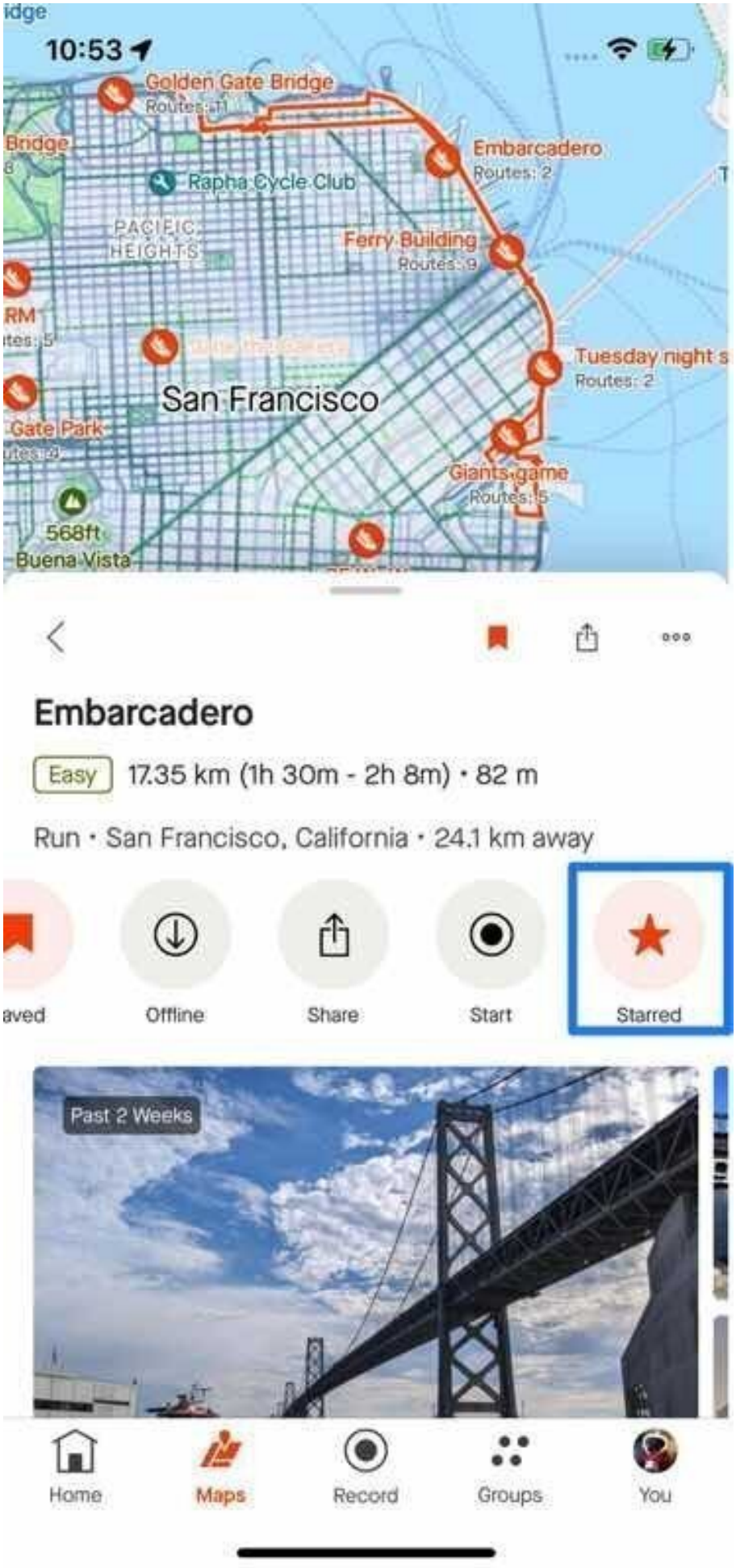
• Core domain: alltrails.com
• Observable subdomains: api.alltrails.com, support.alltrails.com, blog.alltrails.com
• Anti-bot protection: DataDome (deployed on app, web, and API)
• Technology stack (fingerprinting-derived): CDN via Cloudflare/Fastly, frontend React/Next.js, mobile API REST/GraphQL

Layer 3 — Corporate footprint

• Employee data: LinkedIn profiles under "AllTrails engineer" or similar queries reveal team structure, stack usage, and infrastructure decisions
• Job postings: historically disclosed AWS and Kubernetes usage
• GitHub: potential public repositories or accidental leaks
• Financial layer: Permira (lead investor, $150M round, 2021), Spectrum Equity (majority shareholder since 2018), total funding ~$151M across 6 rounds

Layer 4 — Third-party SDK exposure

AllTrails integrates 17 third-party SDKs including Facebook SDK, Google AdMob, and Firebase Analytics. The app requests 11 iOS permissions: camera, contacts, photo library, location (in-use and always-on), HealthKit read/write, Bluetooth. These integration points are not investigative targets in themselves, but they define the data collection surface when assessing platform risk.



Operational Methodology

Step 1 — Passive enumeration

Begin without authentication. Run Google dorking:

```
site:alltrails.com/members/
site:alltrails.com/members/ "[target name or username]"
```

Cross-reference usernames with Sherlock or Maigret for cross-platform identity correlation. A username active on AllTrails appearing on Instagram, Reddit, or Strava constitutes a confirmed identity pivot.

Step 2 — Account-level reconnaissance

Create an authenticated account. AllTrails requires login to view full profile content. Once authenticated, navigate to the target profile directly via URL pattern alltrails.com/members/[username]. Extract: completed trail list, activity timestamps, photo uploads, and geographic clustering.

Step 3 — GPS track analysis

Public GPS tracks on AllTrails display start/end coordinates. Repeated tracks starting from the same geographic cluster indicate home base or regular departure point. Cross-reference with Google Earth or OpenStreetMap to verify location type (residential, workplace, recurring venue).

Validation step: correlate start-point coordinates across multiple activities. If 3+ separate activities originate within a 200-meter radius, that point warrants geolocation verification.

Step 4 — Photo metadata extraction

Photos uploaded to trail galleries may retain EXIF data. Download using standard EXIF tools. Check for GPS coordinates embedded in image metadata. Even stripped images can be geolocated via background landmark analysis using Google Earth or Yandex reverse image search.

Step 5 — Cross-platform triangulation

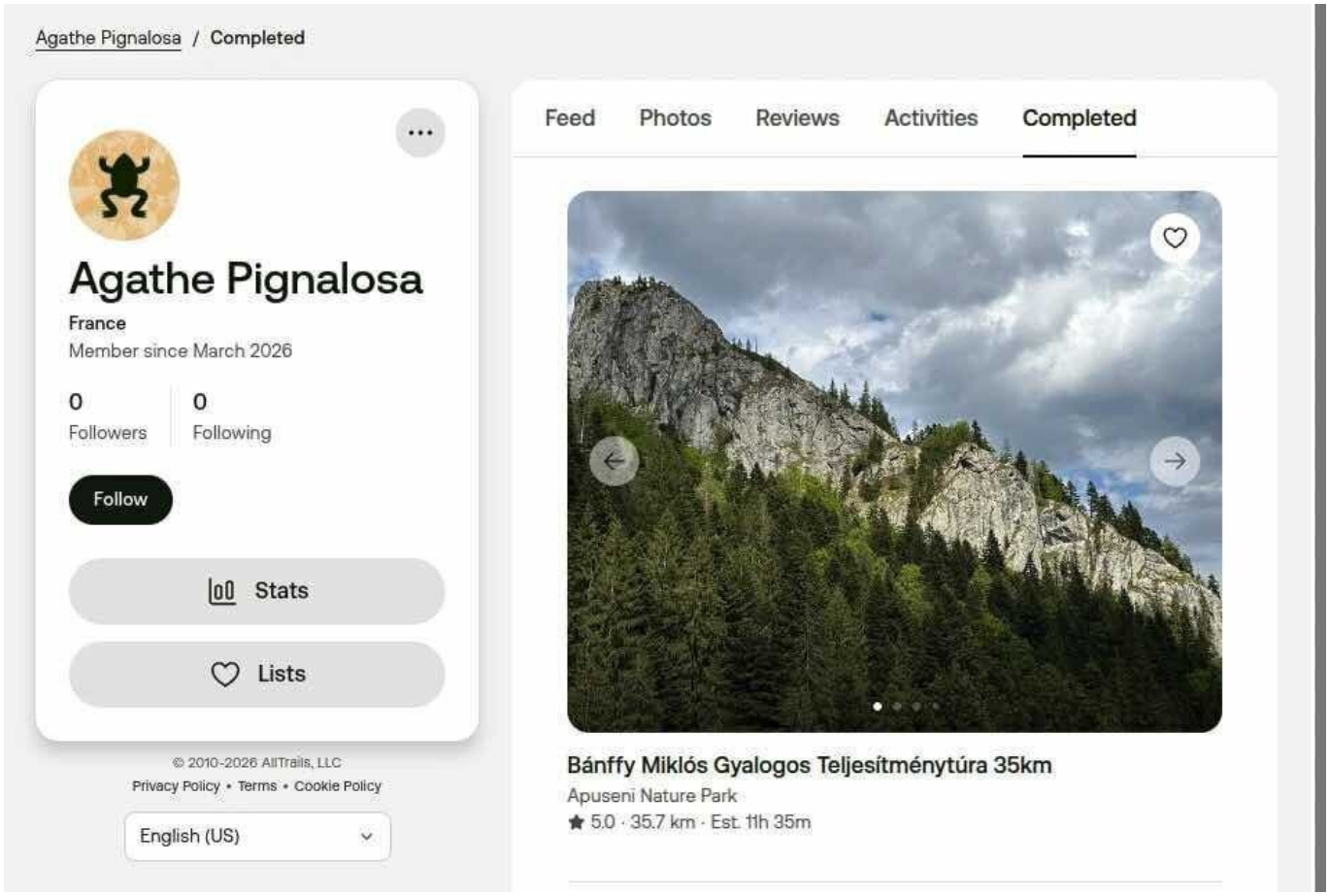
Username → Instagram/Reddit/Strava search confirms identity. Profile photo → reverse image search (Google Images, Yandex) identifies cross-platform accounts. Trail activity dates → cross-reference with public records, social posts, or news mentions for timeline correlation.

Step 6 — Infrastructure reconnaissance (corporate targets)

For corporate OSINT:

```
amass enum -d alltrails.com
subfinder -d alltrails.com
```

Supplement with SecurityTrails or RiskIQ for passive DNS and historical records. Use Shodan/Censys for exposed services. Job posting archives on LinkedIn and Wayback Machine reveal technology stack decisions and hiring patterns over time.



Risks and Limitations

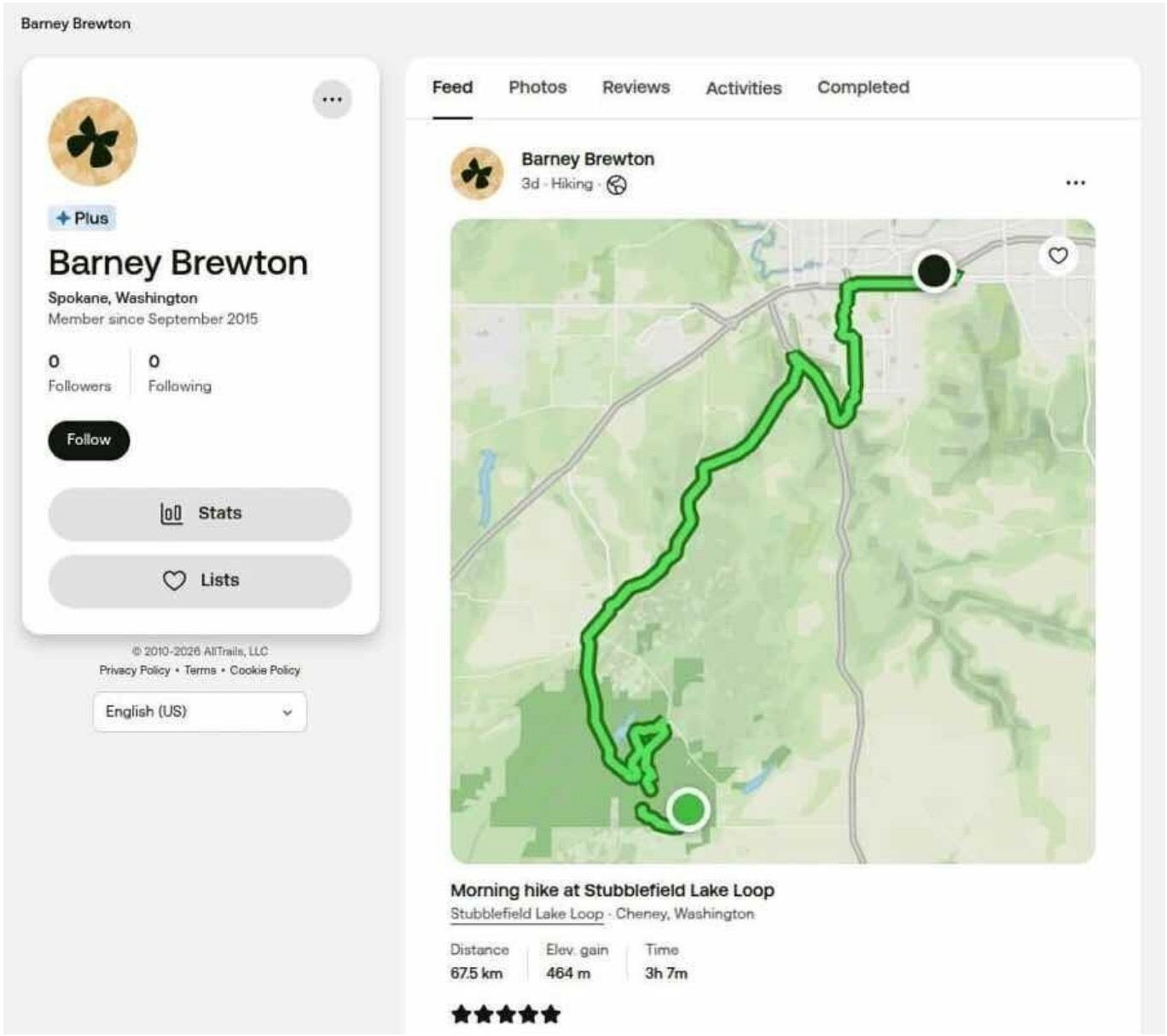
Data gaps. AllTrails records only explicitly tracked activities. A target using paper maps, a separate GPS device, or no tracking at all produces an empty or near-empty profile. Absence of data is not evidence of absence of movement.

Anti-scraping controls. DataDome deployment on AllTrails' API, web, and mobile app blocks automated collection at scale. Manual collection is still feasible but time-constrained.

Privacy setting changes. A privacy-aware target can retroactively restrict all activities. The change applies forward; existing public activities must be individually locked. However, if data was indexed before restriction, cached versions may persist in search engine archives or third-party databases.

Third-party sync inconsistencies. User reports on Reddit describe Garmin activities set as private becoming public on AllTrails after sync. This is a documented but unconfirmed platform behavior — treat synced-activity visibility as unreliable until tested directly.

Geolocation precision. GPS tracks in the platform are accurate to consumer device standards (~3–5 meters in open terrain). Urban canyons and forest cover degrade this. Verify coordinates independently before treating them as confirmed locations.



Analytical Layer

The structural pattern across AllTrails, Strava, and similar platforms is consistent: fitness apps are designed for sharing, not privacy. Default-public settings serve retention and network effect logic — more visible data drives more engagement, more engagement drives more users. Privacy controls exist but are buried, retroactively limited, and non-obvious for non-technical users.

The Biden official case is not an anomaly. It is a demonstration of the baseline risk present in any platform where movement data is user-generated, publicly accessible, and search-indexed. The same methodology applies to any target — corporate executive, government employee, activist, journalist — who uses a fitness tracking platform with default settings.

The cross-border implication is distinct: AllTrails operates in 191 countries. GDPR creates theoretical data subject rights in the EU, but the investigative surface is still exposed before any right-of-erasure request is processed. Data once indexed or archived is not recoverable through privacy requests alone.

The DataDome deployment signals that AllTrails treats its trail database as a strategic proprietary asset worth protecting at infrastructure level — not just user data. This distinction matters: bulk scraping is defended against; manual, authenticated, record-by-record access is not.

Closing Insight

The investigative value of AllTrails is not in any single data point. It lies in the correlation layer: GPS start points identify locations, timestamps establish patterns, cross-platform username pivots confirm identity, photo metadata provides independent verification. No individual element is conclusive. Combined across sources and validated against independent geographic data, the picture becomes operationally precise.

The platform's own architecture makes this possible — not through a vulnerability, but through design.

Join the community:

- Newsletter → https://projectosint.substack.com/
- Telegram → https://t.me/osintprojectgroup