Handout Recherchetag 25

Mit Werbedaten Handys tracken – und sich selbst davor schützen

Keto Schumacher & Julian Schmidli, SRF Data

Ein Grossteil des Internets, wie wir es heute kennen, ist verwanzt mit Werbetrackern. Kleine Spione, die uns Nutzerinnen und Nutzer ausspähen und notieren, was wir gerade tun: Was wir suchen, wer wir sind – und oft auch: wo wir uns gerade befinden. Diese Daten von Millionen von Schweizerinnen und Schweizern werden auf Werbemarktplätzen gehandelt – und auf Schattenmarktplätzen verkauft. In einer jahrelangen Recherche und einer Serie von Berichten u.a. für Rundschau, 10vor10, SRF.ch und die SRF-Podcast-Serie «Die Cookiefalle» hat SRF Data aufgedeckt, welches Missbrauchspotenzial in diesen Daten steckt – und welche Gefahr damit auch für Journalistinnen und Journalisten. Hier ein paar Ratschläge, wer sich mit dem Thema und solchen Daten befassen will.

Kenne den Rechtsrahmen
Das Paradox liegt auf der Hand: Die Nutzung von solchen Nutzerdaten zu Werbezwecken und Profiling kann legal sein. Werden sie aber für andere Zwecke – bspw. journalistische Zwecke – genutzt, betritt man schnell eine juristische Grauzone, die sehr gefährlich werden kann. Solche Daten lassen Rückschlüsse zu, die in die Privat- und teilweise Intimsphäre von Personen eindringen. Dazu haben die wenigsten eingewilligt, als sie beim Cookie-Banner «alles akzeptieren» klickten. Unsere Rechtfertigung: Wir berichten über die Gefahr die-ser Daten, können also ein höheres öffentliches Interesse vorweisen. Ausserdem haben wir gesonderte Massnahmen ergriffen um die Daten, die sich in unserem Besitz befinden, ausserordentlich gut und sicher aufzubewahren. Niemand ausser wir hat Zugriff auf diese Daten – und nach Ende der Berichterstattung werden sie gelöscht.

Halte dich an klare ethische Richtlinien Wir sind im Besitz von Standortdaten von 1.3 Millionen Geräten in der Schweiz sowie mehr als 50 Mio. Geräten weltweit – teilweise mit Bewegungsprofilen von mehreren Wochen. Das bedeutet: Die Wahrscheinlichkeit ist sehr gross, dass sich darin auch Geräte von Freunden, Familie, Kolleg:innen von uns (und euch) befinden – und wir so sehr einfach auf Informationen stossen könnten, die nicht für uns bestimmt sind. Wir haben uns deshalb sehr bewusst einen ethischen Kodex aufgestellt, welche Geräte wir uns genauer anschauen und deren Besitzer identifizieren wollen – und welche nicht.

Misstraue den Daten(händlern) Die Werbebranche redet sich selbst ein, dass dieses System der Werbedaten und personalisierten Werbung eine Art «heiliger Gral» mit magischen Kräften ist. Doch wer hinter dieses System sieht, merkt schnell: Viele der Informationen sind längst nicht so gut und genau, wie sie den Anschein machen. So findet man in diesen Werbedaten auch

maz – Die Schweizer Journalistenschule, Murbacherstrasse 3, CH–6003 Luzern, +41 41 226 33 33, office@maz.ch, maz.ch

recycelte, gefälschte oder manipulierte Datenpunkte. Oft sind Standorte nur von der IP-Adresse abgeleitet und dementsprechend ungenau. Manchmal stimmen die Zeitstempel nicht oder sind um Jahre verschoben. Es braucht viel Umsicht und Wissen, um Aussagen aus solchen Daten machen zu können.

Nutze Technologie clever
Wer Werbedaten in die Hände bekommt, hat es schnell mit Millionen oder Milliarden von Datenpunkten zu tun. Das heisst auch: Ohne Programmieren geht hier nichts mehr. Wir haben mit Python und Dask gearbeitet, um die Daten (parallel) zu prozessieren. Und die Tools wktmap.com und Overpass Turbo haben geholfen, die richtigen Fragen an die Daten zu stellen. Zum Beispiel: Welche Geräte senden aus militärischen Ein-richtungen?

Schütze dich vor Tracking
Es gibt im Netz viele Ressourcen dazu, wie man sich als Journalist:in sicher im Internet bewegt. Auf srf.ch/data haben wir eine simple grafische Anleitung für alle publiziert. Die Digitale Gesellschaft Schweiz hat einen Ratgeber (digitale-gesellschaft.ch/ratgeber) zur digitalen Selbstverteidigung. Die Electronic Frontier Foundation hat Tool Guides (ssd.eff.org). Grundsätzlich empfehlen können wir: Ad-Blocker (U Block Origin, Privacy Badger), Datensparsame Browser wie Brave oder Mullvad, VPN mit Trackerblockern nutzen (Mullvad o.a.; keine Gratis-VPN!), möglichst nirgends eingeloggt sein, keine Google Produkte nutzen (stattdessen bspw. DuckDuckGo als Suchmaschine, Protonmail als Mailprovider usw.), trackingfreie OS fürs Handy (GrapheneOS). Vor allem: Standort und Werbetracking auf dem Handy ausschalten.