

Wischnen, Tippen, Zoomen: Forscher tracken anhand von Touch-Gesten

Unsere Bewegungen auf dem Touchscreen sind so individuell, dass sie uns trackbar machen, zeigt ein kürzlich veröffentlichter Forschungsartikel. Obwohl gerade diese Art des Trackings große Risiken birgt, wird bisher wenig darüber gesprochen.

So unverwechselbar und einzigartig wie unsere Handschrift sind auch die Bewegungen, die wir auf unseren Touchscreens machen – das behauptet zumindest ein Forschungsteam der australischen Commonwealth Scientific and Industrial Research Organisation (CSIRO)¹. Ein im April veröffentlichter Artikel² zeigt auf, dass diese Bewegungsdaten so individuell sind, dass sie eine genaue Wiedererkennung von Usern und damit eine Form des Trackings ermöglichen: „[M]it unserer Methodologie können wir User mit einer Erfolgsrate von über 90 % re-identifizieren“.

Um herauszufinden, wie hoch der Informationsgehalt der individuellen Touch-Daten wirklich ist, wurde die Anwendung TouchTrack entwickelt, die jetzt auch in Googles PlayStore verfügbar³ ist. In die App wurden mehrere kleine Open-Source-Spiele eingebunden, die über typische Touchbewegungen funktionieren. Die so abgegriffenen Daten von insgesamt 89 Versuchspersonen wurden dann mathematisch auf ihre Eindeutigkeit (Uniqueness) hin untersucht.

Das Ergebnis: Schon wenige Samples einer einzelnen Bewegung (zum Beispiel das Wischen nach links über den Bildschirm) enthalten signifikante Informationen über den User. Je mehr Daten verschiedener Bewegungen vorliegen, desto besser können User wiedererkannt werden. Wischbewegungen und die Handschrift auf dem Bildschirm sind besonders eindeutig. Tippbewegungen oder das Schreiben auf einer Touch-Tastatur eher weniger.

Sind unsere Touch-Daten schutzbedürftig?

Daten über unsere sogenannten Touch-Events – also unsere individuelle Bedienung von Touchscreens über Bewegungen wie Wischen, Tippen, Zoomen oder die „Handschrift“ auf dem Display – sind über Programmierschnittstellen (APIs) einfach zugänglich. Diese Programmierschnittstellen sind vorprogrammierte Funktionen, die eine Verständigung zwischen Hard- und Software ermöglichen, also beispielsweise zwischen Anwendung und Touchscreen.

Dass die Informationen darüber, wo und wie wir unseren Touchscreen berühren, so einfach zugänglich sind, ist nicht verwunderlich. Ansonsten könnten wir nicht mit unseren Apps auf Smartphones oder Tablets interagieren. Jedoch erlauben einige

APIs auch das Abgreifen sehr spezifischer Details, bei denen es fragwürdig ist, ob eine App nicht auch ohne diese Informationen gut funktionieren könnte.

Die Forschungsergebnisse sind gerade deshalb so interessant, weil Touch-Daten so einfach abgreifbar sind und im öffentlichen Diskurs um Tracking und Privacy bisher wenig beachtet werden. Die Forscher weisen in ihrem Artikel auf eine Reihe von Besonderheiten und Risiken dieser Daten und des auf ihnen basierenden Trackings hin (eigene Übersetzung):

Im Vergleich zu „üblichen“ Tracking-Mechanismen, z. B. basierend auf Cookies, Browser-Fingerprints, Browser-User-Agents, Log-Ins und IP-Adressen, gibt es mehrere Faktoren, die das Tracking basierend auf Touch-Informationen potenziell riskanter machen. Während die anderen Mechanismen virtuelle Identitäten wie Online-Profile tracken, birgt „touch-based tracking“ das Potenzial, die eigentliche (physische) Person am Gerät zu tracken und zu identifizieren. Es kann mehrere User, die das gleiche Gerät verwenden, tracken und unterscheiden. Weiterhin erlaubt es das kontinuierliche Tracking von Usern und führt zum „cross-device tracking“, durch das ein User potenziell über mehrere mobile Geräte verfolgt werden kann.

Hassan Jameel Asghar stellte die Arbeit kürzlich im Rahmen eines Vortrags auf dem diesjährigen Privacy Enhancing Technologies Symposium⁴ vor.

Quelle: <https://netzpolitik.org/2018/wischnen-tippen-zoomen-forscher-tracken-anhand-von-touch-gesten/>

Anmerkungen

- <https://www.csiro.au/>
- <https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf>
- <https://play.google.com/store/apps/details?id=com.csiro.data61.touchtrack&hl=de>
- <https://petsymposium.org/> (ab 2:45:00)
- <https://netzpolitik.org/author/wiebke-denkena/>



Wiebke Denkena

Wiebke Denkena⁵ studiert Liberal Arts and Sciences und beschäftigt sich mit Themen wie Online-Überwachung, Künstlicher Intelligenz oder Online-Dating – gerne aus kulturwissenschaftlicher Perspektive. Davor hat sie einen Bachelor in Geomatik gemacht. Sie unterstützt das Team von netzpolitik.org von August bis Oktober 2018 als Praktikantin.