

Big Data wird persönlich: Verhaltensgesteuerte Zielgruppenansprache

10. Übungsblatt

Hatten Sie jemals das Gefühl, jemand verfolgt Sie im Web und beobachtet jeden Ihrer Klicks? Fragen Sie sich auch, warum Sie direkt, nachdem Sie ein Auto, Kleid oder Kosmetikprodukt gesucht haben, entsprechende Anzeigen oder Pop-ups eingeblendet bekommen? Ja, Sie liegen richtig: Ihr Verhalten wird überwacht. Und das alles, um Ihnen beim Surfen im Web möglichst zielgenaue Anzeigen auf den Seiten einzublenden. Das ist die dunkle Seite von Big Data. Spezielle Websites und Unternehmen, deren Geschäftstätigkeit darin besteht, Internetnutzer im Auftrag von Werbetreibenden und Vermarktern zu identifizieren und zu überwachen, sammeln Daten über alle Ihre Schritte im Web. Google mit seinen mehr als 3,5 Mrd. Websuchen jeden Tag weiß mehr über Sie als Ihre Mutter. Viele der Tracking-Tools sammeln unglaublich persönliche Daten, wie Alter, Geschlecht, Rasse, Einkommen, Familienstand, gesundheitliche Probleme (anhand der Gesundheitsthemen, über die Sie sich informieren), angeschauter Fernsehsendungen und Filme, gelesene Magazine und Zeitungen sowie gekaufte Bücher. Triebfeder dieser aufwendigen Datenerhebung ist eine milliardenschwere OnlineWerbeindustrie (31 Mrd. USD). Facebook mit seiner umfangreichen Datensammlung über ungefähr 1 Milliarde Nutzer verfolgt die Schritte der Nutzer im Web über ihre Likes, sogar wenn diese sich ausloggen. Diese soziale Netzwerk-Site ist ein einziges riesiges Tracking-System, das sich genau merkt, was Sie mögen, was Ihre Freunde mögen und alles, was Sie auf Ihrer Pinnwand enthüllen (siehe Fallstudie am Ende des Kapitels). Googles soziales Netzwerk-Tool Plus weiß, mit wem Sie auf Gmail befreundet sind, welche Orte Sie bei Google Maps aufrufen und wie Sie Ihre Zeit auf den mehr als zwei Millionen Websites in Googles

Anzeigennetzwerk verbringen. Diese Daten werden von Google gesammelt, auch wenn Plus als soziales Netzwerk nur von wenigen genutzt wird. Tracking-Unternehmen behaupten, dass die von ihnen gesammelten Daten anonym sind. Die Praxis belegt allerdings das Gegenteil. Wissenschaftler haben bewiesen, dass sich mit nur wenigen Daten wie Alter, Geschlecht, Postleitzahl und Familienstand ganz leicht einzelne Personen identifizieren lassen. Darüber hinaus kombinieren Tracking-Unternehmen ihre Onlinedaten mit Daten, die sie von Offline-Firmen kaufen, die zum Beispiel in den USA die Einkäufe praktisch aller Amerikaner verfolgen und dabei die angegebenen Klarnamen und andere Identifikatoren abgreifen. Die

Verwendung echter Identitäten im Web nimmt in rasantem Tempo zu. Eine Untersuchung des Wall Street Journals von fast 1.000 Websites ergab, dass 75 % dieser Sites inzwischen Facebook- oder Twitter-Code in Form eines Like- oder eines Tweet-Buttons beinhalten. Solcher Code kann die Identität von Personen mit ihren Webbrowser-Aktivitäten in bisher nicht gekanntem Ausmaß verknüpfen und sogar die Seite feststellen, auf der ein Nutzer landet, selbst wenn der Button niemals angeklickt wurde. Eine andere Studie des Journals untersuchte ungefähr 70 populäre Websites, bei denen die Angabe von Login-Daten erforderlich ist. Ergebnis war, dass in ungefähr einem Viertel aller Fälle die Sites den richtigen Namen des Nutzers, seine E-Mail-Adresse oder andere persönliche Daten an Dritte weitergaben. Werbegiganten im Web wie Google, Microsoft und Yahoo! suchen alle nach Möglichkeiten, wie sie ihre riesigen Datenbestände zum Onlineverhalten der Nutzer zu Geld machen können. Während Suchmaschinen-Marketing zweifelsohne früher die effektivste Werbeform war, ist die nicht zielgerichtete Bannerwerbung sehr ineffizient, da sie bei jedem eingeblendet wird, unabhängig von seinen eigentlichen Interessen. Logischerweise können Unternehmen für diese Werbeform nicht viel Geld verlangen. Wenn sie jedoch die Onlinebewegungen von den über 245 Millionen Internetnutzern in den Vereinigten Staaten verfolgen, können sie sich ein ziemlich klares Bild von jedem einzelnen Nutzer machen und diese Informationen heranziehen, um nutzerspezifisch Anzeigen zu schalten, die für ihn von Interesse sein könnten. Das würde den Marketingprozess wesentlich effizienter machen und wäre für alle Beteiligten profitabler. Sogar wenn Sie Ihr Handy nutzen, um auf das Internet zuzugreifen, sich bei Ihrem Facebook-Account anzumelden, Twitter-Feeds abzurufen, Videos zu schauen und Musik zu hören, werden Sie ständig überwacht. Das mobile Web arbeitet hart daran, alles über Ihre Aufenthaltsorte, Gewohnheiten und Freunde in Erfahrung zu bringen – und alles in der Hoffnung, Ihnen noch mehr Produkte und Dienstleistungen zu verkaufen. Neue Technologien auf Smartphones können Ihren Aufenthaltsort auf wenige Meter genau orten. Die routinemäßige Nutzung Ihres Smartphones erlaubt es sogar, Bewegungsprofile von Ihnen zu erstellen, die dann an die Unternehmensdatenbanken weitergeleitet, dort gespeichert und analysiert werden, um sie an Werbetreibende zu verkaufen. Die meisten der bekanntesten Apps ermitteln Ihren Aufenthaltsort und geben die Daten weiter. Polizeibehörden haben zum Beispiel ein großes Interesse an den Aufenthaltsorten von Kriminellen und Verdächtigen. Außerdem gibt es natürlich viele Fälle, in denen Sie automatisch oder auf Aufforderung mitteilen wollen, wo Sie sich gerade befinden. Wenn Sie zum Beispiel verletzt sind, wäre es schön, wenn Ihr Handy den zuständigen Notdiensten Ihren Standort mitteilt, oder Sie sind in einem Restaurant und wollen Ihre Freunde darüber informieren, wo Sie sich aufhalten und was Sie gerade machen. Doch was ist, wenn Sie nicht wollen, dass jemand weiß, wo Sie sich gerade befinden, und schon gar nicht Werbetreibende und Vermarkter?

Standortdaten, die über Handys erhoben wurden, sind sehr wertvoll, da Werbefirmen Ihnen ganz gezielt in Abhängigkeit von Ihrem Standort Werbung, Coupons und Sonderangebote unterbreiten können. Diese Technologie ist die Grundlage für viele standortbasierte Dienste, zu denen auch Smartphone-Karten, Shopping-Apps und soziale Apps gehören, die es Ihnen ermöglichen, Ihren Freunden mitzuteilen, wo Sie sich aufhalten und was Sie gerade machen. Die Umsätze des globalen Markts der standortbasierten Dienste werden sich 2015 laut Gartner auf 10,3 Milliarden US-Dollar belaufen. Sowohl Apple mit seinem iPhone als

auch Google mit seinen Android-basierten Smartphones erheben Standortdaten ihrer Nutzer und bauen große Datenbanken auf, die Ihren Aufenthaltsort ziemlich genau lokalisieren können. Werbefirmen zahlen Apple und Google für diese Informationen und die Schaltung ihrer mobilen Anzeigen, wodurch sie zu einer immer wichtigeren Einnahmequelle werden. 2012 verdiente Google mit mobilen Anzeigen 2,2 Milliarden US-Dollar. Smartphone-Apps, die standortbasierte Dienste anbieten, sind aufgrund der GPS-Fähigkeit des Smartphones ebenfalls Quelle persönlicher Standortdaten. Gehen Sie ruhig davon aus, dass mit zunehmender Genauigkeit der verhaltensgesteuerten Zielgruppenansprache (behavioral targeting) Ihre Bewegungen in Zukunft noch viel stärker unter die Lupe genommen werden. Es wird bereits Software entwickelt, die Werbetreibende dabei hilft, die Nutzer über mehrere Geräte hinweg zu verfolgen und dabei bildschirmübergreifende Identitäten zu erstellen. Das bedeutet, dass Unternehmen demnächst auf Ihrem Handy Anzeigen einblenden, auf der Basis von Ihren Interessen, die Sie beim Surfen im Web auf Ihrem PC bekundet haben.

Quellen: Claire Cain Miller, „The Plus in Google Plus? It’s Mostly for Google“, New York Times, 14. Februar 2014; Elizabeth Dwoskin, „Internet Users Tap Tech Tools That Protect Them From Prying Eyes“, The Wall Street Journal, 23. März 2014; Claire Cain Miller und Somni Sengupta „Selling Secrets Of Phone Users to Advertisers“, The New York Times, 5. Oktober 2013; Natasha Singer, „Their Apps Track You, Will Congress Track Them?“, The New York Times, 5. Januar 2013; Spencer E. Ante, „Online Ads Can Now Follow Your Home“,

Quelle der Fallstudie: **laudon_wirtschaftsinformatik_2015**

Aufgabe 1

Warum ist die verhaltensgesteuerte Zielgruppenansprache (behavioral tracking) heutzutage ein so großes ethisches Problem? Identifizieren Sie die verschiedenen Interessengruppen, die dafür und dagegen sind.

Lösung

- Online- und Bewegungsprofile können Nutzer genau identifizieren
- Eingriff in die Privatsphäre
- Daten lassen vielfältige Rückschlüsse zu, z. B. politische Einstellung
- Polizei und Rettungskräfte haben Interesse an standortbasierte Daten, um Kriminelle besser zu verfolgen oder einen medizinischen Notfall schneller zu erreichen
- Aufenthaltsort kann falsche Personen erreichen

Aufgabe 2

Inwiefern profitieren Unternehmen von der verhaltensgesteuerten Zielgruppenansprache? Ergeben sich auch Vorteile für die einzelnen Nutzer? Erläutern Sie Ihre Antwort.

Lösung

- gezielte Ansprache ist für Unternehmen erfolgversprechender
- Nischenprodukte können so besser vermarktet werden
- Nutzer bekommt Werbung für seine Interessen
- Werbung kann dann zur Entscheidungshilfe verwendet werden
- kostenfreie Nutzung Angebote von Websites oder Dienstleistern gegen Weitergabe der Daten

Aufgabe 3

Was würde passieren, wenn das Verhalten im Internet nicht überwacht würde?

Lösung

- Großteil der Werbung ist zielgruppenspezifisch
- Kunden würden unpassendere Werbung bekommen
- weniger Wirksamkeit, geringere Einnahmen
- Markt würde einbrechen