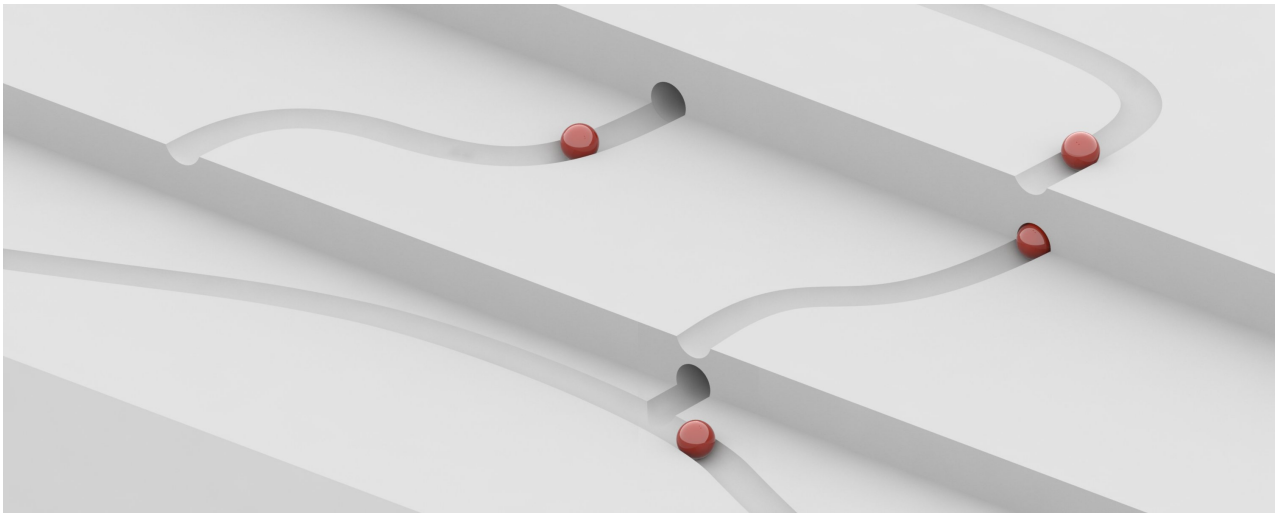

INTERNET & WEB

Privatsphäre im Internet: Wie wir unbewusst sensible Daten preisgeben

Im digitalen Alltag ist die Nutzung eines breiten Spektrums an Online-Diensten und –Anwendungen zur Normalität geworden. Das Zeitalter des „Internet der Dinge" beschert den Benutzern eine Fülle von physischen Geräten, die Daten über das Internet abrufen und austauschen. Diese Geräte wie Computer, Smartphone, Smart-TV oder Smart-Watch können im Internet surfen, Online-Dienste nutzen, miteinander kommunizieren sowie persönliche Informationen und Aktivitäten sammeln. Durch diese Vernetzung von Geräten und den Datenaustausch über verschiedene Web-Dienste hinterlassen die Benutzer aber auch einen großen digitalen Fußabdruck[1].

Hierbei liefern Nutzer unbewusst viele persönliche Daten aus, allein schon durch das Aufrufen von Webseiten. Dies umfasst nicht nur die Information, welche Webseiten besucht werden, sondern auch die Informationen über die genutzten physischen Geräte. Besonders profitieren davon Dritt-Parteien, die auf den Webseiten in Form von Werbung, als interaktives Angebot wie Facebook-Like-Button oder versteckt eingebunden sind[2].

Mit der Themen-Analyse der besuchten Webseiten werden dann die personenbezogenen Interessen gespeichert. Zudem werden die Inhalte, die die Benutzer freiwillig in sozialen Netzwerken wie Facebook teilen,

ausgewertet und geben damit zusätzliche vertrauliche Informationen an die Online-Dienste weiter.

Verbinden die Dritt-Parteien all diese Daten mit weiteren Informationen wie beispielsweise Facebook-Likes[3], dem Einkaufsverhalten[4], mobilen Ortungsinformationen oder der genutzten physischer Geräte[5], können eine Vielzahl an sensiblen privaten Daten gewonnen werden[6]. Dazu gehören persönliche Interessen oder Probleme der Nutzer, die sich beispielsweise aus Suchanfragen[7] ergeben, konkrete Profilinformationen wie Name und Adresse aus einer Bestellung, politische oder religiöse Ansichten sowie der finanzielle und gesundheitliche Status[8].

Das Risiko für die Benutzer leitet sich beispielsweise ab, wenn Unternehmen diese personenbezogenen Daten zum Nachteil des Benutzers ausnutzen und individuelle Preise sowie Angebote erstellen. Reale Beispiele sind einerseits die Ermittlung des Finanzstatus von Kunden[9], der individuell erstellt wird und sich aus dem geografischen Standort/Wohnort des Nutzers ergibt (berechnet aus der verwendeten IP-Adresse) sowie der Zusammenstellung der Einkäufe.

Andererseits vergibt ein Versicherungsunternehmen personalisierte Krankenversicherungen[10] [11] anhand der Online-Abschätzung des Risikopotenzials des Kunden. Dieses wird berechnet, indem die besuchten Webseiten ausgewertet werden und eine Evaluation des Risikopotenzials aus den Interessen oder Sportaktivitäten der Kunden erschlossen wird.

Dieser Verlust der Anonymität führt auch in weiteren Fällen zur Preisdiskriminierung, wie beispielsweise bei einem erhöhten Preis für Flugtickets[12], nur weil der Benutzer ein teures Marken Smartphone zur Buchung nutzt und die Buchung aus einem reichen Wohnviertel durchführt.

Dieses Sammeln von Benutzerinformationen (auch Web-Tracking genannt) ist ein reales Problem und wird auf nahezu jeder Webseite eingesetzt, um das Nutzerverhalten zu analysieren[13]. Die größten Tracking-Unternehmen wie Google/doubleclick und Facebook können den Benutzer so auf über 90% der meistbesuchten Webseiten in Deutschland verfolgen[14]. Dabei sind meistens 20-70 verschiedene Tracking-Dienste auf diesen Webseiten eingebunden, um Informationen zum Benutzerverhalten zu sammeln.

Wie Forschungsergebnisse beweisen, sind diese Tracking-Unternehmen in der Lage, einen Benutzer über das Web hinweg zu identifizieren[15], mit dem Ziel, personenbezogene Werbung zu platzieren und so die Verkaufszahlen zu steigern.

Diese Benutzer-Verfolgung und Identifizierung mit dem Sammeln detaillierter Benutzerdaten ist wertvoll und rentabel. Insbesondere wenn die Daten mit realen Identitäten wie Namen, Adresse und anderen persönlichen Informationen verknüpft werden können. Die damit verbundenen Bedrohungen und negativen Auswirkungen für Benutzer – wie die vorgestellte Preisdiskriminierung – sind vielseitig, so dass wir kaum alle zukünftigen Auswirkungen abschätzen können.

Welche konkreten Tracking-Methoden dabei zum Einsatz kommen, welche weiteren Risiken dabei entstehen und mit welchen einfachen Mitteln sich Benutzer dagegen schützen können, erfahren Sie in den Folgeartikeln.

---

[1] https://www.pnas.org/content/110/15/5802

[2] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[3] https://www.ndss-symposium.org/wp-content/uploads/2017/09/P02_1.pdf

[4] http://www.capitolhilltop.org/extra/papers/Langsner_InternetPrivacySecurity.pdf

[5] https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf

[6] https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner

[7] https://www.freehaven.net/anonbib/cache/search-engine-pets2017.pdf

[8] https://www.wsj.com/articles/SB10001424052748703977004575393173432219064

[9] https://money.cnn.com/2013/08/26/technology/social/facebook-credit-sc

ore/index.html

[10] https://www.petsymposium.org/2014/papers/Vissers.pdf

[11] https://www.ncbi.nlm.nih.gov/pubmed/25895907

[12] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.352.3188

[13] https://www.springerprofessional.de/reducing-user-tracking-through-automatic-web-site-state-isolatio/2335330

[14] https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf

[15] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.587.648

Veröffentlicht am Montag, 15.04.2019

AUTOR
Martin Stopczynski

Vielen Dank für Ihr Interesse.
Weitere Blog Beiträge finden Sie unter adiccon.de