

Wer sucht, der findet: Micro-Tracker

Bei der Suche nach dem Wohnungsschlüssel versprechen die neuen Micro-Tracker Abhilfe: Ein kleines, zentimetergroßes Ortungsgerät¹ in Form eines Schlüsselanhängers am Schlüsselbund kann mit dem Smartphone aufgespürt werden. Im Unterschied zu Mobiltelefonen oder GPS-Geräten haben die Micro-Tracker allerdings keine eigene Anbindung an das Internet, sondern melden via Bluetooth² ihre Anwesenheit automatisch an nahegelegene Geräte, die mit dem Internet verbunden und in das passende Ortungsnetzwerk integriert sind (wie z. B. Laptops, Tablets, Smartphones). Was Micro-Tracker so attraktiv macht ist, dass sie im Vergleich zu herkömmlichen Ortungsgeräten klein, kompakt und mit langlebigen Batterien ausgerüstet sind. Sie funktionieren praktisch überall, solange ein passendes mobiles Endgerät in der Nähe ist. Mit der stetigen Zunahme an internetfähigen Geräten stehen dadurch bereits jetzt engmaschige, lokale Ortungsnetzwerke zur Verfügung, die vor missbräuchlicher Verwendung nicht gefeit sind.

Daten aus Micro-Trackern sind wertvoll, was bisherige Forschungsergebnisse zur Datenanalyse tragbarer Bluetooth-Sensoren, wie z. B. Fitness-Tracker, untermauern. Sie speichern Daten wie die zurückgelegten Schritte, aus denen anhand einer forensischen Analyse Aktivitäten, Routinen und Ungereimtheiten identifiziert werden können (Hantke&Dewald 2020). Aber auch während der Corona-Krise können Anwendungen, die auf Bluetooth-Signalerkennung basieren, wertvolle Informationen zum Infektionsverlauf in der Bevölkerung liefern (Dyo et al. 2020) (siehe [Pandemiemanagement](#)). Angesichts des Risikos des Datenhacks, wird dem Datenschutz in allen angebotenen Lösungen etwa durch entsprechende Verschlüsselung der übertragenen Daten Rechnung getragen. Was passiert aber, wenn jemand unbemerkt einen Micro-Tracker im Rucksack eines anderen platziert, um die Person so einfach übers Smartphone verfolgen zu können? Das Micro-Tracker-Design mancher Anbieter verspricht zusätzliche Schutzmechanismen, die strafrechtlich relevanten Angriffen auf die Privatsphäre, wie z. B. Stalking, entgegenwirken sollen.³ Im Idealfall erhält das eigene Smartphone eine Benachrichtigung, wenn sich über eine längere Zeit ein unbekannter Micro-Tracker in der Nähe mitbewegt. Hat die gestalkte Person allerdings keine passende App installiert, erhält sie auch keine Benachrichtigung. Daher gibt das Mini-Ortungsgerät zusätzlich einen Ton ab, wenn es sich für einen längeren Zeitraum nicht in der Nähe des Geräts befindet, an dem es registriert wurde. Anhand des akustischen Signals können auch Perso-

¹ Auf Englisch „Tracking Device“, aber aufgrund der Größe auch „Micro-“ oder „Mini-Tracker“ oder in Hinblick auf ihre Funktion „Bluetooth-Tracker“ oder „Sensor Tags“ genannt. Auch unter den gängigen Markennamen, wie z. B. AirTag (Apple) oder SmartTag (Samsung) u. a., sind Micro-Tracker bekannt.

² Aber auch NFC- oder Ultrabreitband-Technologien kommen bei der Objektsuche zum Einsatz.

³ support.apple.com/en-us/HT212227.

nen ohne passende App den Micro-Tracker auffinden. Bis der unbekannte Micro-Tracker anfängt zu piepen, dauert es zwischen acht und 24 Stunden. Ein Selbstversuch zweier Journalisten zeigte, dass der Lautsprecher eines Micro-Trackers problemlos deaktiviert werden kann und es mit Micro-Trackern tatsächlich besonders einfach ist, Personen zu stalken.⁴

Micro-Tracker zeitigen ein hohes Missbrauchspotenzial und werfen damit breitere gesellschaftliche Fragen auf. Was passiert, wenn die umfassende Bereitstellung privater Micro-Tracking-Technologien öffentliche Sicherheit gefährdet? Welche gesellschaftlichen Abhängigkeiten können zukünftig durch technologische Pfadabhängigkeiten, Lock-in-Effekte und Technologie-Monopole⁵ entstehen? Es ist z. B. vorstellbar, dass Micro-Tracker-BesitzerInnen einer bestimmten Marke zukünftig eventuell einem höheren Stalking-Risiko ausgesetzt sind als die einer anderen Marke.⁶ Die zentrale Frage bleibt, wie bei zunehmend komplexeren Bedingungen, z. B. durch intransparente proprietäre Systeme, die Freiheit, Anonymität und Handlungsautonomie von BürgerInnen nachhaltig garantiert werden kann. Denkbar wäre demnach ein alternatives Anwendungsszenario, in dem BürgerInnen universelle und nachhaltige Micro-Tracker in unabhängigen, kollaborativen Ortungssystemen nutzen (siehe Themen [Dezentralisierte Kollaborationsplattformen](#) und [Lebensmittel-Tracking](#)), z. B. um Sharing-Modelle umzusetzen und die Verfügbarkeit gemeinschaftlich genutzter Gegenstände im Auge behalten zu können. In einem FTA-Prozess könnten die zukünftigen Potenziale und Herausforderungen von Micro-Trackern weiter exploriert und in einem umfassenderen gesellschaftlichen Kontext verortet werden.

Zitierte Literatur

- Dyo, V., Ali, J. und Ieee, 2020, Privacy-preserving Identity Broadcast for Contact Tracing Applications, *12th Wireless Days Conference (WD 2021)*.
Hantke, F. und Dewald, A., 2020, How can data from fitness trackers be obtained and analyzed with a forensic approach?, *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 7-11 Sept.

⁴ [washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/](https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/).

⁵ derstandard.at/story/2000126019954/kartellbeschwerde-ungewolltes-tracking-und-co-fragen-rund-um-apples-airtags.

⁶ Wenn z. B. vergleichbare Standards für das Sicherheitsdesign der Micro-Tracker oder notwendige Infrastrukturen (zugängliche Ortungsnetzwerke) fehlen.