



Digitale Profilbildung und Gefahren für die Verbraucher

Zusammenfassung

Technische Universität München

Lehrstuhl für BWL - Marketing und Konsumforschung

Dieses Gutachten wurde im Auftrag des
Verbraucherzentrale Bundesverbandes e.V. erstellt.

Im November 2010

A. Klein, F. Leithold, C. Zell, J. Roosen

Inhaltsverzeichnis

Einleitung	3
1. Marketingziele der Nutzerdatenerfassung und der Verbraucherprofilbildung.....	4
2. Techniken zur Nutzerdatenerfassung	4
3. Data-Mining-Verfahren und Auswertung der erhobenen Daten	10
4. Risiken für den Verbraucher	10
5. Schutzmöglichkeiten des Verbrauchers im Internet.....	11
6. Auswirkungen der Profilbildung auf die Position des Verbrauchers	12
7. Schlussfolgerungen	13

Einleitung

Die Nutzung des Internets und seiner Inhalte hat in den vergangenen Jahren deutlich zugenommen. Neben der Kommunikation gewinnen auch der E-Commerce, Online-Services und Soziale Netzwerke zunehmend an Bedeutung. Als Konsequenz dieser Präsenz der Nutzer im Internet werden verstärkt personenbezogene und potenziell personenbeziehbare Daten gespeichert und verwendet. Durch Technologien zur Datenerhebung ergibt sich ein erhebliches Sicherheitsrisiko für den Schutz der Daten sowie die Privatsphäre der Nutzer. Die erhobenen Daten stellen jedoch für Unternehmen die Basis für die Erstellung von Nutzerprofilen und darauf aufbauende gezielte Marketingmaßnahmen für bestimmte Nutzergruppen dar. Das vorliegende Gutachten setzt sich daher mit Marketingzielen und der Entwicklung von Nutzerprofilen auseinander. Es werden alle gängigen Techniken zur Nutzerprofilerstellung im Internet sowie potenziell daraus resultierende Risiken für den Verbraucher und gezielte Schutzmöglichkeiten gegen diese Technologien aufgezeigt, denn jedes der beschriebenen Verfahren ermöglicht es, Daten unterschiedlicher Aktualität und verschiedenster Sensibilität in Erfahrung zu bringen.

Sowohl die Erfassung von Nutzerdaten im Internet als auch die daraus resultierende Profilerstellung bergen Nutzen, aber auch hohes Risikopotential in sich. Zum einen ist es möglich, den Besucher im Such- und Auswahlprozess gewünschter Informationen, Produkte und Dienstleistungen effektiv zu unterstützen. Dabei spielen vor allem Techniken der Personalisierung und des individualisierten Marketings eine große Rolle. Zum anderen besteht durch Aggregation personenbezogener Daten unterschiedlicher Quellen die Gefahr der unerlaubten Weitergabe der Daten an Dritte sowie der Entstehung vom Kunden nicht gewollter detaillierter Nutzerprofile.

In diesem Zusammenhang werden auch die derzeitige Transparenz der Nutzerdatenerfassung im Internet und Einwilligungsmöglichkeiten dargestellt. An vielen Stellen sind Geschäftsbedingungen und Datenschutzerklärungen übermäßig lang und schwer verständlich für den Verbraucher. Nach der Einholung der Nutzerzustimmung werden Daten unterschiedlichster Herkunft verwendet, um ein umfassendes Nutzerprofil zu erstellen.

Darauf aufbauend werden ebenfalls weitere Auswirkungen auf die Position des Verbrauchers am Markt berücksichtigt. Der Verbraucher sieht sich in diesem Zusammenhang mit einem zunehmenden Druck zur Datenpreisgabe im Internet konfrontiert, da er ansonsten am Marktgeschehen nicht teilnehmen kann. Durch die steigende, über den einzelnen Nutzer verfügbare Datenmenge ergeben sich sowohl informationstechnische, wie auch finanzielle Konsequenzen. Der Verbraucher steht deshalb unter anderem einem durch sein Nutzerprofil beeinflussten Angebot in informationeller und preislicher Hinsicht gegenüber.

Abschließend wird neben dem Aufklärungsbedarf gegenüber dem Verbraucher auch der Handlungsbedarf seitens der Wirtschaft und der Politik aufgezeigt. Es sollte Ziel des Verbraucherschutzes sein dem „mündigen“ Verbraucher durch Selbstinformation eine Nutzung von Internetdienstleistungen ohne die Verletzung seiner Privatsphäre zu

ermöglichen. Zusätzlich besteht die Notwendigkeit eines verständlicheren und transparenteren Umganges mit persönlichen Informationen bei den Unternehmen.

1. Marketingziele der Nutzerdatenerfassung und der Verbraucherprofilbildung

Für das Marketing lassen sich durch die Bildung von Verbraucherprofilen vielfältige Ziele erreichen. Für Unternehmen kann die Absatzförderung innerhalb spezifischer Marktsegmente oder für einzelne Kunden im Vordergrund stehen. Auch der Test von Preissetzung und Angebot ist möglich, um die Nachfragekurve, den kundenspezifischen Absatz für Produkte oder den Erfolg einer Webseite zu bestimmen. Die Profilbildung hat zum Ziel, so viel wie möglich über den Kunden in Erfahrung zu bringen, sein Verhalten einzuschätzen und dieses Wissen für betriebliche Zwecke nutzen zu können.

Das Nutzerprofil stellt eine abstrakte Repräsentation des einzelnen Nutzers durch bestimmte Attribute – Interessen, Vorlieben, getätigte Transaktionen – dar und wird auf Basis erfasster und mittels sogenannter Data-Mining-Verfahren analysierter Daten erstellt. Ein wichtiges Ziel der Profilbildung ist für viele Unternehmen die Neukundengewinnung im Hinblick auf den Kundenlebenszeitwert. So können potenzielle Neukunden mit besonderen Angeboten oder Gutscheinen angesprochen werden. Mit Aktionen wie Treue-Boni oder Rabatten kann im Marketing die Bindung von Bestandskunden gezielt gefördert werden. Auch kundenspezifische Umsatzraten und somit Wettbewerbspositionen einzelner Anbieter lassen sich ermitteln. Werbung, Zielseiten, Angebote und Preise können (zum Teil in Echtzeit) zusätzlich auf die speziellen Verhaltensweisen eines Nutzers ausgerichtet werden. Mithilfe sogenannter Targeting-Verfahren ist es möglich, den Nutzer beim Besuch der Seite wiederzuerkennen, das jeweilige Verhalten zu erfassen und Webinhalte und –services dementsprechend dynamisch den Nutzerpräferenzen anzupassen.

2. Techniken zur Nutzerdatenerfassung

Zur Erhebung der Nutzerdaten werden im Allgemeinen reaktive und nicht-reaktive Verfahren unterschieden. Reaktive oder auch explizit genannte Verfahren zur Erhebung von Nutzerdaten zeichnen sich durch die aktive Beteiligung des Nutzers am Datengenerierungsprozess aus. Der Nutzer gibt seine Daten freiwillig an, die dann vom Anbieter gespeichert werden. Die Nutzerdaten werden i. d. R. in Form von Fragebögen, Formularen oder Textfeldern erhoben, wie beispielsweise in Registrierungsprozessen, beim sogenannten Relevance Feedback^{1,2}, oder durch Drittanbieter wie Markt- oder Meinungsforschungsinstitute. Problematisch bei reaktiven Verfahren ist, dass z. B. im E-Commerce die Erstellung eines Profils für den Nutzer obligatorisch ist und innerhalb des Registrierungsprozesses demografische Daten,

¹ Im Relevance-Feedback bewertet der Nutzer Nützlichkeit, Relevanz oder Gefallen von Websites oder bspw. den Treffern einer Suchanfrage

² Beispiele hierfür sind Portale wie ePinions, NetFlix oder Ciao

Adressdaten und Altersangaben meist Pflichteingabefelder sind. Im eigenen Interesse sieht sich der Nutzer mit der Notwendigkeit konfrontiert, wahrheitsgemäße Angaben zu machen, die langfristig beim Anbieter der Website gespeichert werden. Hier ist also für den Verbraucher darauf zu achten, nur die nötigsten Angaben zu machen und im eigenen Interesse auf das Ausfüllen von nicht-obligatorischen Feldern zu verzichten.

Nicht-reaktive oder sogenannte implizite Verfahren zur Nutzerdatenerhebung zeichnen sich vor allem dadurch aus, dass der Nutzer nicht aktiv und/oder bewusst am Prozess der Datengenerierung und Speicherung beteiligt ist. Die Daten werden – oftmals ohne Wissen des Nutzers – im Hintergrund erfasst und ergeben sich aus dem Nutzungsverhalten des Besuchers auf der Website. Zur Erfassung solcher Daten existieren unterschiedliche Ansätze, die zum Teil auf server-, teils auf clientseitig eingesetzter Technologie basieren. Diesen Technologien gemeinsam ist, dass der Nutzer größtenteils keine expliziten Einflussmöglichkeiten auf die Erfassung und Speicherung seiner Daten hat, da dies, ebenso wie die anschließende Auswertung, meist automatisiert und maschinengesteuert abläuft.

Im Folgenden sollen zur näheren Erläuterung Techniken und Verfahren zur nicht-reaktiven Nutzerdatenerhebung beschrieben werden:

HTTP-Cookies sind vom Webserver zum Browser gesendete Daten und dienen der Zwischenspeicherung von Informationen über den Benutzer auf Webseiten. Erhobene Daten sind beispielsweise IP-Adressen, Nutzerkennwörter, Name und Adresse des Besuchers, Zeitpunkte des Aufrufs der Seite oder die Herkunftsseite (Referrer-URL). Das Deaktivieren von Cookies bringt auf der einen Seite eine erhöhte Sicherheit für den Verbraucher, kann jedoch auf der anderen Seite zu stark eingeschränkten Internetnutzungsmöglichkeiten führen, da viele webbasierte Dienste und Services vom Nutzer verlangen, Cookies im Browser zuzulassen.

Beim **Pixeltracking** werden auf den einzelnen Webseiten Bilder einer Größe von 1x1 Pixel integriert. Diese werden beim Aufruf der Seite geladen und sind mit einer JavaScript-Anwendung verbunden, die es ermöglicht, aus dem Aufruf der Seite dynamisch Parameter (z.B. Nutzer, Seite, Session-ID, Browser, Betriebssystem, etc.) auszulesen. Eine detaillierte Analyse des Nutzungsverhaltens auf der Seite, wie beispielsweise Aufrufzeit, Verweildauer und Reihenfolge der angeklickten Seiten (sog. Klicksequenz oder Clickstream) kann so erfolgen. Werden Schutzprogramme oder Proxyserver verwendet, können die entsprechenden Zählpixel allerdings zum Teil blockiert werden. Plug-Ins wie beispielsweise Adblock Plus oder Counterpixel bieten für den Firefox-Browser geeignete Maßnahmen an.

Softwareagenten sind Programme, die situationsbedingt und ohne den direkten Eingriff des Benutzers Entscheidungen treffen können, um vorgegebene Ziele zu erreichen. So können z.B. aus einem vielfältigen Angebot passende Inhalte für den Nutzer selektiert werden. Meist werden Interessen, Präferenzen oder Eigenschaften des Nutzers gespeichert. Softwareagenten sind in der Lage mit anderen Agenten zu kommunizieren. Problematisch wird dieses Verfahren in dem Moment, in dem es der unmittelbaren Kontrolle des Benutzers entgleitet, beispielsweise durch mangelnde Transparenz über die ermittelten, gespeicherten oder

weitergegebenen Daten. So ist beispielsweise eine unerwünschte Weitergabe personenbezogener Daten oder auch ganzer Nutzerprofile an andere Services denkbar. Beim anbieterseitigen Einsatz von Softwareagenten gestalten sich Erkennbarkeit und Schutzmöglichkeiten daher schwierig, weil der Nutzer häufig nicht nachvollziehen kann, inwieweit derartige Programme vom Betreiber der Website eingesetzt werden.

Modifizierte Browser dienen der Kundenbindung an ein bestimmtes Unternehmen, indem bestimmte Dienste und Links prominent in der Werkzeugleiste im Blickfeld des Nutzers platziert werden. Sie sind in der Lage, das Nutzungsverhalten aufzuzeichnen und an die Anbieter weiterzuleiten. So leitet beispielsweise die Yahoo-Toolbar bei entsprechender Einstellung nicht nur die URLs der besuchten Seiten weiter, sondern liest auch die Inhalte bestimmter Cookies aus, ermittelt die Seitenladezeiten und übermittelt diese Informationen zusammen mit einer eindeutigen Identifikationsnummer an Yahoo. Grundsätzlich kann sich der Internetnutzer durch den Einsatz von regelmäßig aktualisierten Webbrowsern wie dem Firefox oder auch dem Internet Explorer und der Vermeidung der Installation von Modifikationen schützen.

Auch die Verlaufsgeschichte des Browsers, die so genannte **Browser History**, die beim Benutzer gespeichert ist, kann von bestimmten Skripten auf den Seiten der Webanbieter ausgelesen werden und dient so zur Datenerfassung. In ihr sind beispielsweise besuchte Seiten, Zeitpunkte und Häufigkeiten der Besuche abgespeichert. Eine effektive Schutzmöglichkeit besteht in der regelmäßigen Löschung der History, die manuell im Browser vorgenommen werden kann. Auch die Einstellung der regelmäßigen automatischen Löschung der History in regelmäßigen Abständen ist möglich.

Die Methode der sogenannten **Deep Packet Inspection (DPI)**, auch als Packet Sniffing bezeichnet, arbeitet auf Datenpaketebene³ und klinkt sich direkt in den Datenverkehr zwischen Client und Server. Sie kann zusätzliche Informationen über das Nutzerverhalten bereitstellen. Datenpakete, die vom Webserver an den Nutzer verschickt werden, werden zur Datenerhebung verwendet. Die Sniffer-Programme werden entweder server- oder clientseitig oder entlang der Verbindung zwischen den beiden eingesetzt und können durch das Auswerten der Package-Informationen gezielt Informationen über das Nutzerverhalten geben. Da das Auslesen der Daten durch den Internet-Service-Provider selber erfolgt, gibt es nur wenige Möglichkeiten sich zu schützen. Dies kann beispielsweise über Plug-Ins und Verschlüsselungstechniken geschehen.⁴

Der Einsatz von sogenannten **Mastracking-Verfahren** ermöglicht die Interaktion des Besuchers mit der Webseite genauer zu verfolgen und Bereiche zu identifizieren, die die Aufmerksamkeit des Benutzers stärker als andere auf sich gezogen haben. Werden die Daten aus dem Mastracking mit anderen Nutzerdaten kombiniert, so lassen sich Verhaltensprofile

³ Eine HTML-Anfrage wird in sog. Packages, Datenpakete, zerlegt, die beim Empfänger der Anfrage wieder zusammengesetzt werden müssen. Sie enthalten entsprechende Informationen über Inhalt, Herkunft und Bestimmungsort.

⁴ Beispielsweise über Plug-Ins wie SSL Guard: <https://addons.mozilla.org/en-US/firefox/addon/14916/> oder Perspectives <http://www.cs.cmu.edu/~perspectives/firefox.html>, Stand: 3.11.10

bestimmter Nutzer oder Nutzergruppen erstellen. Webseiten und Webinhalte lassen sich so auf die spezifischen Bedürfnisse der Nutzer abstimmen. Mastracking-Verfahren lassen sich zum Teil mit den Firefox Plug-Ins NoScript oder ADBlock Plus blockieren. Hundertprozentiger Schutz kann jedoch nicht in allen Fällen mit Sicherheit gewährleistet werden.

Bei **Webserver-Logfiles** handelt es sich um Textdateien, die eine genaue Analyse des Datenverkehrs (Datenzu- und Abgänge, sog. Traffic) zwischen Server und Clients auf der Seite ermöglichen. Standardmäßig erfasste Daten sind IP-Adresse des Nutzers, Webserver, Besucherzahl und -zeit, Herkunft der Besucher, Eintritts- und Ausstiegszeiten, verwendeter Browser und Betriebssystem, angefragte Dateien und übertragene Inhalte. Darüber hinaus ist es möglich im Rahmen von E-Commerce-Anwendungen Daten wie Umsatz und Einkaufsvolumen festzuhalten. Mit Hilfe von Authentifizierungsdaten ist es außerdem möglich, User-ID's zu speichern und potentiell mit getätigten Transaktionen zu verknüpfen. Es gibt Erweiterungen für den Browser, mit denen Webanalyse-Tools und Zählpixel erkannt und zum Teil geblockt werden können. Auch die bereits zuvor erwähnte Verwendung von Proxy-Servern und die Vergabe dynamischer IP-Adressen können einen Schutz für den Verbraucher darstellen.

Die nachfolgende Tabelle gibt eine kurze Übersicht über eingesetzte Techniken und Verfahren zur Nutzerdatenerfassung im Web. Dargestellt werden hierbei vor allem die Aspekte der Erkennbarkeit der jeweiligen Technik für den Nutzer, seine Zustimmungsmöglichkeiten zur Datenerfassung sowie Schutzmöglichkeiten und Risikopotentiale der Verfahren.

Eingesetzte Technik	Erkennbarkeit	Zustimmung	Erfasste Daten	Schutzmöglichkeit	Risikopotential
Reaktive Verfahren					
Registrierung	Ja	Ja*	Demografische Daten, Mikrogeografische Daten	Verzicht auf Ausfüllen nicht-obligatorischer Eingabefelder	Lokalisierung, demografische Segmentierung, bei Login eindeutige Zuordnung von Nutzer und Nutzungsverhalten
Relevance Feedback	Ja	Ja	Interessen, Präferenzen	Verzicht auf Teilnahme	Koppelung von persönlichen Präferenzen/Interessen und User-ID bzw. Login
Sonstige Benutzereingaben (Fragebögen, Umfragen, etc.)	Ja	Ja	Demografische Daten, Mikrogeografische Daten, Einkommen, Beruf (sozialer Status), Interessen, Präferenzen	Verzicht auf Teilnahme	Koppelung von User-ID/Login, demografischen Daten, geografischen Daten und sonstigen Daten (Einkommen, Haushaltsgröße) möglich
Nichtreaktive Verfahren					
Cookies	Nein	Ja **	User/Session-ID, IP-Adresse, Referrer, Start-&Exit, Timestamp, Clickstream	Löschen der Cookies nach Beendigung der Session, Verweigerung von Cookies	Koppelung von User-ID/Login mit Nutzungsverhalten und Präferenzen (angeklickte Seiten, Verweildauer, Nutzungsverlauf)
Softwareagenten	Nein	Ja **	Benutzerpräferenzen, Einkaufsdaten Produktdaten	Verzicht auf den nutzerseitigen Einsatz von Agentenprogrammen Verwendung von Proxyservern oder dynamischen IP-Adressen	Koppelung von User-ID/Login mit Präferenzen, Interessen, Kontrollverlust des Nutzers durch autonomes Handeln des Programms

Eingesetzte Technik	Erkennbarkeit	Zustimmung	Erfasste Daten	Schutzmöglichkeit	Risikopotential
Pixel Tracking	Nein	Nein	User/Session-ID, (IP-Adresse), Referrer, Start-&Exit, Timestamp, Clickstream, Hits, Pageviews	Blockierung von Zählpixeln durch Plug-Ins	Externes Auslesen von IP-Adresse und angeschaute Seiten
Modifizierte Browser	Ja	Ja	User/Session-ID, IP-Adresse, Referrer, Start-&Exit, Timestamp, Clickstream, Hits&Pageviews	Verzicht auf Toolbars und Modifizierte Browser	Koppelung von Browserhistorie mit Nutzungsverhalten und User-ID/Login
Browser History	Nein	Nein	Browsing-Historie	Regelmäßige Löschung der Historie	Auslesen des früheren Nutzungsverhaltens möglich
Deep Paket Inspection	Nein	Nein	Package-Inhalt, Start & Ziel-IP	Verschlüsselung, Plug-Ins	Erfassung sämtlicher gesendeter Inhalte des Nutzers (ID, Nutzungsverhalten), Ableitung von Interessen, Präferenzen möglich
Maustracking	Nein	Nein	Klickverhalten des Nutzers auf der Webseite	Blockieren von Tracking-Verfahren über Plug-Ins	Detaillierte Erfassung der Interaktion des Nutzers mit der Webseite möglich
Server-Logfile Analyse	Nein	Nein	User/Session-ID, IP-Adresse, Referrer, Start-&Exit, Timestamp, Clickstream, Hits&Pageviews	Browser-Plug-Ins, Proxy-Server Anonymisierungsdienste	s. Cookies

3. Data-Mining-Verfahren und Auswertung der erhobenen Daten

Um die Bildung eines möglichst umfassenden und detaillierten Nutzerprofils zu ermöglichen, werden in den meisten Fällen integrative Ansätze verfolgt, die es sich zum Ziel machen, Daten unterschiedlichster Herkunft mit einzubeziehen: Reaktiv erhobene Informationen wie demografische Angaben, Herkunft, Familienstand etc. werden zu Analysezwecken mit nicht-reaktiv erhobenen Daten aus Tracking-Logs, Server-Logs oder sonstigen im vorherigen Abschnitt beschriebenen Verfahren zusammengefasst.

Werden die Nutzungsdaten homogenisiert und aggregiert ist es möglich, anhand automatischer Datenanalyseverfahren Muster und Regelmäßigkeiten zu ermitteln sowie umfassende und potentiell personenbeziehbare Kundenprofile zu erstellen. Dies geschieht mithilfe der Anwendung von Data-Mining-Techniken auf die bestehenden Datensätze und kann auch als Web-Usage-Mining bezeichnet werden. Die generellen Ziele des Mining-Prozesses können unterteilt werden in Entdeckung impliziten Wissens (Erkenntnisgewinnung) und Vorhersage. Unter „Erkenntnisgewinnung“ fallen das sogenannte Clustering (Bildung von Kundensegmenten aufgrund gemeinsam auftretender Eigenschaften), die Bildung von Assoziationsregeln (wie oft werden Produkte X und Y zusammen gekauft?) und die Analyse von Klicksequenzen (welche Seiten werden nacheinander angeklickt?).⁵ Unter „Vorhersage“ werden der Prozess der Klassifikation (in welches Kundensegment fällt Käufer X aufgrund seiner Kauf- und/oder Klickhistory?) und der Verhaltensvorhersage (was wird der Kunde als nächstes tun?) gefasst.

Liegen die mittels Datenbereinigung und Mining-Verfahren aufbereiteten und aggregierten Daten vor, so lassen sich aus diesen mithilfe unterschiedlicher Anwendungsverfahren Benutzerprofile erstellen. Mögliche Ansätze sind hierbei schlagwortbasierte Profile, semantische Netze oder konzeptbasierte Modelle. Alle haben zum Ziel, die bestehende Wissensbasis über den Nutzer möglichst effektiv und aussagekräftig abzubilden, um dieses für die jeweiligen anschließenden Ziele (Marketing, Personalisierung etc.) zu nutzen.

4. Risiken für den Verbraucher

Die systematische Erfassung, Speicherung und Auswertung von Kundendaten mittels reaktiver und nicht-reaktiver Verfahren sowie Mining-Techniken und eine anschließende Profilerstellung birgt deutliche Risiken für den Verbraucher. Bei den nicht-reaktiven Erhebungstechniken erfolgt die Erfassung der Nutzeraktivitäten im Web ohne das Einverständnis des Verbrauchers und in den meisten Fällen ohne sein Wissen. Da davon ausgegangen werden kann, dass der Verbraucher, der sich ohnehin mit einem Überangebot an Information im Web konfrontiert sieht, kaum jede einzelne Datenschutzerklärung der Anbieter von Webservices lesen und verstehen wird, besteht hier ein besonders

⁵ Perner (2002)

problematischer Sachverhalt. Ebenso ist für den Nutzer oft nur schwer nachvollziehbar, in welchem Maße eine Datenweitergabe an Dritte stattfindet oder stattgefunden hat. Daher besteht hier zusätzlich das Gefahrenpotential, dass der Verbraucher sein Recht auf Auskunft und Löschung der Daten nicht mehr oder nur in unzureichendem Maße wahrnehmen kann, was zudem ein Bewusstsein für die dauerhafte beziehungsweise langfristige Speicherung seiner Daten voraussetzen würde. Selbst wenn der Nutzer eine Löschung seiner Daten an einer Stelle beantragt, zieht dies nicht automatisch die Löschung bei Drittempfängern nach sich. Ein so erstelltes Nutzerprofil, das sich nicht mehr in der Wahrnehmung der zugehörigen Person befindet, kann auf längere Zeit im Netz bestehen bleiben und trägt zum Verlust der informationellen Selbstbestimmung des Internetnutzers bei. Auch steigt bei einer Weitergabe der Daten an Dritte die Möglichkeit eines potentiellen Datenmissbrauchs oder Datendiebstahls, so dass die zu Beginn rechtmäßig erworbenen Daten unter Umständen entwendet und für unerwünschte Massen-E-mails und Werbung sowie kriminelle Zwecke (bspw. Phishing) verwendet werden können. Vor allem aber die Aggregation von Daten unterschiedlicher Herkunft durch eigens darauf ausgerichtete Anbieter schafft die Möglichkeit, ein umfassendes und aktuelles Profil über den individuellen Nutzer zu bilden. Aggregierte Informationen aus demografischen Daten, Einkaufsdaten, (mikro-) geografischen Daten und Profilinformatoren liefern ein vielfach facettenreiches Nutzerprofil und bilden somit ein potentiell hohes, ernstzunehmendes und nur schwer zu kontrollierendes Risiko für den Verbraucher. Besonders Soziale Netzwerke fallen durch Sicherheitslücken, mangelhaften Datenschutz und die langfristige Speicherung und Weitergabe von Daten an Dritte negativ auf. Auch die Auslagerung eines Teils der unternehmensinternen oder der privaten Daten zu externen Anbietern oder Dienstleistern (Cloud Computing) wirft erhebliche neue Fragen bezüglich Datensicherheit und Datenschutz auf. Als besonders kritisch erscheinen die augenblicklichen Entwicklungen beim Datenschutz im Mobilfunkmarkt. Die tiefgreifende System-Integration der Smartphone-Apps ermöglicht den Anbietern persönliche Profile bis auf den metergenauen Standort sowie die Telefonnummern der eigenen Kontakte zu ermitteln. In diesem Zusammenhang entstehende Geodaten können von Drittparteien zu kriminellen Zwecken missbraucht werden. Die zunehmende Automatisierung in der Bildverarbeitung führt zu immer mehr Datenspurten im Internet, die in steigendem Maße auf den einzelnen Verbraucher bezogen werden können.

5. Schutzmöglichkeiten des Verbrauchers im Internet

Wie bereits beschrieben, sind die Schutzmöglichkeiten und Sicherheitseinstellungen, die der Verbraucher beim Besuch im Internet lokal auf seinem eigenen Rechner vornehmen kann zum Teil unzureichend und hinderlich für das Surfen im Internet. Es besteht daher die Notwendigkeit über die Deaktivierung von Website-Technologien wie JavaScript oder Cookies hinaus Möglichkeiten zu finden, einen sinnvollen Schutz der Privatsphäre des Verbrauchers im Internet zu gewährleisten. Lösungsmöglichkeiten können hierbei sowohl nutzerseitig als auch auf Anbieterseite zum Einsatz kommen. Der Nutzer kann einerseits durch den Einsatz von Anonymisierungstechniken (im E-Commerce und bei

Kreditkartenzahlungen) für ein erhöhtes Maß an Sicherheit und Datenschutz sorgen, andererseits tragen Aufklärungs- und Kontrollmaßnahmen durch Institutionen und Verbände dazu bei, eine öffentliche Wahrnehmung für das Thema zu schaffen, um Maßnahmen auf Anbieterseite voranzutreiben. Es existiert ebenfalls eine Reihe von Drittakteuren (z.B. Initiativen, Gütesiegel). Handlungsziel von Anbietern und Drittakteuren ist zum einen die Verwendung verschlüsselter Technologien, zum anderen die Aufklärung des Verbrauchers über bestehende Risiken und Handlungsanweisungen zum Verhalten im Internet. Auch die Bereitstellung von Standards für Anbieter von Internetplattformen fällt unter den Handlungsbereich der Drittanbieter. In diesem Kontext kann beispielsweise die Integration von automatisierten Verfahren zum Auslesen der Datenschutzerklärungen von Anbietern und Betreibern eine sinnvolle Maßnahme darstellen. Zusammengefasst lässt sich festhalten, dass vor allem die Kombination unterschiedlicher Maßnahmen auf allen Seiten zu einer effektiven Erhöhung der Verbrauchersicherheit im Internet führt und so dem Prozess der Profilbildung entgegenwirken und diesen auf ein verbrauchererträgliches Maß zu beschränken versuchen kann.

6. Auswirkungen der Profilbildung auf die Position des Verbrauchers

Der Prozess der Profilbildung hat zum Teil erhebliche Auswirkungen auf die Position des Verbrauchers am Markt. Zum einen kann es zu einer informationellen Diskriminierung der Verbraucher kommen, so dass ihm nicht mehr alle sich am Markt befindlichen Informationen zur Verfügung stehen. Dies geschieht z.B. durch die personalisierte Anpassung der Inhalte einer Internetseite. Zum anderen kann aber auch eine Preisdiskriminierung die Folge einer Nutzerprofilbildung sein. Ein häufiges Beispiel für Preisdiskriminierung im Internet sind bessere Angebote für Kunden, die bereits häufiger bei einem Anbieter etwas gekauft haben. Dadurch erhält ein Nutzer lediglich aufgrund seines Nutzerprofils einen anderen Preis für das gleiche Angebot als andere Nutzer.

Durch Nutzerdatenerfassung und dem daraus resultierenden Profiling resultieren aber nicht nur Risiken für den Verbraucher, sondern auch die Entstehung von Mehrwert ist möglich. Dies zeichnet sich in einer Vielzahl neuer Modelle und Prozesse beispielsweise im E-Commerce und bei Webservices ab. Da das World Wide Web, wie in der Einleitung beschrieben, vor allen Dingen dem Konsum, der Informationsbeschaffung und der Kommunikation dient, soll der Verbraucher sinnvoll und effektiv bei seinen Aufgaben und Bedürfnissen unterstützt werden. Beispiele für unterstützende Dienstleistungen und Services stellen Personalisierungs- und Empfehlungssysteme (Recommender) dar.

Empfehlungssysteme schlagen dem Nutzer in einem bestimmten Anwendungskontext Objekte vor, die für diesen aufgrund seines Profils als relevant eingestuft wurden. Dies kommt z.B. innerhalb Sozialer Netzwerke oder im E-Commerce zum Einsatz. Die Vorschläge können hierbei auf den Empfehlungen anderer Nutzer mit ähnlichen Profilen, auf Produktähnlichkeiten oder allgemeinen Regeln basieren. Ein weiteres Geschäftsmodell, das durch den Einsatz von Nutzerdatenerfassung und Profiling zum Einsatz kommt, ist die sogenannte Personalisierung von Inhalten im Web. Unter Personalisierung wird eine

Anpassung der Webinhalte oder des Seitenaufbaus an die individuellen Ansprüche des Nutzers verstanden, die durch verschiedene Verfahren, welche dabei die über den Nutzer gespeicherten Informationen verwenden, ermöglicht wird. Personalisierung kann dabei explizit (direkte Interaktion des Nutzers mit der Seite, Angabe von Vorlieben und Präferenzen in Formular- oder Auswahlfelder), sessionbasiert implizit (Anpassung der Inhalte dynamisch basierend auf dem aktuellen Nutzungsverhalten) oder sessionübergreifend implizit (Anpassung der Inhalte basierend auf vorherigen Besuchen der Website) erfolgen.

7. Schlussfolgerungen

Das hier vorliegende Gutachten hat weitgehend die bislang verwendeten Verfahren, Risiken und möglichen Schutzmaßnahmen gegen die Sammlung personenbezogener Daten zusammengefasst. Viele existierende Lösungen haben bislang noch keine allgemeine Verbreitung gefunden. Die Mehrheit der Verbraucher sieht allerdings Handlungsbedarf im Bereich Datenschutz in Deutschland. Somit scheint ein Widerspruch zwischen dem theoretischen Bewusstsein um die Gefahren der Ausspähung persönlicher Daten, dem Misstrauen gegenüber den Schutzmöglichkeiten der Technik und der Einhaltung des Datenschutzes durch die Anbieter und dem tatsächlichen Verhalten im Internet zu liegen. Die Ursache hierfür dürfte das Dilemma sein, entweder an der Datenfreigabe teilzunehmen und die Gefahr der missbräuchlichen Verwendung eigener Daten einzugehen oder einen Selbstausschluss aus einem zunehmend populärer werdenden Teil des sozialen und wirtschaftlichen Kontextes vorzunehmen. Die technische Komplexität, die es bislang kaum möglich macht, ohne erhebliches Vorwissen die individuellen Sicherheitseinstellungen an die Erfordernisse der verschiedenen Webseiten anzupassen, stellt ein weiteres Problem dar. Das Ziel aus Verbraucherschutzsicht muss es daher sein, dem „mündigen“ Verbraucher, also jemandem mit durchschnittlichen technischen und juristischen Kenntnissen, die Möglichkeit der Nutzung von Internetdienstleistungen zu ermöglichen, ohne das widerrechtlich personenbezogene Daten gespeichert und für weiterführende Analysen oder Werbung eingesetzt werden. Andererseits muss aber auch den Besonderheiten des Kommunikationsmediums Internet Rechnung getragen werden, welches gerade durch die Anpassung der Informationen an die persönlichen Bedürfnisse der Verbraucher seinen Siegeszug begründet hat. Unternehmen sollten Privacy-Aspekte bereits bei der Planung des Internetangebots berücksichtigen. Potenziell kritische Technologien, die Nutzer mit starken Sicherheitseinstellungen abschrecken, die Verwendung von Flash oder von Pixeltracking sollten hinterfragt werden. Ebenfalls zur Datensicherheit kann das Bereitstellen eines mit Hilfe von SSL verschlüsselten Angebots beitragen. Für die Politik gilt, möglichst die Aufklärungsbemühungen der Verbraucher über den Umgang mit persönlichen Daten weiter aufrecht zu erhalten oder sogar auszubauen, um dem Nutzer im konkreten Anwendungsfall die Entscheidung zu erleichtern. Weiterhin muss ein verantwortungsvoller Umgang der Verbraucher mit den eigenen Daten möglich sein, ohne dass es zu einer informationellen Diskriminierung im Internet kommt. Durch die Förderung komplexitätsreduzierender Maßnahmen wie einer Matrix oder einem Ampelsystem könnte mehr Transparenz geschaffen

werden. Generell wäre die Schaffung einer personalisierten Übersicht über die erhobenen und gespeicherten Daten wie beim Anbieter Google wünschenswert, innerhalb deren es die Möglichkeit zur Löschung der Inhalte gibt. Verbraucher müssen darauf aufmerksam gemacht werden, dass sie selbst ihren Beitrag dazu leisten können, sich nicht zum gläsernen Kunden für die Werbetreibenden und Unternehmen im Internet zu machen.