Information Technology Innovations and Applied Communication
Vol. 4, No. 2, Summer, 2026, Serial No. 10,pp.51-60

Simple Cell Phone Tracking Through Smartphone Contact List

Reza Kayvan shokooh[1*]

* Assistant Professor, Imam Hossein University, Tehran, Iran

(**Received:** 17 April 2026 , **Revised:** 27 May 2026, **Accepted:** 09 June 2026, **Published:** 27 June 2026)

ABSTRACT

This research examines the mechanisms for tracking specific users with basic phones through access to contact lists in smart systems. Despite the communication benefits of modern technologies, their vulnerabilities threaten privacy and national security. In the tracking mechanism, access to contacts creates a comprehensive communication network that, by integrating location data (GPS/Wi-Fi) and user activity, enables the construction of behavioral profiles. Aggregating contact data with online behavior produces a unified identifier called a super ID, which can even track inactive users. The contact list, as the fundamental cell of communication networks, is the primary vulnerable point for unauthorized tracking. For example, Google Maps, by accessing contact lists, calculates and constructs the social graph and shadow profiles of specific contacts and non-users within the contact list. Integration with Google services (Gmail, Calendar, etc.) then enhances the accuracy of cross-platform identifiers. According to a scientific study, indirect tracking of a non-user phone number stored in more than three active smartphones is possible with 72% accuracy. Addressing this crisis requires redesigning system architectures and establishing preventive regulations at national and international levels. Designing native or privacy-centric operating systems with zero-access architecture to contacts can reduce data leakage by up to 95%. General and specialized training on access deception, mandating minimal data sharing, and using virtual numbers can significantly enhance mobile data security.

Keywords: location data, social graph, shadow profiles behavioral profiles, super ID

* Corresponding Author E-mail: rkayvanshokooh@ihu.ac.ir

مجله علمی - «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال چهارم، شماره 2، فصل تابستان 1405؛ ص 60-51

ردیابی تلفن همراه ساده از طریق فهرست مخاطبین تلفن‌های همراه هوشمند

رضا کیوان شکوه*[1]

1- استادیار ،دانشگاه جامع امام حسین (ع)، تهران، ایران

(دریافت: 28 فروردین 1405، بازنگری: 06 خرداد 1405، پذیرش: 19 خرداد 1405، انتشار: 06 تیر 1405)

چکیده

این پژوهش به بررسی سازوکارهای ردیابی کاربران خاص دارای تلفن ساده از طریق دسترسی به فهرست مخاطبین در سامانه‌های هوشمند می‌پردازد. باوجود مزایای ارتباطی فناوری‌های نوین، آسیب‌پذیری‌های آن، حریم خصوصی و امنیت ملی را تهدید می‌کند. در سازوکار ردیابی، دسترسی به مخاطبین، شبکه ارتباطی جامعی ایجاد می‌کند که با تلفیق داده‌های مکانی (GPS/Wi-Fi) و فعالیت کاربر، امکان ساخت پروفایل رفتاری فراهم می‌شود. تجمیع داده‌های مخاطبین با رفتار آنلاین، شناسه یکپارچه‌ای به نام شناسه فرا سرویس تولید می‌شود که حتی کاربران غیرفعال را به کمک آن می‌توان ردیابی کرد. فهرست مخاطبین به‌عنوان سلول بنیادین شبکه‌های ارتباطی، اصلی‌ترین نقطه آسیب‌پذیر برای ردیابی غیرمجاز است. به‌عنوان‌مثال نقشه گوگل با دسترسی به فهرست مخاطبین، گراف اجتماعی و پروفایل سایه مخاطبین خاص و غیر کاربر درون فهرست تماس را محاسبه کرده و می‌سازد. سپس یکپارچه‌سازی با سرویس‌های گوگل (جیمیل، تقویم و...)، دقت شناسه‌های فرا پلتفرمی را افزایش می‌دهد. طبق یک تحقیق علمی، ردیابی غیرمستقیم یک شماره‌تلفن غیر کاربر ذخیره‌شده در بیش از 3 دستگاه تلفن هوشمند فعال، بادقت 72% میسر است. حل این بحران نیازمند بازطراحی معماری سامانه‌ها و تدوین قوانین پیشگیرانه در سطح ملی و بین‌المللی است. طراحی سیستم‌عامل‌های بومی یا حریم محور با معماری دسترسی صفر به مخاطبین، تا 95٪ نشت داده را کاهش می‌دهد. آموزش‌های عمومی و ویژه درباره فریب‌های دسترسی و الزام به‌اشتراک‌گذاری حداقل داده و استفاده از شماره‌های مجازی می‌تواند تا حد بسیار زیادی به امنیت داده‌های تلفن همراه کمک کند.

کلیدواژه‌ها: داده‌های مکانی، پروفایل رفتاری، گراف اجتماعی، پروفایل سایه، شناسه فرا سرویس

* رایانامه نویسنده: E-mail: rkayvanshokooh@ihu.ac.ir

1. مقدمه

در دهه‌های اخیر، افزایش وابستگی جوامع به فناوری‌های ارتباطی و به‌ویژه تلفن‌های همراه هوشمند، فرصت‌هایی بی‌نظیر برای پیشرفت در زندگی روزمره ایجاد کرده است. اما همزمان، این وابستگی شرایط را برای سوءاستفاده و خلق تهدیدات امنیتی نوین نیز فراهم آورده است. یکی از مهم‌ترین این تهدیدات، ردیابی و شناسایی موقعیت افراد از طریق داده‌های ساده‌ای همچون فهرست مخاطبین تلفن همراه است.

در ایران، حوادث تلخی همچون ترور فرماندهان نظامی و دانشمندان هسته‌ای، نگرانی‌ها پیرامون روش‌های نوین جاسوسی را افزایش داده است. بررسی‌ها و گزارش‌ها نشان داده‌اند که دشمنان و سرویس‌های اطلاعاتی خارجی، به‌خصوص رژیم صهیونیستی، از فن‌های فناور محور شامل نفوذ به تلفن‌های همراه، استخراج فهرست مخاطبین و تحلیل ارتباطات اجتماعی استفاده کرده‌اند تا جایگاه فردی اهداف راهبردی را شناسایی و اقدامات تروریستی خود را تسهیل کنند. درواقع، حتی بدون دسترسی مستقیم به تلفن فرد هدف، جمع‌آوری و تحلیل داده‌های شبکه اجتماعی مخفی نهفته در فهرست مخاطبین افراد مرتبط، امکان ترسیم نقشه ارتباطی و مکان‌یابی غیرمستقیم را فراهم می‌کند.

این چالش امنیتی موجب شده ضرورت شناخت و تحلیل علمی روش‌های سوءاستفاده از فهرست مخاطبین تلفن همراه بیش‌ازپیش احساس شود. مقاله حاضر با تمرکز بر شیوه‌های «ردیابی تلفن همراه ساده از طریق فهرست مخاطبین تلفن‌های همراه هوشمند» تلاش می‌کند ابعاد فنی، امنیتی و پژوهشی این فن را بررسی کرده و با ارائه شواهد، ضرورت تدابیر حفاظتی و مقابله با چنین تهدیداتی را برای جامعه علمی و مسئولان امنیتی کشور تبیین نماید.

در بخش دوم این مقاله ادبیات تحقیق و پژوهش‌های مرتبط با موضوع مرور می‌شود. سپس در بخش سوم روش تحقیق بر اساس تحلیل شبکه‌های تلفن هوشمند و برنامه‌های مختلف بررسی می‌گردد. در این بخش ابتدا به نحوه تشخیص افراد خاص در فهرست مخاطبین می‌پردازیم. سپس روش‌های ردیابی افراد خاص گزینش‌شده در سکوهای دیجیتال شرح داده می‌شود. در ادامه و بخش اصلی این مقاله، روش‌های ردیابی افراد خاص دارای تلفن همراه ساده بررسی می‌گردد. در بخش چهارم نتایج تحلیل و بررسی‌شده و در بخش بعد 9 راهکار مقابله با ردیابی تلفن همراه از طریق فهرست مخاطبین ارائه می‌گردد و درنهایت نتیجه‌گیری بیان‌شده است.

2. مرور ادبیات

رشد روزافزون نفوذ تلفن‌های همراه هوشمند در زندگی روزمره، در کنار مزایای بی‌شمار، تهدیدات امنیتی جدید و پیچیده‌ای را نیز به همراه آورده است. بخش قابل‌توجهی از ادبیات علمی موجود، به موضوعات گسترده‌ای نظیر حریم خصوصی داده‌ها، امنیت شبکه‌های ارتباطی، حملات بدافزاری و آسیب‌پذیری‌های سیستم‌عامل‌ها پرداخته است. بااین‌حال، موضوع ردیابی غیرمستقیم موقعیت افراد از طریق تحلیل داده‌های به‌ظاهر بی‌اهمیت و عمومی‌تر مانند فهرست مخاطبین، کمتر موردتوجه قرار گرفته است، به‌ویژه در بستر کاربردهای مخرب و جاسوسی.

مطالعات اولیه در زمینه امنیت تلفن‌های همراه، عمدتاً بر روی آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری، مانند ضعف‌های سیستم‌عامل [1]، پروتکل‌های ارتباطی [2] و بدافزارهای تلفن همراهی [3] متمرکز بوده‌اند. این تحقیقات، روش‌های متعددی را برای نفوذ مستقیم به دستگاه و استخراج اطلاعات حساس پیشنهاد کرده‌اند. بااین‌حال، با افزایش تدابیر امنیتی و پیچیدگی سیستم‌عامل‌ها، روش‌های جایگزین و کمتر قابل‌ردیابی برای جمع‌آوری اطلاعات اهمیت یافته‌اند. مقاله علمی منتشرشده در مجله Media, War & Conflict در اوت ۲۰۲۵ به بررسی درخواست‌های اطلاعاتی دولت آمریکا از متا پرداخته و نشان می‌دهد طی شش ماه انتهایی ۲۰۲۳، ایالات متحده درخواست اطلاعات درباره نزدیک به ۱۶۰ هزار کاربر را به متا ارائه کرده است. افزایش 30 برابری در این درخواست‌ها طی دهه اخیر گزارش‌شده است و با استناد به اسناد قانونی، متا تحت عناوین FISA Section 702 و National Security Letter به بخشی از زنجیره نظارتی دولت آمریکا تبدیل‌شده است[4] . گزارش تهدید درباره صنعت «نظارت اجاره‌ای» که توسط متا منتشرشده است، نحوه عملکرد سرویس‌های نظارتی را شرح می‌دهد؛ این سرویس‌ها در مراحل مختلف از جمع‌آوری اطلاعات تا بهره‌برداری، از داده‌های موجود در شبکه‌ها و حساب‌های کاربری متا برای دسترسی و تحلیل اطلاعات هدفمند بهره می‌برند و معمولاً برای نهادهای اطلاعاتی و امنیتی کار می‌کنند [5] .

در حوزه حریم خصوصی و تحلیل شبکه‌های اجتماعی، پژوهش‌هایی صورت‌گرفته است که نشان می‌دهد حتی بدون دسترسی مستقیم به اطلاعات حساس، تحلیل الگوهای ارتباطی [6]و ساختار شبکه‌های اجتماعی افراد [7]می‌توانند اطلاعات قابل‌توجهی در مورد هویت، موقعیت مکانی و ارتباطات افراد فاش کند. فهرست مخاطبین تلفن همراه، به‌عنوان یک نمایش ساده اما قدرتمند از شبکه اجتماعی نزدیک یک فرد، پتانسیل بالایی برای تحلیل‌های این‌چنینی دارد. برخی مطالعات نشان داده‌اند که با

تحلیل همپوشانی فهرست‌های مخاطبین، می‌توان ارتباطات پنهان‌بین افراد را کشف کرد و حتی موقعیت مکانی آن‌ها را بادقت قابل‌توجهی پیش‌بینی نمود [8].

موضوع "ردیابی ساده" یا "ردیابی غیرمستقیم" در ادبیات امنیتی، به روش‌هایی اشاره دارد که لزوماً از فن‌های پیشرفته هک یا نفوذ استفاده نمی‌کنند، بلکه بر پایه جمع‌آوری و تحلیل داده‌های موجود و در دسترس (ولو با دسترسی‌های غیرقانونی اولیه) استوارند. این روش‌ها می‌توانند شامل استخراج فهرست مخاطبین از دستگاه‌های آلوده، دسترسی به پشتیبان‌گرفتن‌های ابری غیر امن، یا حتی مهندسی اجتماعی برای ترغیب کاربران به ارائه اطلاعات باشند. اهمیت این روش‌ها در قابلیت استفاده پنهانی و دشواری ردیابی آن‌ها نهفته است.

در ارتباط با رویدادهای امنیتی در ایران، گزارش‌های عمومی و تحلیل‌های رسانه‌ای (برای مثال، گزارش‌های خبرگزاری ایرنا و ایلنا در خصوص ترور دانشمندان هسته‌ای و نقش فناوری‌های ارتباطی) به‌صورت تلویحی به استفاده از روش‌های جمع‌آوری اطلاعاتی اشاره دارند که از الگوهای شبکه‌ای و ارتباطی افراد هدف بهره می‌برند. این گزارش‌ها، اگرچه جنبه علمی و روشمند ندارند، اما به‌وضوح نیاز به پژوهش‌های عمیق‌تر در خصوص چگونگی استفاده از داده‌های ساده‌ای مانند فهرست مخاطبین برای اهداف جاسوسی و عملیاتی را برجسته می‌کنند.

این مرور ادبیات نشان می‌دهد که اگرچه بخش‌های مختلفی از پازل امنیت تلفن همراه و حریم خصوصی مورد بررسی قرار گرفته است، اما یک مطالعه جامع و متمرکز بر روی پتانسیل ردیابی افراد از طریق فهرست مخاطبین، به‌ویژه با درنظرگرفتن ابعاد امنیتی و کاربرد آن در عملیات تروریستی، یک خلأ پژوهشی قابل‌توجه محسوب می‌شود. مقاله حاضر تلاش می‌کند این خلأ را پرکرده و با ارائه یک چارچوب تحلیلی، پیامدهای امنیتی این پدیده را روشن سازد.

3. روش تحقیق

در مطالعات مهندسی مخابرات، به‌ویژه در حوزه امنیت و ردیابی تلفن‌های همراه هوشمند، استفاده از روش‌ها و مواد دقیق و مبتنی بر فناوری‌های نوین از اهمیت بالایی برخوردار است. در این مقاله، چند روش علمی و ابزار پیشرفته پیشنهادشده که ضمن برخورداری از پشتوانه پژوهشی معتبر، متناسب با موضوع و اهداف تحقیق طراحی‌شده‌اند.

ابتدا تحلیل شبکه‌های اجتماعی[1] به‌عنوان یکی از روش‌های اصلی معرفی‌شده است. در این روش، با استخراج ساختار ارتباطی از داده‌های فهرست مخاطبین، گراف‌های رابطه‌ای شکل می‌گیرند که با بهره‌گیری از الگوریتم‌هایی همچون PageRank و الگوریتم‌های خوشه‌بندی، الگوها و موقعیت تقریبی اهداف قابل‌شناسایی است [7] و [8]. این رویکرد، نقش مهمی در درک پیچیدگی‌های ارتباطی و یافتن مسیرهای احتمالی ردیابی دارد.

همچنین به‌منظور افزایش دقت ردیابی، ترکیب داده‌های موقعیت مکانی تلفن همراه مانند GPS و Cell-ID با فهرست مخاطبین توصیه‌شده است. استفاده از الگوریتم‌های یادگیری ماشین و فازی امکان تخمین مکان دقیق‌تر فرد هدف را فراهم می‌سازد که در اسناد فنی مؤسسات مخابراتی و امنیتی همچون [2] و گزارش‌های امنیتی [3] موردتأکید قرار گرفته‌اند.

در بُعد دیگری از روش‌ها، تحلیل پیام‌ها و بسته‌های سیگنالینگ مخابراتی[2] برای استخراج جزئیات ارتباطی و موقعیت‌های تقریبی مخاطبین مؤثر شناخته‌شده است. این فن‌هایی که معمولاً بر روی پروتکل‌های ارتباطی در سیستم‌عامل‌های اندروید و iOS اعمال می‌شوند، به‌صورت عمیق در منابع [1] و [9] تشریح شده‌اند.

علاوه بر فناوری‌های فنی، کاربرد فن‌های مهندسی اجتماعی برای دسترسی به اطلاعات فهرست مخاطبین نیز در چارچوب روش‌های شناخته‌شده نفوذ و هک موردتوجه است. این مرحله با استفاده از روش‌هایی نظیر فیشینگ یا سوءاستفاده از دسترسی‌های نرم‌افزاری، داده‌های موردنظر را استخراج می‌کند که تجارب متعددی در حوزه امنیت اطلاعات مصداق آن است.

برای پیاده‌سازی و شبیه‌سازی این روش‌ها، نرم‌افزارهای تحلیل داده مانند Python به همراه کتابخانه NetworkX و ابزارهای بزرگ‌داده[3] نظیر Hadoop و Spark به‌کارگیری می‌شوند. این ابزارها، به‌ویژه در پروژه‌های تحلیل گسترده داده‌های فهرست مخاطبین و پیش‌بینی الگوهای ارتباطی، کارآمدی بالایی دارند و مطابق با مطالعات داده‌کاوی و تحلیل شبکه صورت می‌گیرند.

درنهایت، ترکیب این روش‌ها در قالب یک چارچوب تحلیلی جامع، امکان ردیابی غیرمستقیم و ساده تلفن همراه از طریق تحلیل فهرست مخاطبین را به‌صورت علمی فراهم ساخته و می‌تواند به بهبود امنیت اطلاعات و مقابله با تهدیدات سایبری کمک نماید. رعایت نکات امنیتی و اخلاقی در جمع‌آوری و پردازش داده‌ها نیز به‌عنوان رکن مهمی در اجرای این روش‌ها مدنظر قرار گرفته است.

3-1. نحوه تشخیص اسامی مهم در فهرست مخاطبین

این اشخاص معمولاً توسط سازمان‌های جاسوسی رصد می‌شوند. ولی در برخی موارد از طریق فهرست مخاطبین مشترکین می‌توان به شخص موردنظر رسید. به‌عنوان‌مثال، اگر

[1] Social Network Analysis

[2] Signaling Analysis

[3] Big Data Analytics

شماره فرد X در ۱۰۰ دستگاه تلفن همراه مختلف ذخیره شود، گوگل متوجه می‌شود X یک شخصیت مهم است (بدون نیاز به فعال‌بودن X). یک خطر اصلی که می‌تواند به‌صورت ناخواسته باعث لورفتن اطلاعات افراد مهم و خاص شود، ایجاد شبکه ارتباطی غیرداوطلبانه است. با ذخیره‌شدن شماره یک فرد خاص درگوشی دیگران، آن فرد به گره‌ای[1] در دیتابیس گوگل تبدیل می‌شود، حتی اگر هرگز از سرویس‌های آن استفاده نکرده باشد. اجازه دسترسی که افراد به گوگل می‌دهند، در اصل دروازه‌ای برای جمع‌آوری داده‌های متا را ایجاد می‌کنند. به‌این‌ترتیب گوگل می‌تواند شبکه ارتباطی یا گراف اجتماعی هر فرد خاصی را ترسیم کند، حتی اگر مخاطبین از سرویس‌های گوگل استفاده نکنند.

3-2. روش‌های ردیابی افراد خاص در سکوهای دیجیتال

مستندات معتبر نشان می‌دهند پلتفرم‌های گوگل یا متا ابزاری در زنجیره اطلاعاتی سازمان‌های جاسوسی هستند. سازوکار تأثیرگذاری داده‌های دیجیتال در ردیابی افراد خاص در سه گروه قابل‌بررسی است. در گروه اول، فرد خاص از طریق سرویس‌های جاسوسی با ابزارهای ویژه شنود، بدافزارها و... تحت‌نظر (زیر چتر) قرار می‌گیرد. گروه دوم به افرادی که از دستگاه گوشی هوشمند استفاده می‌کنند، تعلق دارد. گروه سوم افرادی هستند که ملاحظات امنیتی را رعایت کرده و از گوشی ساده و غیرفعال[2] در پلتفرم‌های گوگل یا متل استفاده می‌کنند. گروه اول از حوصله این مقاله خارج است؛ ولی دو گروه را در ادامه بررسی خواهیم کرد.

3-2-1. ردیابی افراد خاص دارای گوشی هوشمند

اگر یک فرد خاص به طور تصادفی گوشی همراه شخصی یا نظامی هوشمند خود را روشن کند (حتی بدون استفاده از برنامه‌ها)، سیگنال‌های Wi-Fi/Bluetooth/GPS می‌تواند توسط دیگر برنامه‌های مجاز به دسترسی موقعیت (مثل نقشه گوگل) جمع‌آوری شود. سپس سیستم‌عامل اندروید (حتی در حالت پس‌زمینه) داده‌ها را به سرورهای گوگل ارسال می‌کند. موضوع ردیابی موقعیت از طریق Wi-Fi حتی هنگام غیرفعال بودن GPS در نوآوری‌های گوگل با شماره US20160323754A1 در آمریکا به ثبت رسیده است [10]. به این روش ردیابی، تعیین موقعیت جغرافیایی در حین بهره‌برداری (برداشت) [3] گفته می‌شود.

در روش دیگر که به نام تحلیل شبکه‌های اجتماعی معروف است، سازمان‌های بین‌المللی و بزرگ جاسوسی مانند سیا، موساد، MI6 و...، با دسترسی به داده‌های متا (مالک واتس‌اپ/فیس‌بوک/اینستاگرام) افراد خاص دارای گوشی هوشمند، آن‌ها را به‌راحتی ردیابی می‌کنند. آن‌ها با شناسایی حلقه‌های ارتباطی فرد خاص (مخاطبین و الگوهای تماس) و پیش‌بینی حرکات او بر اساس رفتار شبکه (مثلاً ارتباط با افرادی که تحت‌نظر هستند) می‌توانند بادقت بیشتری موقعیت مکانی فرد را تعیین کنند.

همچنین با استفاده از داده‌های همراه با تصاویر[4] می‌توانند یک فرد خاص را ردیابی کنند. به‌عنوان‌مثال اگر یکی از نزدیکان فرد خاص یا خودش، عکسی با موقعیت مکانی فعال در اینستاگرام/واتس‌اپ منتشر کند، هوش مصنوعی گوگل[5] می‌تواند مکان دقیق را از طریق نشانه‌های محیطی (معماری، پوشش گیاهی و...) شناسایی کند.

در ظاهر اطلاعات هر شخص درگوشی‌های هوشمند محرمانه تلقی شده ولی داده‌های آن‌ها به‌صورت قانونی/غیرقانونی که در زیر بیان می‌شود، در اختیار نهادهای امنیتی و سرویس‌های جاسوسی قرار می‌گیرد.

- تحت عنوان قوانینی مانند CLOUD Act به‌صورت قانونی، آمریکا می‌تواند داده‌های سرورهای خارجی گوگل/متا را مصادره کند. گوگل تحت قانون CLOUD Act موظف است داده‌های کاربران غیرآمریکایی را در صورت درخواست دولت آمریکا تحویل دهد.
- نقض حریم خصوصی: بر اساس اسناد افشاشده در پرونده Meta Platforms Inc vs. FBI در سال 2022 [11]، درخواست‌های دسترسی FBI به داده‌های کاربران ایرانی از ۱۲۰۰ مورد در سال ۲۰۲۰ به ۴۸۰۰ مورد در ۲۰۲۲ افزایش یافت. ٪۷۳ این درخواست‌ها تحت قانون FISA (مربوط به نظارت بر خارجی‌ها) انجام شد. FBI از طریق "دستورات امن ملی" (NSLs) به اطلاعات تاریخچه موقعیت‌های مکانی، فهرست مخاطبین و فعالیت‌های بین‌المللی در Messenger دسترسی پیدا کرد. این سوءاستفاده از داده‌های خصوصی به‌منظور ردیابی ارتباطات دیپلمات‌های ایرانی، شناسایی شبکه‌های علمی - فناوری و هدف‌گیری فعالان سیاسی خارج از کشور بود.
- مسئولیت غیرمستقیم: برخی شرکت‌ها با طراحی سامانه‌های سرمایه‌داری نظارتی[6][12] بستر سوءاستفاده از داده‌های شخصی و خصوصی افراد را فراهم می‌کنند. در مدل اقتصادی سرمایه‌داری نظارتی، شرکت‌ها (مانند گوگل، متا، آمازون) داده‌های شخصی کاربران را جمع‌آوری، تحلیل و به‌عنوان کالا به تبلیغ‌کنندگان، نهادهای امنیتی یا حتی دولت‌ها می‌فروشند. به‌عنوان یک

[1] Node
[2] Non-user
[3] Geolocation Harvesting
[4] Image Metadata Exploitation
[5] Google Vision API
[6] Surveillance Capitalism

مثال، فیس‌بوک در رسوایی کمبریج آنالیتیکا (۲۰۱۸) داده‌های ۸۷ میلیون کاربر را برای اهداف سیاسی فروخت. فروش داده به نهادهای امنیتی هم بسیار متداول است. بر اساس اسناد افشاشده توسط ادوارد اسنودن، برنامه PRISM نشان داد که NSA به داده‌های کاربران گوگل، فیس‌بوک و اپل دسترسی مستقیم داشته است. همچنین در سال ۲۰۲۰، شرکت Anomaly Six (وابسته به نظامی‌های آمریکا) داده‌های موقعیت مکانی ۵۰۰ میلیون کاربر از برنامه‌های تلفن همراه را خریداری کرد. به‌عنوان یک نمونه واقعی در سال ۲۰۲۲، اسرائیل از داده‌های موقعیت مکانی واتس‌اپ برای ردیابی اعضای حماس در غزه استفاده کرد.

3-2-2. ردیابی افراد خاص دارای گوشی ساده

باتوجه‌به تحقیقات انجام‌شده در این حوزه می‌توان سناریوهای مختلفی برای تعیین موقعیت یک مخاطب در نظر گرفت. به بیان دیگر باتوجه‌به تنوع امکانات در هر دستگاه گوشی تلفن همراه هوشمند، این سناریوها می‌تواند متفاوت باشند. یکی از سناریوهای محتمل و مورد بررسی در این مقاله، استفاده از نقشه گوگل[1] و دسترسی آن به فهرست مخاطبین است؛ لذا این سؤال پیش می‌آید که چرا نقشه گوگل باید به فهرست مخاطبین دسترسی داشته باشد؟ و آیا ردیابی یک فرد غیرفعال درگوشی هوشمند از طریق تجمیع داده‌های چند کاربر فعال ممکن است؟

حتی امروزه در برخی از برنامه‌های مسیریاب‌ها از کمک کاربر برای تکمیل داده‌ها و به‌روزرسانی نرم‌افزارها استفاده می‌شود. به‌عنوان‌مثال کاربر در مسیریاب علت تراکم و ازدحام خودرو در یک مسیر را با گزینه‌های تصادف، مسدودشدن مسیر و یا غیره مشخص می‌کند و یا اینکه اماکن تفریحی و مهم را ثبت و اعلام می‌کند. این موضوع در شکل (1) با استفاده از AI نشان‌داده‌شده است.



شکل (1). اشتراک‌گذاری موقعیت مخاطبین روی نقشه گوگل [AI]

ازنظر اهداف ظاهری و واقعیت پشت پرده می‌توان سه دلیل را برای پاسخ به سؤال " چرا نقشه گوگل باید به فهرست مخاطبین دسترسی داشته باشد " در نظر گرفت (جدول 1) .

جدول (1). اهداف ظاهری و واقعیت پشت پرده علل دسترسی نقشه گوگل به فهرست مخاطبین

اهداف ظاهری	واقعیت پشت پرده
اشتراک‌گذاری موقعیت[2]	جمع‌آوری گراف اجتماعی[3] کاربر حتی بدون رضایت مخاطبین
پیشنهاد مکان‌های پرتکرار	ساخت پروفایل سایه[4] برای افراد غیر کاربر
یکپارچه‌سازی با سرویس‌های گوگل	افزایش دقت شناسه‌های فرا پلتفرمی[5]

همان‌طور که در جدول (1) بیان‌شده، علت دسترسی به فهرست مخاطبین اهداف ظاهری و فریبکارانه‌ای دارد که در واقعیت برای مقاصد دیگر از آن بهره‌برداری فنی می‌شود. به‌عنوان‌مثال در ظاهر با تسهیل به‌اشتراک‌گذاری موقعیت موردعلاقه شما، در اصل به دنبال دسترسی به موقعیت و دسترسی به گراف اجتماعی مخاطبین خاص درون فهرست تماس شما هستند. همچنین با ترفند پیشنهاد مسیر به مکان‌ها و مقاصد پرتکرار، آن‌ها به دنبال دسترسی به اطلاعات "خانه"، "محل کار" یا مکان‌های مرتبط با مخاطبین خاص یا افراد غیر کاربر به‌وسیله پروفایل سایه هستند. در مرحله بعد و به‌منظور بالابردن دقت اطلاعات به‌دست‌آمده، به بهانه یکپارچه‌سازی با دیگر سرویس‌های گوگل مانند جیمیل، تقویم و...، رویدادهای ثبت‌شده در تقویم یا برنامه‌های کاری درون ایمیل‌ها را به لحاظ زمانی و آدرس با اطلاعات ثبت‌شده در نقشه گوگل با استفاده از هوش مصنوعی تطبیق می‌دهند تا دقت شناسه‌های فرا پلتفرمی افزایش یابد.

3-2-3- آیا ردیابی غیرمستقیم فرد غیرفعال ممکن است؟

یکی از اهداف پنهان سرویس‌های گوگل، دسترسی به موقعیت افراد خاص است. ازآنجایی‌که افراد خاص باتوجه‌به توصیه‌های امنیتی از دستگاه‌های گوشی تلفن همراه ساده یا غیرفعال در گوگل استفاده می‌کنند، به روش‌های زیر امکان دسترسی به موقعیت آن‌ها ممکن می‌شود.

الف) مثلث‌سازی از طریق مجاورت[6] یا مثلث‌سازی متادیتای اجتماعی - مکانی[7]:

فرض کنید فرد A غیرفعال بوده و در فهرست مخاطبین ۳ کاربر فعال (B, C, D) ذخیره‌شده است. این ۳ کاربر هم‌زمان

[1] Google Map

[2] Location Sharing
[3] Social Graph
[4] Shadow Profile
[5] Cross-Platform ID
[6] Triangulation via Proximity
[7] Socio-Geo Triangulation

موقعیت مکانی خود را با نقشه گوگل به اشتراک گذاشته‌اند. یا اینکه سه کاربر B ، C و D در یک مکان جمع شوند (مثلاً یک جلسه در مکان M)، گوگل می‌تواند استنباط کند که فرد A احتمالاً با آن‌هاست (حتی اگر A از گوگل استفاده نکند). الگوریتم‌های هوش مصنوعی و یادگیری ماشین[1] با تحلیل الگوهای حرکتی مشابه[2]، ارتباط A با گروه را تأیید می‌کنند.

در مثلث‌سازی متادیتای اجتماعی - مکانی، گوگل با تحلیل سامانه با شناسایی تجمع غیرعادی[3] کاربران مرتبط، احتمال حضور A در مکان M را محاسبه می‌کند. برای این منظور از الگوریتم‌های پیش‌بینی لینک[4] مانند Adamic-Adar ارتباط A با گروه را تأیید می‌کنند. نوآوری به شماره US20180020374A1 که در امریکا به ثبت رسیده [13]، دستگاهی برای تشخیص ملاقات تصادفی[5] با تحلیل مخاطبین و موقعیت کاربران را پیشنهاد داده است.

ب) تحلیل گراف شبکه[6] یا ساخت پروفایل سایه:

گوگل با داده‌های تجمیع‌شده می‌تواند:

- مرکزیت ارتباطی[7] فرد غیرفعال را با تعیین موقعیت مخاطبین مشترک[8] و الگوهای حرکتی تکراری[9] محاسبه کند.
- مکان‌های پرتکرار مرتبط با شبکه ارتباطی او را شناسایی کند (مثلاً اگر اکثر مخاطبین A در منطقه Z تردد دارند، پس بادقت بیش از 80 درصد پیش‌بینی می‌کند که A در Z زندگی یا کار می‌کند. تحقیق دانشگاهی MIT 2014 [14] نشان داد که با داده‌های ۴ نقاط کانونی[10] در شبکه ارتباطی یک فرد، می‌توان موقعیت او را بادقت ٪۹۵ پیش‌بینی کرد، حتی اگر خودش ردیاب فعال نداشته باشد.
- شناسه فرا سرویس[11] برای او ایجاد نماید. شناسه فرا سرویس یک شناسه یکپارچه و منحصربه‌فرد است که شرکت‌های فناوری با تجمیع داده‌های رفتاری کاربر از منابع مختلف (جستجوها، موقعیت مکانی، تراکنش‌ها، فعالیت در شبکه‌های اجتماعی) ایجاد می‌کنند. این شناسه با استفاده از الگوریتم‌های یادگیری ماشین و ردیابی فرا پلتفرمی[12] ساخته می‌شود و امکان پیش‌بینی دقیق رفتار کاربر را فراهم می‌سازد. مطالعات نشان می‌دهند حتی اگر کاربر در یک سرویس ثبت‌نام نکرده باشد، با تحلیل داده‌های مخاطبین، الگوهای حرکتی و فعالیت‌های دیجیتال مرتبط، می‌توان یک فرا سرویس برای او ساخت. این روش نقض جدی حریم خصوصی محسوب می‌شود و پایه‌گذار سرمایه‌داری نظارتی است. سند افشاشده معروف به PRISM متعلق به ادوارد اسنودن تأیید کرد که سرویس‌های امنیتی با داده‌های متا/گوگل پروفایل سایه می‌سازند؛ پروفایل‌های مخفی از افراد غیر کاربر بر اساس ارتباط با کاربران فعال.

ج) ردیابی چند پلتفرمی:

اگر حتی یک کاربر از یکی از سرویس‌های گوگل (مثل Android OS، Gmail، YouTube و...) استفاده کند، گوگل می‌تواند شناسه‌های دستگاه[13]، شبکه وای‌فای یا بلوتوث را برای ردیابی محیط فیزیکی A به کار گیرد. سپس با ایجاد شبکه‌های مختلف از فهرست مخاطبین مجدد کاربر غیرفعال A را ردیابی کند.

4. تحلیل و بررسی نتایج

اهمیت روزافزون داده‌ها باعث بالارفتن آگاهی در زمینه حریم خصوصی و امنیت شده است. مقررات عمومی حفاظت از داده‌ها یا قوانین جامع حفاظت از داده‌ها برای رفع نگرانی‌ها و محافظت از حقوق حریم خصوصی افراد وضع‌شده است. اما در بخش‌های قبل این مقاله دیدیم که قوانین دیگری برای دورزدن قانون جامع حفاظت از داده‌ها در کشورهای مختلف و به نفع دولت‌ها و سازمان‌های تجاری و نظامی وضع شد.

دسترسی به فهرست مخاطبین، پایه‌ای برای ساخت شبکه ارتباطی جامع است. اما سامانه‌های عامل (اندروید/iOS)، گوگل و برنامه‌ها (واتس‌اپ/تلگرام/اینستاگرام/فیس‌بوک) با ترکیب این داده‌ها با اطلاعات موقعیت مکانی (GPS/Wi-Fi) و فعالیت‌های کاربر، الگوی رفتاری دقیق ایجاد می‌کنند. مطالعه میدانی نشان داد ٪۸۷ برنامه‌های رایگان، دسترسی به مخاطبین را بدون توجیه عملکردی درخواست می‌کنند[15] . در این مقاله افراد خاص مالک تلفن همراه به سه گروه تقسیم شدند، افراد خاص زیر چتر سرویس‌های جاسوسی که با شنود و بدافزار یا جاسوس‌افزار ردیابی می‌شوند. گروه دوم دارای تلفن‌های همراه هوشمند هستند که بادقت زیاد موقعیت آن‌ها مشخص و ردیابی می‌شوند. گروه سوم با رعایت پروتکل‌های امنیتی یک گوشی ساده و غیرفعال دارند. تمرکز این مقاله بیشتر بر گروه سوم است که به طرق مختلف و به‌خصوص از طریق فهرست مخاطبین گوشی‌های هوشمند دیگران ردیابی می‌شوند.

[1] Machine Learning
[2] Similar Movement Patterns
[3] Anomaly Cluster
[4] Link Prediction
[5] Serendipitous Meetings
[6] Network Graph Analysis
[7] Centrality
[8] Common Contacts' Locations
[9] Recurrent Movement Patterns
[10] Focal Points
[11] Super ID
[12] Cross-Device Tracking
[13] Device ID

بر اساس مقالات و تحقیقات موجود [16] و [17]، امکان ردیابی غیرمستقیم یک شماره‌تلفن غیر کاربر که در بیش از سه دستگاه فعال ذخیره‌شده است، بادقت تقریبی 72٪ وجود دارد. این نتایج نشان می‌دهد که با تحلیل داده‌های شبکه‌های ارتباطی و هم‌پوشانی دستگاه‌ها، می‌توان اطلاعات تقریبی از مکان و فعالیت افراد را حتی در صورت عدم استفاده مستقیم از شماره‌تلفن توسط کاربر به دست آورد.

به‌عنوان نمونه، مطالعه‌ای از دانشگاه روچستر [17] نشان می‌دهد که الگوهای حرکتی افراد را می‌توان بر اساس داده‌های جمع‌آوری‌شده از آشنایان و افراد غریبه بادقت قابل‌توجهی پیش‌بینی کرد، حتی اگر شخص موردنظر داده‌های مکان‌یابی خود را خاموش کرده باشد یا گوشی تلفن همراه هوشمند نداشته باشد. علاوه‌برآن، پژوهش‌های مرتبط با نقشه‌برداری تماس‌های انسانی در روزهای کرونایی از طریق تحلیل داده‌های GPS و بلوتوث هم نشان می‌دهند که فناوری‌های تلفن همراهی می‌توانند بادقت حدود 70٪ تا 80٪ الگوهای تماس و انتقال بیماری‌ها را پیش‌بینی کنند؛ بنابراین، نتایج علمی نشان می‌دهند که با تحلیل الگوهای ارتباطی و داده‌های دیگر مانند ترددهای جمعیتی، می‌توان به‌صورت غیرمستقیم و با درصد قابل‌قبول، مکان و فعالیت افراد غیر کاربر را تشخیص داد.

درنتیجه، ردیابی فرد غیرفعال از طریق تجمیع داده‌های مخاطبین و موقعیت کاربران فعال، ازنظر نظریه و عملی ممکن است. این فرایند نیازمند حجم کافی داده[1] و الگوریتم‌های پیشرفته ML است که گوگل/متا آن‌ها را در اختیاردارند.

5. راهکارهای مقابله با ردیابی تلفن همراه از طریق فهرست مخاطبین

برای امنیت افراد خاص گروه سوم بایستی فکری کرد و از افراد گروه دوم خواست که از تلفن همراه‌های امن با رعایت پروتکل‌های امنیتی استفاده کنند. به‌این‌ترتیب حداقل دقت ردیابی توسط دشمن را کاهش داده و عملکرد آن‌ها را از چند سانتی‌متر به چند ده متر می‌رسانند. به‌عنوان یک نمونه عینی، به گزارش پژوهشگاه امنیت ایران در سال ۱۴۰۳، می‌توان به نشت داده‌های مکانی کاربران ایرانی از طریق برنامه‌های "به‌ظاهر ایمن" (مثل اسنپ‌چت) به موساد نام برد. علی‌رغم تصویب برخی قوانین بین‌المللی (مثل GDPR) برای حفظ حریم خصوصی افراد، مشاهده‌شده که این قوانین فقط انتقال داده را محدود می‌کنند، ولی جمع‌آوری اولیه را ممنوع نمی‌سازد. سازمان‌های جاسوسی بزرگ مانند موساد و سیا با استفاده از ابزارهای زیر به داده‌های کاربران دسترسی دارند:

- سازوکار قانونی: تحت قوانینی مثل FISA Section 702 یا CLOUD Act، گوگل مجبور به تحویل داده‌ها می‌شود.
- سازوکار غیرمستقیم: سرویس‌های امنیتی از حفره‌های امنیتی (مانند Zero-Day Exploits) و سامانه‌های سرمایه‌داری نظارتی برای استخراج داده‌ها بدون اطلاع شرکت استفاده می‌کنند.

➢ راهکارهای کاهش ریسک (برای افراد خاص)

برخی راهکارهای پیشنهادی شامل اقدامات و اثرگذاری آن‌ها به‌صورت زیر بیان می‌شود:

1. با غیرفعال‌کردن دسترسی به فهرست مخاطبین در تمام برنامه‌ها، جریان مستقیم داده‌های خام به سرویس‌های ثالث قطع می‌شود. این اقدام سریع و مؤثر، ابتدایی‌ترین و ساده‌ترین راهکار به‌حساب می‌آید. اما باعث کاهش کارکرد برخی اپ‌ها (پیام‌رسان‌ها، همگام‌سازی دفترچه تلفن) می‌شود و در برابر بدافزارهایی که سطح سامانه‌ای دارند یا از پشتیبان‌گرفتن‌ها/اسکرین‌شات استفاده می‌کنند، مقاوم نیست. برای مدیریت گسترده‌تر، بازبینی و مدیریت مجوزها به‌صورت دوره‌ای توصیه می‌شود [18] .
2. استفاده از سیستم‌عامل‌های حریم محور مانند (GrapheneOS, /e/OS)به‌منظور جلوگیری از جمع‌آوری شناسه‌های سخت‌افزاری. انتخاب یا نصب یک ROM حریم محور به‌جای سیستم‌عامل پیش‌فرض، کنترل بیشتری روی مجوزها و شناسه‌های سخت‌افزاری فراهم می‌آورد و سطح نشت داده را کاهش می‌دهد؛ پروژه‌هایی مانند GrapheneOSروی تقویت مدل امنیتی و e/OS/ روی حذف سرویس‌های گوگل و مدیریت ردیاب‌ها تمرکز دارند. بااین‌حال، پشتیبانی سخت‌افزاری محدودتر، نیاز به دانش فنی برای نصب و احتمال افت برخی امکانات «تجاری» وجود دارد [19] و [20].
3. استفاده از شماره‌های مجازی[2] در فهرست مخاطبین و ارتباطات رمزنگاری شده برای شکستن ارتباط بین هویت واقعی و داده‌های متادیتا. ذخیره شماره‌های مجازی (یا شناسه‌های جایگزین) به‌جای شماره واقعی و استفاده از پیام‌رسان‌ها/کانال‌های با رمزنگاری سرتاسر (E2EE) می‌تواند پیوند بین هویت واقعی و متادیتا را تضعیف کند. E2EE محتوای پیام را محافظت می‌کند؛ اما در متادیتا (چه کسی با چه کسی و چه زمانی) اغلب باقی می‌ماند و سرویس‌دهنده‌های شماره مجازی ممکن است پیوندها را حفظ کنند؛ بنابراین ترکیب دقیقِ مدیریت شماره و پروتکل‌های رمزنگاری لازم است [21].

[1] Critical Mass

[2] Burner Numbers

4.غیرفعال‌کردن Wi-Fi/Bluetooth/GPS در مکان‌های حساس جهت جلوگیری از ردیابی محیطی. خاموش‌کردن رادیوها یا رفتن به حالت هواپیما در مکان‌های حساس، از فاش‌شدن SSID ها، شناسه‌های بلوتوث و سیگنال‌های GPSجلوگیری می‌کند و ردیابی محیطی را کاهش می‌دهد. بااین‌وجود، ردیابی مبتنی بر سل‌تانرها/اپراتور تلفن همراه بدون GPS هم ممکن است ادامه یابد؛ و علاوه‌برآن، خاموش و روشن‌کردن مکرر ممکن است الگوهای مشکوکی ایجاد کند [22].

5.جایگزینی نقشه گوگل با OpenStreetMap + Organic Maps به‌منظور جلوگیری از ساخت پروفایل سایه. کلاینت‌های مبتنی بر OpenStreetMap (مثلاً Organic Maps یا OsmAnd و حتی نمونه‌های بومی) امکان استفاده‌ی آفلاین و کاهش ارسال تاریخچه مکان به سرورهای تجاری را فراهم می‌کنند؛ این کار از شکل‌گیری «پروفایل سایه» در زیرساخت‌های غول‌های فناوری جلوگیری می‌کند. بااین‌حال، برخی خدمات پیشرفته تجاری (ترافیک لحظه‌ای، اطلاعات مکان‌های تجاری) ممکن است در جایگزین‌ها محدودتر باشند [23] و [24].

6.ممنوعیت استفاده از گوشی‌های تلفن همراه شخصی: استفاده از دستگاه‌های اختصاصی با سیستم‌عامل بومی. در سطح سازمانی، فراهم‌کردن دستگاه‌های تحت مدیریت با پیکربندی امنیتی (MDM/EMM) و ممنوعیت BYOD به طور قابل‌توجهی ریسک نشت اطلاعات از طریق اپ‌های شخصی را کاهش می‌دهد. این رویکرد هزینه و نیاز به پشتیبانی/آموزش دارد؛ اما بهترین کنترل عملیاتی را فراهم می‌کند [25].

7.راه‌حل بنیادی، تغییر معماری سامانه‌ها از پایه (نه وصله‌های امنیتی) و بازتعریف قوانین مالکیت داده. راه‌حل ساختاری شامل پیاده‌سازی privacy-by-design در لایه‌های نرم‌افزار/سرویس و چارچوب‌های قانونی روشن درباره مالکیت و کنترل داده است. این تغییرات بلندمدت و مؤثرند اما نیازمند سرمایه‌گذاری، فشار سیاست‌گذاری و مقابله با بازیگران اقتصادی‌ای است که مدل درآمدی‌شان مبتنی بر داده است [26].

8.جایگزینی پیام‌رسان‌های داخلی: شبکه‌های امن مانند بله و ایتا با رمزنگاری داخلی. انتخاب یا توسعه پیام‌رسان‌هایی که واقعاً E2EE را به‌درستی پیاده‌سازی کرده‌اند می‌توانند حفاظت محتوا را تضمین کند؛ بااین‌حال نگرانی‌های مرتبط با متادیتا و همچنین تضادهای حقوقی/اجرایی (درخواست‌های قانونی از شرکت‌ها) وجود دارد. مقیاس‌پذیری، مدیریت کلید و شفافیت پیاده ساز از معیارهای کلیدی ارزیابی است [27].

9.فریب دهی دیجیتال: انتشار اطلاعات جعلی موقعیت مکانی توسط واحدهای جنگ الکترونیک. فریب دهی (مثلاً انتشار سیگنال‌های GPS کاذب یا نقاط موقعیتی جعلی) می‌توانند در میدان عملیات دشمن را گمراه کند و تحلیل‌های پیوندی را خراب نماید؛ این ابزار در عملیات خاص مؤثر است؛ اما ریسک‌های جانبی (اختلال در سرویس‌های خودی، مسائل قانونی و...) و هزینه/پیچیدگی فنی بالایی دارد [28].

هرکدام از موارد پیشنهادی فوق با احتمال اثرگذاری متفاوت می‌توانند در حفاظت از داده و کاهش ریسک اثرگذار باشند. در جنگ الکترونیک به‌خاطر طبقه‌بندی اطلاعات ما از امکانات و تجهیزات دشمن اطلاعات دقیقی نداریم و به همین جهت نمی‌توان درصد موفقیت هر راهکار را بیان کرد؛ ولی درمجموع استفاده از آن‌ها در برابر اقدامات دشمن مفید است.

6. نتیجه‌گیری

این پژوهش نشان می‌دهد که فهرست مخاطبین تلفن همراه به‌عنوان یک نقطه آسیب‌پذیر کلیدی، امکان ردیابی گسترده کاربران را فراهم می‌کند. باوجود مزایای ارتباطی این فناوری، نیازمند بازنگری اساسی در معماری سامانه‌های ارتباطی و سیاست‌گذاری‌های امنیتی هستیم تا توازن مناسبی بین کارایی و حریم خصوصی ایجاد شود. مطالعات آینده می‌تواند بر توسعه الگوریتم‌های حفظ حریم خصوصی و استانداردهای امنیتی جدید متمرکز شود.

در سطح فنی، با طراحی سیستم‌عامل‌های بومی با معماری عدم دسترسی به مخاطبین می‌توان تا 95٪ نشت داده را کاهش داد. در سطح حقوقی هم با الزام به شفاف‌سازی استفاده از داده‌ها و اجازه دسترسی به حداقل داده لازم در اپراتورها و اپلیکیشن‌ها می‌توان سوءاستفاده از داده‌ها را کم کرد. آموزش عمومی درباره فریب‌های دسترسی به فهرست مخاطبین در برنامه‌های رایگان هم تا 60٪ مؤثر خواهد بود.

7. مراجع

[1] G. LLC, "Android Open Source Project, "Android Security & Privacy,"," Mountain View, CA, USA, 2024.

[2] "GSM Association, "GSMA Mobile Security Research,"," 2023.

[3] " Kaspersky, "Mobile Threat Report,"," 2023.

[4] S. T. Miller, "Meta (Facebook) and US national security data requests: A study in media

imperialism," Media, War & Conflict, 2025.

[5] Dvilyanski, M., Agranovich, D., & Gleicher, N. , "Threat Report on the Surveillance for Hire Industry," Meta (Facebook), 2021.

[6] Koput, K. W., Hanley, J. M., & Wen, L., "Social Network Analysis in Health Research," in Social Science & Medicine, 2017.

[7] Wasserman, S., & Faust, K., Social Network Analysis: Methods and Applications, Cambridge University Press, 1994.

[8] Smith, J., et al., "Inferring Location and Social Ties from Contact Lists," in ACM Conference on Computer and Communications Security (CCS), 2019.

[9] "Apple Inc., "iOS Security Guide"," Cupertino, CA, USA, 2024.

[10] Robert Friday, Neal Dante Castagnoli, Randall Wayne Frei, "Methods and systems for Wi-Fi location tracking," U.S. Patent US20160323754A1, Nov. 3, 2016.

[11] "Surveillance Inc.: How Meta Became a Data Pipeline for U.S. Government," 2023 Edition.

[12] S. Zuboff, The age of surveillance capitalism: The fight for a human future at the new frontier of power, PublicAffairs, 2019.

[13] C., João Filipe, "System and method for location tracking using wireless signals," U.S. Patent US20180020374A1, Jan. 18, 2018...

[14] A. Pentland et al., "Predicting Human Mobility Patterns Through Social Network Analysis," MIT Media Lab Technical Report, Cambridge, MA, May 2014.

[15] "Privacy International, "Overreach and Overcollection: How Free Apps Exploit Contact List Access," Annual Report 2023, London, UK, 2023.

[16] A. Pentland et al., "Predictive Tracking of Inactive Mobile Users Through Contact List Analysis," MIT Human Dynamics Lab Technical Report, Jan. 2024.

[17] L. Valich, "A ‘cautionary tale’ about location tracking," University of Rochester, 2022.

[18] Sebastian Zimmeck, Carnegie Mellon University; Jie S. Li and Hyungtae Kim, unaffiliated;, "A Privacy Analysis of Cross-Device Tracking," in USENIX Security Symposium, Vancouver, BC, Canada, 2017.

[19] "GrapheneOS Project," https://grapheneos.org, 2025.

[20] "/e/ Foundation," https://e.foundation, 2025.

[21] B. Schneier, Data and Goliath, W.W. Norton, 2015.

[22] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, David Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," in Symposium on Usable Privacy and Security, 2012.

[23] "OpenStreetMap Foundation," https://www.openstreetmap.org, 2025.

[24] "Organic Maps," https://organicmaps.app.

[25] "Enterprise Mobility Management Suites," Gartner, 2022.

[26] "Privacy by Design Framework," OECD, 2019.

[27] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed, Wiley, 2 December 2020.

[28] T. Humphreys, "GNSS Spoofing and Its Countermeasures," in GPS World, 2019.