"Ich habe doch nichts zu verbergen."

Was Google und Co. über uns wissen

Info-Dokument des Informatik-Kurses J2 2018/19

26. Februar 2019

Inhaltsverzeichnis

1 Einleitung

Die meisten von uns haben heutzutage ein Smartphone. Und ähnlich viele verwenden vermutlich Google als Suchmaschine. Nicht umsonst steht das Wort googeln im Duden. Es ist schließlich äußert praktisch, eine Vielzahl an verfügbaren Informationen überall und jederzeit abrufen zu können. Auch wenn man wohl nicht sagen kann, das ganze Internet sei vollumfänglich gut, so sind wir uns wohl doch einig, dass zumindest dieser Teil des Internets nur Vorteile für uns hat - oder vielleicht doch nicht? Denn auch Google ist ein Unternehmen, das Gewinn machen möchte. Doch mit was könnte eine Suchmaschine Geld verdienen? Natürlich, man könnte Werbung schalten und Website-Betreiber für bessere Platzierungen bezahlen lassen. Doch heutzutage ist eine weitere Geschäftspraktik viel präsenter - der Datenverkauf. Denn Google hat Milliarden, wenn nicht Billionen an Suchanfragen von uns. Und diese Daten sind den richtigen Leuten sehr viel Wert. Doch was wissen Google und Facebook wirklich über uns und was genau machen sie mit diesen Daten? Mit dieser Frage haben wir uns beschäftigt und unsere Ergebnisse nachfolgend zusammengetragen.

2 Wer sammelt eigentlich meine Daten?

Daten über den Nutzer sammelt eigentlich fast jede App und Website. Das ist auch per se nicht schlimm, schließlich wollen die Anbieter ihre Services verbessern und sind daher darauf angewiesen zu wissen, wie ihre Services genutzt werden. Gefährlich wird es erst dann, wenn eine Firma sehr viele Daten über einen Nutzer bekommt. Und solche Firmen gibt es. Hier genannt seien Google, Facebook, Amazon und Microsoft. Und das sind nur die größten und bekanntesten der Datensammler.

3 Warum werden meine Daten gesammelt?

Von Seiten der Firmen heißt es meistens "Wir sammeln Daten zur Verbesserung unserer Dienste". Dies mag oftmals auch durchaus der Fall sein. Auch werden mit den vielen Daten zum Beispiel neuronale Netze trainiert, was letztendlich auch dem Nutzer zugutekommt. Doch natürlich hat das Sammeln von Daten für Firmen wie Google und Facebook vor allem einen Grund: Geld verdienen. Beide Firmen sind mit einem recht hohen Wert an der Börse notiert und beide Firmen verdienen den Großteil ihres Gewinns mit den Daten ihrer Nutzer. Daten werden in diesem Fall weiterverkauft,

um zum Beispiel personalisierte Werbung anzuzeigen, welche deutlich mehr Wert ist als ünpersönliche"Werbung.

4 Direkte Datensammlung

4.1 Google MyActivity

Nutzt man Google als Suchmaschine und ist dabei angemeldet oder hat man ein Android-Gerät, so zeichnet Google eventuell unter Google MyActivity den Suchverlauf und Statistiken zur Nutzung des Android-Gerätes auf. Zu den gesammelten Daten gehören zum Beispiel auch Mikrofon- und Standortdaten. Auch weiß Google, wann welche App genutzt wird. Die Kategorien können alle auf der Website "pausiert"werden, was jedoch nicht zwangsläufig bedeuten muss, dass Google aufhört, den Nutzer zu bespitzeln, da zum Beispiel bei Nutzung der Google-Services immer Standortdaten erhoben werden, auch wenn ein aktiver Widerspruch des Nutzers dagegen vorliegt.

4.2 Microsoft Activity

Nutzt man einen Windows-Rechner mit Windows 10 und hat sein Benutzerkonto mit seinem Microsoft-Konto verknüpft, so zeichnet Microsoft, ähnlich wie Google, eventuell Cortana-Suchanfragen, App-Verläufe und Browserdaten auf. Die gesammelten Daten sind hier einsehbar.

4.3 Amazon

Auch Amazon sammelt natürlich Daten über einen,wenn man zum Beispiel nach Produkten sucht oder dort Einkauft. Den Verlauf der angeschauten und gekauften Produkte kann man auf seinem Amazon-Profil einsehen. Amazon sammelt beim Verwenden der App oder der Website noch wesentlich detailliertere Daten wie "Klick-Verläufe", diese Daten bekommt man jedoch erst, wenn man sich speziell mit dieser Forderung an den Support wendet.

4.4 Facebook

Und selbstverständlich sammelt auch Facebook Daten über die Nutzung seiner Services wie zum Beispiel angeschaute und gelikte Posts. Natürlich wird auch gespeichert, mit wem man befreundet ist oder über den Messenger oder WhatsApp chattet. Die von Facebook gespeicherten Daten kann man über den Support anfragen, wobei man den vollständigen Datensatz vermutlich erst nach einigem Nachhaken bekommt.

5 Indirekte Datensammlung mit Trackern

5.1 Was sind Tracker eigentlich?

Tracker (von engl. to track = (nach-)verfolgen) sind kleine Programme, die in Websites, Apps oder Werbung eingebunden werden. Wird die entsprechende App oder Website nun von einer Person aufgerufen, sendet der Tracker Informationen wie IP-Adresse, Standort, Gerätedaten, Uhrzeit etc. an den Server der Tracking-Firma.

5.2 Wozu dienen Tracker?

Die Daten, die Firmen wie Google oder Facebook über diese Tracker bekommen, nutzen sie, um zum Beispiel Nutzungsstatistiken zu bekommen oder dem Nutzer personalisierte Werbung anzuzeigen.

5.3 Wo gibt es überall Tracker?

5.3.1 Websites

Auf Websites wie der des Spiegel oder der Bild-Zeitung sind Tracker hinterlegt. Diese werden aktiviert, sobald man die Website aufruft.

5.3.2 Werbung

Auch in Werbung, die auf Websites angezeigt wird, befinden sich Tracker. Diese dienen hauptsächlich dazu, dem Nutzer personalisierte Werbung anzuzeigen.

5.3.3 Apps

Zudem sind in vielen Android- wie auch iOS-Apps Tracker integriert. Diese senden oftmals schon beim Starten der App Daten an den jeweiligen Anbieter. Auch diese Tracker dienen der Beschaffung von Nutzungsstatistiken und der personalisierten Werbung.

5.4 Wie funktionieren diese Tracker genau?

Wie bereits eingangs erwähnt sind Tracker kleine Programme, die z.B. in eine App integriert sind. Wird die App nun gestartet, so wird auch der Tracker gestartet und sendet Daten an den Anbieter des Trackers. Je nach Ausführung des Trackers werden dabei nicht nur Daten wie die IP-Adresse etc. an das Unternehmen gesendet, sondern unter Umständen auch sensible Nutzungsdaten. So sendet zum Beispiel die App Kayak, mit der man die Preise verschiedener Airlines vergleichen kann, Daten wie das Datum der Reise, den Abflug- und Ankunftsflughafen, die Anzahl der Angefragten Tickets und die gebuchte Klasse, z.B. Economy oder Business, an Facebook. Andere Apps senden sogar einzelne User-Interaktionen wie aufgerufene Menüs an Facebook.

5.5 Was ist daran jetzt so gefährlich?

Diese Daten allein wären alle nicht so schlimm, solang man sie nicht mit einer bestimmten Person verknüpfen kann. Sie könnten also zum Beispiel zu Analysezwecken verwendet werden, ohne dass wirklich Rückschlüsse auf das Gesamtverhalten einzelner Personen gezogen werden können. Problematisch wird es jedoch, wenn Rückschlüsse gezogen werden und die Daten verschiedener Apps einer einzigen Person zugeordnet werden können. Und genau dies ist durch App- und Websitetracker relativ problemlos möglich. Nehmen wir als Beispiel eine Testperson mit einem Android-Gerät. Wird das Gerät eingerichtet, so wird eine einzigartige Google-Advertising-ID erstellt. Diese kann von den Trackern abgerufen werden und wird von ausnahmslos jedem Tracker mitgesendet. Durch diese ID können jedoch ohne größeren Aufwand die Aktivitäten verschiedener Apps einer Person zugeordnet werden, wodurch Firmen wie Google und Facebook, deren Tracker in der Mehrheit der Android-Apps vorhanden sind, ein relativ detailiertes Profil der Person bekommen. Sie wissen unter Umständen, wann welche App benutzt wird. Durch Apps wie Kayak können sie herausfinden, wann die Person einen Urlaub plant. Durch Shopping-Apps und Suchmaschinen können die Interessen der Person herausgefunden werden. Und selbst wenn das Unternehmen nur weiß, wann welche App geöffnet und geschlossen wird, kann ein relativ genaues Profil des Tagesablaufes einer Person erstellt werden.

6 Wie kann ich mich schützen?

Jetzt stellt sich einem vermutlich die Frage, wie man sich dagegen am besten schützen kann. Die naheliegenste Antwort darauf ist gleichermaßen einfach wie naiv: Man nutzt Google und Facebook einfach nicht mehr. Ein Schritt in die richtige Richtung, doch leider bei weitem nicht ausreichend. Wie bereits erwähnt verfolgen Google und Co. uns auch über die eigenen Services hinaus mit Trackern. Und durch die Google-Advertising-ID erfolgt diese Verfolgung weiterhin personenbezogen. Google wird also weiterhin wissen, was ich mache und dies mit meiner Person verknüpfen, auch wenn ich eine andere Suchmaschine verwende. Doch die Situation ist nicht ausweglos. Eine Möglichkeit, zumindest sicher im Internet surfen zu können, besteht zum Beispiel darin, Tracker und Werbung zu blockieren.

6.1 Sicher im Netz unterwegs

Um Tracker und Werbung im Internet zu blockieren, gibt es mehrere Möglichkeiten. Wir können an dieser Stelle nicht alle nennen, daher hier ein paar Programme, die wir nutzen:

6.1.1 Avira Browser Safety

Vom Antivirensoftware-Hersteller Avira gibt es hier ein nützliches Browser-Addon, welches Werbung und Tracker zuverlässig blockiert. Es zeigt zudem an, wie viele Tracker

auf der aktuellen Website blockiert wurden. Das Addon ist für die gängisten Browser verfügbar.

6.1.2 Firefox Lightbeam

Das Browser-Addon des Firefox-Herstellers Mozilla bietet nicht nur Tracking-Protection, sondern zeigt auch noch sehr schön an, welche Tracker auf der Website liegen. Jedoch ist dieses Addon nur für Firefox verfügbar. Es wird hier zum Download angeboten.

6.1.3 Brave-Browser

Das Team hinter Brave hat es sich zur Aufgabe gemacht, das Internet besser zu machen. Der Browser blockiert nicht nur Werbung und Tracker, wodurch unter anderem auch Websites schneller geladen werden, sondern schaltet selber eigene Werbung ohne Tracker. Teile des Gewinns werden dann an die Website weitergeleitet, denn schließlich müssen die Website-Anbieter auch von irgendetwas leben. Den Brave-Browser kann man sich hier herunterladen.

6.2 Werbe- und Tracking-Blocker

Auch mit Tools wie Adblock Plus kann man sich vor Trackern im Netz schützen. Diese Tools sind oftmals kostenlos und tun das, was sie sollen.

6.3 Beispiel Google: Einstellungsmöglichkeiten

Es ist zwar unwahrscheinlich, dass eine Änderung der Einstellungen wirklich Einfluss auf das Ausmaß der gesammelten Daten hat, der Vollständigkeit halber seien die von Google gegebenen Einstellungsmöglichkeiten aber nachfolgend genannt: In den Datenschutz-Einstellungen von Google kann man die Daten-Dienste "pausieren". Ob Google dann tatsächlich keine Daten mehr sammelt oder weitersammelt und dem Nutzer dies einfach nicht anzeigt ist jedoch nicht bekannt. Allzu gutgläubig sollte man dabei jedoch nicht sein, Google verdient sein Geld schließlich fast ausschließlich mit Daten.

6.4 Sicher am Smartphone

Leider ist es nicht ganz so einfach, Tracker in Smartphone-Apps zu blockieren. Da sie ein fester Teil der App sind, bleibt einem nur die Möglichkeit, die App nicht zu nutzen. Oftmals weiß man jedoch nicht mal, ob in einer App Tracker enthalten sind. Auf der Website haystack.mobi sind die Tracker einiger Android-Apps dargestellt. Jedoch ist diese Datenbank bei weitem nicht vollständig und für iOS gibt es gar keine solche Datenbank. Auch weisen nicht alle App-Entwickler in ihrer Datenschutzerklärung auf den Einsatz von Trackern in ihren Apps hin, wodurch es tatsächlich fast unmöglich ist, festzustellen, welche Apps sicher sind.

6.5 Sicher am PC

Nutzt man Windows 10, so bietet einem Microsoft in der Home-Version bezüglich der Diagnosedaten nur zwei Einstellungsmöglichkeiten: Ëinfachünd "Vollständig". Man kann das weitergeben der Diagnosedaten an Microsoft also standardmäßig gar nicht komplett abschalten. Dies funktioniert also nur über Umwege. Ein paar der Möglichkeiten sind nachfolgend aufgelistet:

- Avira-PrivacyPal installieren: Mit der (kostenpflichtigen) Software kann der Datenhunger von Windows recht einfach unterdrückt werden.
- Diagnosedaten einsehen und löschen: Wie in der Präsentation des Info-Abends erklärt, kann man die gesammelten Daten einsehen und einen Löschantrag stellen. Dies macht man unter Einstellungen - Datenschutz - Diagnose und Feedback - "Diagnosedaten-Viewer"bzw weiter unten "Löschen"
- Event Tracing beenden [ACHTUNG: Nur für erfahrene Benutzer!]: Über die Computerverwaltung kann man den Dienst, der für die Telemetrie verantwortlich ist, beenden. Bei Änderungen in der Computerverwaltung ist allerdings höchste Vorsicht geboten, da die Änderung einer falschen Datei zur Zerstörung des Betriebssystems führen kann. Die gespeicherten Daten sind dann zwar noch abrufbar, allerdings sollte man dafür erfahren im Umgang mit Linux Live sein. Daher ist diese Vorgehensweise wie bereits erwähnt nur erfahrenen Nutzern zu empfehlen. Um den Dienst abzuschalten, macht man einen Rechtsklick auf das Windowslogo und geht dann in Computerverwaltung - Dienste und Anwendungen - Dienste - "Benutzererfahrung und Telemetrie im verbundenen Modus", klickt auf "Beendenünd wählt bei Starttyp "Deaktiviertäus. Diese Einstellung muss nach jedem Funktions-Update wieder vorgenommen werden, da Windows bei einem Funktions-Update die Werte wieder zurücksetzt.

6.6 Allgemein

Seit der EU-DSGVO (Datenschutzgrundverordnung) hat jeder EU-Bürger das Recht darauf, bei allen Websites und Service-Anbietern alle zu seiner Person gespeicherten Daten anzufragen. Von diesem Recht sollte man auf jeden Fall Gebrauch machen. Auch wenn man mit den eigentlichen Daten nicht viel anfangen kann, ist es doch ein Statement an den Anbieter, dass man Wert auf seine Daten und den Datenschutz legt. Die entsprechende Service-Seite zur Anfrage der Daten ist oftmals etwas versteckt und nicht selten bekommt man den vollständigen Datensatz auch erst, nachdem man sich persönlich an den Support wendet, doch trotzdem sollte man sich die Mühe machen. Es kann ja auch mal ganz interessant sein zu sehen, was z.B. Amazon von einem weiß.

7 Disclaimer

Alle Angaben im Dokument sind ohne Gewähr. Zur genannten Avira-Software gibt es auch entsprechende Alternativen von anderen Herstellern, der Einfachheit halber wurde hier aber jeweils nur die Avira-Lösung genannt. Das Dokument wurde erstellt von Patrick Müller (mueller.patrick@protonmail.com) mit Informationen, die vom Informatik-Kurs J2 2018/19 gesammelt wurden. Das Dokument darf nur in voller Länge und speziell mit diesem Absatz verbreitet werden.

P.S.: Datenschutzbestimmungen:
Es erfolgt kein Verkauf von Daten an Dritte. Die Daten werden für interne Zwecke wie zum Beispiel das Erstellen von Statistiken verwendet. Vertrauliche Daten werden entsprechend behandelt. Erfolgte ein Antrag auf Vernichtung der Daten, so ist dieser zum gewünschten Zeitpunkt ausgeführt worden. Eine Einsicht in die von Ihnen erfassten Daten kann per Mail an oben genannte Adresse beantragt werden und wird zum nächstmöglichen Zeitpunkt bearbeitet. Selbiges gilt für Anträge auf Löschung der Daten.