SECURITY BRIEF

Commercial Data Has Become an Intelligence Threat

What Defense and Intelligence Organizations Must Know About Mobile Data Exposure

~10 Years	No Hacking Needed	Personnel Tracking
Exposure Known to Intelligence Community	Commercial Data Purchased by Adversaries	Movements of American Military and IC personnel in theater & home

The Battlefield Has Moved

For years, the national security community treated commercially available mobile data as a privacy issue. Today, it has become something far more dangerous: a battlefield intelligence source capable of exposing the movements, behaviors, and locations of American military personnel to foreign adversaries in near real time.

Recent reporting detailing how adversaries are exploiting commercially available location data to surveil and potentially target US forces in the Middle East should serve as a wake-up call for every defense and intelligence organization relying on conventional consumer mobility platforms. The issue is no longer hypothetical. It is operational.

> *The exposure has been known for nearly a decade, yet the risk remains active, growing, and exploitable without a single act of hacking.*

The most alarming part of the story is not simply that commercial location data exists, but that the exposure has been known for nearly a decade. From covert forward operating bases in Syria to sensitive nuclear storage facilities in Europe, commercially harvested mobile telemetry has repeatedly demonstrated the ability to reveal the patterns of life of military personnel, contractors, and even family members.

And unlike traditional espionage, this intelligence does not require hacking, insider recruitment, or sophisticated cyber intrusion. It can simply be purchased.

The Consumer Ecosystem Was Never Built for Mission Ops

The modern consumer mobile ecosystem was never designed for high-threat government environments. Nearly every commercial smartphone continuously emits sensitive data and/or metadata through advertising IDs, location services, third-party applications, browser trackers, wireless radios, cloud synchronization services, and data brokerage ecosystems that monetize user behavior at massive scale. Even when users believe location sharing is disabled, countless applications and embedded SDKs continue harvesting behavioral and geospatial data behind the scenes.

Commercial Mobile Data Exposure Vectors

DATA SOURCE	EXPLOITATION METHOD	RISK LEVEL
Advertising IDs	Cross-app behavioral correlation	CRITICAL
Third-Party SDKs	Silent background telemetry	CRITICAL
Location Services	Geospatial pattern-of-life analysis	CRITICAL
Browser Trackers	Third-party cookie / fingerprinting	HIGH
Cloud Sync	Metadata harvested from sync traffic	HIGH
Wireless Radios	Passive triangulation & MAC logging	MEDIUM

Sources of commercially harvestable intelligence from standard consumer mobile devices.

This creates a profound operational security problem for military organizations operating in contested environments. A service member carrying a standard consumer smartphone may unknowingly contribute to a digital signature that reveals troop concentrations, deployment patterns, operational tempo, supply routes, training activities, or the locations of sensitive facilities. When aggregated at scale, these signals become actionable intelligence for adversaries.

In addition to the consumer smartphone, other devices within the eco-system also provide similar location data, such as vehicle infotainment systems, heads-up displays, wrist controllers, bar code scanners, drone controllers and any embedded computer with the capability to communicate with the outside world.

CRITICAL FINDING

Telling troops to 'practice better OPSEC' is insufficient when the underlying operating system and application ecosystem are fundamentally engineered around data collection and monetization. The burden cannot realistically be placed on the individual user.

Privacy Is Now Operational Protection

Foreign adversaries do not distinguish between 'consumer data' and 'military data.' They exploit whatever information is available, accessible, and scalable. The same advertising ecosystem designed to deliver personalized marketing can just as easily reveal force posture, deployment timelines, command relationships, and operational movements.

As warfare becomes increasingly data-driven, mobile privacy is no longer optional. It is operational protection.

The recent disclosures surrounding the exploitation of commercial location data against US forces should force a broader reassessment of mobility security across the Department of War and Intelligence Community. The challenge is no longer simply securing classified communications channels. It is now about controlling the digital emissions created by the device's personnel carry and use every day.

STRATEGIC IMPERATIVE

Organizations that continue relying solely on conventional consumer mobility platforms must recognize the strategic risk posed by commercially available data ecosystems. Purpose-built secure mobility platforms that minimize data exposure, restrict telemetry, and reduce digital traceability will become essential components of future operational security architectures.

The battlefield has expanded beyond physical terrain. Today, it includes the invisible commercial data economy that surrounds every connected device.

Certifications and Features – Helpful but Still Risky

Many of the security frameworks and certification programs traditionally relied upon for government mobility assurance were not originally designed to address the modern commercial surveillance ecosystem. Certifications such as National Information Assurance Partnership (NIAP) and Commercial Solutions for Classified Program (CSfC) remain valuable components of a broader security strategy, but they do not natively prevent the collection, aggregation, and monetization of behavioral and location data generated through commercial applications, advertising frameworks, embedded analytics, or user-enabled convenience features. A certified device can satisfy traditional security certification requirements while still emitting large volumes of commercially exploitable telemetry that can be harvested by data brokers or foreign intelligence services.

Convenience features designed for ordinary commercial users may improve usability in consumer environments but can create significant exposure risks for defense and intelligence personnel. In high-threat operational settings, these same features can unintentionally contribute to pattern-of-life development, location correlation, device fingerprinting, and operational surveillance activities conducted by sophisticated adversaries. The broader mobility ecosystem has also suffered from a longstanding lack of purpose-built alternatives designed specifically for national security missions. As a result, many organizations have continued deploying commercial consumer solutions despite years of documented concerns. In some cases, organizations have defaulted to widely available commercial platforms simply because few viable government-focused alternatives exist at scale. This has contributed to operational decisions that have accepted significant surveillance and tracking risk as an unavoidable byproduct of modern mobility rather than addressing the root architectural problem itself.

Scrambling to Adapt

Mobile devices in general present a significant challenge to government users and Agencies are looking to change with the evolving environment. The Army's transition from dedicated government-furnished mobile devices to a bring-your-own-device (BYOD) mobility model reflects an understandable desire to improve user convenience, reduce costs, and simplify access to enterprise services. Under the new approach, government applications and data are isolated within a secure workspace while the users' personal apps, messages, photos, and browsing activity remain outside of Army visibility and control. While this architecture can provide strong protection for government information and enterprise access, it does not fully address a separate and increasingly important operational security challenge: the collection and exploitation of commercially available data generated by the underlying device itself.

The distinction is critical. Secure containerization protects government data from being exposed to personal applications and protects personal data from government oversight. As a result, the device may still generate substantial amounts of metadata and behavioral information that can be collected. This "data exhaust" can include location history, movement patterns, device identifiers, application usage patterns, network telemetry, and other behavioral signals that are unrelated to the government workspace but highly valuable to adversaries. The resulting threat is that a foreign intelligence service can purchase or otherwise obtain commercially available data that allows them to identify military installations, track personnel movements, establish patterns of life, and potentially support surveillance or targeting activities. Adversaries do not necessarily need access to classified information if they can instead reconstruct operational activities through aggregated commercial datasets.

A Purpose-Built Secure Mobility Platform

The altOS platform consists of a mobile operating system and a management server designed around a fundamentally different philosophy than commercial consumer platforms. Maintaining strong security without degrading operational effectiveness is a fundamental requirement for government mobility platforms. The altOS platform is designed to deliver mobile security against advanced threats while preserving a familiar and intuitive user experience built around the Android ecosystem. By minimizing disruption to established workflows, the platform reduces user retraining requirements and accelerates operational adoption across diverse mission environments.

At the same time, altOS incorporates granular administrative controls and isolated user environments that enable organizations to customize device functionality, application access, and security policies according to mission-specific requirements. The altOS platform was designed specifically to address a broader operational security challenge. Rather than focusing exclusively on protecting government applications, altOS takes a multi-pronged approach to security:

altOS's Approach to Mobile Security

01 Advertising ID Elimination

Remove or randomize advertising identifiers to prevent cross-app behavioral profiling and long-term tracking by commercial data brokers by reducing the overall digital signature emitted by the device itself. This includes limiting unnecessary telemetry, controlling application behavior, reducing exposure to advertising identifiers, restricting data sharing with third-party services, and providing administrators with greater control over the mobile ecosystem.

02 Full Device Governance

Provide policy driven control of device resources including all radios (Wi-Fi, Bluetooth, NFC, etc.), peripherals (cameras, microphones, speakers), applications and network access in addition to the ability to granularly control capabilities. The management environment delivers controls designed to limit exposure through inadvertent user activity and provide the audit capabilities for device assurance.

03 Data Security and Containerization

Secure data via altOS containerization by isolating data from public, work and mission personas through encrypted, sandboxed workspaces separate from each other. The objective of the multi-persona environment is not merely to secure government data at rest or in transit, but to reduce the volume of commercially available information that can be harvested, aggregated, and exploited.

04 Controlled Device Communications

Limit uncontrolled synchronization of sensitive metadata to third-party commercial infrastructure that adversaries can correlate. Strictly control background telemetry, geolocation

access, and third-party SDK communications to eliminate silent data harvesting. Enforce hardened browsing policies by default by blocking third-party cookies, fingerprinting scripts, and persistent web trackers.

05 Identity Management

Control the digital footprint left by the device and by the user though obfuscation techniques designed to mitigate operational vulnerabilities. Limit the ability of adversaries to track, target and exploit users, their devices and their behaviors. Apply these capabilities based on the mission both in and out of theater.

As military and intelligence organizations increasingly recognize commercially available data as a legitimate intelligence source, mobility security must evolve beyond traditional concepts of application security and device management. The question is no longer simply whether government data is protected inside a secure container. The more important question is whether the device itself is generating a digital footprint that can be leveraged to identify, monitor, or target personnel. Addressing that challenge requires a fundamentally different approach to mobility. CIS Secure and altOS treat privacy, operational security, and mission assurance as inseparable elements of the same problem.

The platform's deployment flexibility further supports the unique demands of defense, intelligence, and federal civilian agencies. Whether deployed in cloud-based, hybrid, or fully government-owned on-premises infrastructures, altOS enables organizations to align mobility operations with classification requirements, data sovereignty mandates, and organizational risk models. This flexibility allows agencies to maintain strict control over sensitive data and infrastructure while adapting deployments to highly compartmented or geographically distributed operational environments.

The result is a sovereign mobility capability designed to support modern operational requirements while addressing the growing sophistication of adversary threats on both the battlefield and the home front.