

# Die Macht der Daten: Untersuchung der Trackingpraktiken österreichischer Websites

DIPLOMARBEIT

zur Erlangung des akademischen Grades

**Diplom-Ingenieurin**

im Rahmen des Studiums

**Medieninformatik**

eingereicht von

**Doris Gansterer Bakk.techn.**

Matrikelnummer 0025878

an der  
Fakultät für Informatik der Technischen Universität Wien

Betreuung  
Betreuer: ao. Univ. Prof. DI. Dr. Peter Purgathofer

Wien, 22. August 2016 \_\_\_\_\_

(Unterschrift Verfasserin)

\_\_\_\_\_

(Unterschrift Betreuer)

# Selbstständigkeitserklärung

”Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit einschließlich Tabellen, Karten und Abbildungen, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.“

Wien, 22. August 2016

Doris Gansterer  
Spittelbreitengasse 28/15  
1120 Wien

# Kurzfassung

Sobald eine Person im Internet surft, werden personenbezogene Daten gesammelt, analysiert und weiterverarbeitet. In dieser Diplomarbeit wird eine Einführung in das Thema des Online-Trackings geboten. Anhand praktischer Beispiele wird aufgeführt, welche Daten von welchen Unternehmen und zu welchem Zweck erhoben werden. Dazu werden die Begriffe First-Party-Tracking und Third-Party-Tracking erklärt. Es werden derzeit gängige Trackingtechnologien wie HTTP-Cookies, Etags, Web Bugs, History Sniffing, Fingerprinting sowie Tracking mittels Social-Media-Plug-ins oder des Internetproviders dargestellt. Anhand von gesetzlichen, organisatorischen und technischen Maßnahmen werden Möglichkeiten zum Datenschutz und der Wahrung der Privatsphäre aufgezeigt. Im Rahmen dieser Arbeit werden zehn beliebte österreichische Websites auf ihre Tracking- und Profilingtechniken hin analysiert. Abschließend wird ein Best-Practice-Beispiel präsentiert.

# Abstract

Once a person is online, personal data are collected, analyzed and processed. This thesis gives an introduction to tracking on the Internet. By using examples from known companies, it shows which data are collected from whom and for what reasons. The terms first-party tracking and third-party tracking are explained. Common tracking technologies are presented, such as HTTP cookies, etags, web bugs, history sniffing, fingerprinting or tracking via social media plug-ins or the Internet provider. Legal, self-regulating and technical measures for data protection and privacy are discussed. Furthermore, the tracking and profiling techniques of ten popular Austrian websites are analyzed and the results are presented. The thesis concludes with an example of best practices.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Motivation und Fragestellung . . . . .	2
1.2	Aufbau der Arbeit . . . . .	3
<b>2</b>	<b>Tracking im Internet</b>	<b>5</b>
2.1	Was ist Internet-Tracking und wofür wird es eingesetzt? . . . . .	6
2.1.1	Bekämpfung von Internet-Kriminalität . . . . .	10
2.1.2	Website-Analyse . . . . .	11
2.1.3	User-Profilung und Online-Marketing . . . . .	14
2.2	Tracking-Technologien . . . . .	20
2.2.1	HTTP-Cookie . . . . .	20
2.2.2	Flash-Cookie . . . . .	22
2.2.3	HTML5-Cookie . . . . .	24
2.2.4	Etags . . . . .	26
2.2.5	Evercookie . . . . .	28
2.2.6	Supercookie . . . . .	29
2.2.7	Web Bugs . . . . .	29
2.2.8	History Sniffing . . . . .	30
2.2.9	Browser-Fingerabdruck . . . . .	32
2.2.10	Canvas Fingerprinting . . . . .	34
2.2.11	Geräte-Fingerabdruck . . . . .	38
2.2.12	Tracking durch Social-Media-Buttons . . . . .	41
2.2.13	Tracking mittels Internetdiensteanbieter . . . . .	50
2.3	Gefahren durch Tracking . . . . .	54
2.3.1	Preismanipulation . . . . .	54
2.3.2	Personenscoring . . . . .	57
2.3.3	Filterblase . . . . .	61

<b>3</b>	<b>Schutzmaßnahmen</b>	<b>66</b>
3.1	Gesetzliche Maßnahmen . . . . .	67
3.1.1	Das Österreichische Datenschutzgesetz . . . . .	68
3.1.2	Telekommunikationsgesetz . . . . .	71
3.1.3	Das E-Commerce-Gesetz . . . . .	79
3.1.4	Internationaler Datenschutz . . . . .	81
3.2	Organisatorische Maßnahmen . . . . .	86
3.2.1	Nutzungsbedingungen . . . . .	86
3.2.2	Datenschutz-Gütesiegel . . . . .	94
3.2.3	Selbstregulierungs-Systeme . . . . .	103
3.3	Technische Maßnahmen . . . . .	110
3.3.1	Einstellungen im Browser . . . . .	111
3.3.2	Browsererweiterungen . . . . .	119
<b>4</b>	<b>Trackingbeispiele in Österreich</b>	<b>130</b>
4.1	Österreichischer Rundfunk ORF - www.orf.at . . . . .	133
4.2	Tageszeitung Der Standard - www.derstandard.at . . . . .	134
4.3	Tageszeitung KURIER - www.kurier.at . . . . .	136
4.4	Kronen Zeitung - www.krone.at . . . . .	143
4.5	Kleinanzeigenportal Willhaben - www.willhaben.at . . . . .	146
4.6	Gelbe Seiten HEROLD - www.herold.at . . . . .	147
4.7	Online-Stellenmarkt - www.karriere.at . . . . .	149
4.8	Bundesministerium für Finanzen - www.bmf.gv.at . . . . .	150
4.9	Raiffeisen Bank - www.raiffeisen.at . . . . .	151
4.10	Erste Bank und Sparkasse - www.sparkasse.at . . . . .	152
4.11	Tracking-Ergebnisse . . . . .	153
<b>5</b>	<b>Fazit und Best Practice</b>	<b>158</b>
<b>6</b>	<b>ANHANG</b>	<b>161</b>
	<b>Literaturverzeichnis</b>	<b>168</b>

# Abbildungsverzeichnis

2.1	User-Authentifizierung bei Facebook . . . . .	11
2.2	Weltweiter Einsatz von Website-Analyse-Tools . . . . .	13
2.3	Infografik zu Datenmerkmalen bei Acxiom . . . . .	17
2.4	Tracking in der Werbebranche . . . . .	18
2.5	Firefox Canvas Fingerabdruck . . . . .	36
2.6	Google Chrome Canvas Fingerabdruck . . . . .	37
2.7	Safari Canvas Fingerabdruck . . . . .	37
2.8	Opera Canvas Fingerabdruck . . . . .	37
2.9	Zwei-Klick-Button auf heise online . . . . .	43
2.10	Aktiver Twitter-Button auf heise online nach dem ersten Klick . . . . .	43
2.11	Aktiver Twitter-Button auf heise online nach dem zweiten Klick . . . . .	44
2.12	Shariff-Social-Media-Buttons auf heise online . . . . .	44
2.13	Zwei-Klick-Lösung auf futurezone.at in 2011 . . . . .	45
2.14	AddThis Sammel-Social-Media-Button auf futurezone.at in 2016 . . . . .	46
2.15	Web-Entwickler Konsole von Firefox, Reiter Sicherheit auf der Homepage von futurezone.at . . . . .	48
2.16	Ghostery-Ersatzbuttons von Facebook und Twitter auf der Homepage von futurezone.at . . . . .	48
2.17	Infografik zu Tracking eines Kunden, der ein Auto kaufen möchte . . . . .	56
2.18	Infografik zu Lösungen von Fitbit für Gesundheit im Unternehmen . . . . .	59
3.1	Startseite von www.futurezone.at . . . . .	75
3.2	Informationsseite zu Cookies von eur-lex.europa.eu . . . . .	77
3.3	Startseite von www.heute.at . . . . .	80
3.4	Registrieren auf Facebook . . . . .	87
3.5	Wortanzahl der Facebook Datenschutzbestimmung . . . . .	88
3.6	TRUSTe-Gütesiegel von Zynga . . . . .	95
3.7	TRUSTe-Zertifizierungsbestätigung von Zynga . . . . .	96
3.8	Homepage von nugg.ad 2011 . . . . .	97
3.9	Homepage von nugg.ad 2016 . . . . .	98

3.10	Fragebogen von nugg.ad auf derstandard.at . . . . .	99
3.11	Wiener Linien - Ticket Shop . . . . .	101
3.12	Euro-Label-Zertifikat des Wiener Linien Online-Shops . . . . .	102
3.13	”Advertising Option Icon” auf der Homepage von msn Österreich . . . . .	105
3.14	Informationen zu Anzeigen via Microsoft . . . . .	106
3.15	Werbeanzeige mit ”AdChoice Icon” auf der kurier.at-Startseite . . . . .	108
3.16	Marktanteil Browser in Österreich . . . . .	110
3.17	Cookie-Browser-Einstellungen . . . . .	111
3.18	Marktanteil Suchmaschinen in Österreich . . . . .	116
3.19	Marktanteil Suchmaschinen weltweit . . . . .	117
3.20	Firefox Datenschutz-Einstellungen . . . . .	118
3.21	Sperre von Werbeblocker auf bild.de . . . . .	121
3.22	Einsatz von Flashblock auf derstandard.at . . . . .	122
3.23	Werbeanzeigen auf derstandard.at . . . . .	123
3.24	Einsatz von Ghostery auf willhaben.at . . . . .	124
3.25	Durch Ghostery blockierte Social-Media-Buttons . . . . .	125
3.26	Visuelle Tracker-Darstellung durch Disconnect auf krone.at . . . . .	127
4.1	Bezahlte Artikel auf www.kurier.at . . . . .	137
4.2	Erster Teil: Gegenüberstellung bezahlter Artikel/ tatsächlicher Kurier-Artikel . . . . .	138
4.3	Zweiter Teil: Gegenüberstellung bezahlter Artikel/ tatsächlicher Kurier-Artikel auf www.kurier.at . . . . .	139
4.4	Gesponserte Artikel auf www.kurier.at . . . . .	141
4.5	Informationstext zu ”outbrain.com” auf www.kurier.at . . . . .	142
4.6	Bezahlte Artikel auf www.krone.at . . . . .	145
4.7	Tracking-Analyse in Österreich . . . . .	157

# 1 Einleitung

Sobald ein User online geht und im Internet surft, findet zwischen der aufgerufenen Webseite und dem verwendeten Browser ein Datenaustausch statt. Dieser ist notwendig, um eine Verbindung zum Webserver herzustellen, eine aufgerufene Webseite vollständig zu laden, ihre Darstellung korrekt anzuzeigen und ihre Funktionen verfügbar zu machen.

Bei diesem Prozess können auch Daten des Webclients, also des Anwenders, gespeichert werden, die unabhängig und für den Aufbau einer Internetseite nicht notwendig sind. Die Datenübertragung findet im Hintergrund und für den Benutzer nicht wahrnehmbar statt. Sofern ein Internetuser nicht bewusst bzw. freiwillig Daten von sich preisgibt, etwa weil er online ein Formular ausfüllt, ein Profil oder Konto anlegt bzw. einen Blogbeitrag oder ein Kommentar verfasst, bemerkt dieser das Speichern und Sammeln seiner Daten von externen Stellen nicht.

Dem Anwender bleibt verborgen, welche seiner Daten im Detail gespeichert werden, dass diese analysiert, weiter verarbeitet und aus den Ergebnissen neue Daten aggregiert und für zusätzliche Zwecke verwendet werden, welche Unternehmen daran beteiligt sind und dass das Erheben von Daten über mehrere Websites hinweg stattfinden kann.

Zu den bekanntesten und größten Datenmonopolen gehören Google und Facebook. Deren Kerngeschäft ist die Vermarktung personenbezogener Daten, womit sie größtenteils ihr Bestehen und ihre angebotenen Dienstleistungen finanzieren.

Big Data, Data Mining, Direktmarketing, Adresshandel oder Data Broker sind diverse Begriffe, die aus einem Wirtschaftszweig stammen, der sich mit der Verarbeitung, Auswertung und dem Handel großer Datenmengen, unter anderem von Personenprofilen, beschäftigt.



Dem gegenüber stehen Datenschützer sowie nationale und internationale Datenschutzgesetze, die sich mit der Wahrung der Privatsphäre und der Rechte jedes Einzelnen bezüglich seiner Daten befassen und diese der Wirtschaft gegenüber verteidigen.

## 1.1 Motivation und Fragestellung

Die Motivation sich in dieser Diplomarbeit mit dem Thema Tracking im Internet auseinanderzusetzen beruht darauf, eine differenzierte Betrachtungsweise zu den beiden Aussagen *"Ich habe nichts zu verbergen."* und *"Es ist ja nur Werbung."* zu schaffen und infrage zu stellen. Erstere suggeriert im Allgemeinen kriminelle Hintergedanken, wenn für das Gegenteil eingetreten wird. Zweitere stellt eine Verharmlosung geläufiger Trackingmechanismen und darauf beruhenden Werbepraktiken dar.

Wenn von Privatpersonen erwartet wird, dass sie nichts zu verbergen haben, dann sollte dies auch für jene Unternehmen gelten, die mit den von Internetusern generierten Daten Geld verdienen und hohe Profite erwirtschaften. Sie sollten transparente, vollständige, aussagekräftige und verständliche Informationen zu ihren Geschäftspraktiken liefern.

Ziel dieser Arbeit ist es daher ein Bewusstsein für Usertracking im Internet und dem damit einhergehenden Datensammeln, -analysieren, -auswerten und die Kommerzialisierung der Tracking-Ergebnisse zu entwickeln. Um den technischen Sachverhalt für Laien verständlicher darzustellen, werden in jedem Kapitel aktuelle, relevante und praktische Beispiele miteingebunden.

Die Fragen, wer sammelt, wie, aus welchem Grund Benutzerdaten, ist dieses Vorgehen rechtlich erlaubt, welche Auswirkungen kann Internet-Tracking haben und was kann der Einzelne dagegen tun, sollen bestmöglich beantwortet werden. Der Leser soll ein Gefühl dafür bekommen, was seine personenbezogenen Daten wert sind. Weiters wird die Verantwortung der Entwickler hinsichtlich zugrundeliegender technischer Systeme und Anwendungen, der Gesetzgeber bezüglich sinnvoller Datenschutzregelungen und rechtlicher Normen und der Gesellschaft gegenüber einer versierten Medienkompetenz thematisiert.

## 1.2 Aufbau der Arbeit

Die Diplomarbeit ist in drei Abschnitte unterteilt: Tracking im Internet, Schutzmaßnahmen und Trackingbeispiele in Österreich.

Zu Beginn von Kapitel 2 wird erklärt, was Web-Tracking ist, welche Daten von einem Internetuser gespeichert werden können, was der Unterschied zwischen First-Party- und Third-Party-Tracking ist und welche die gängigsten Anwendungsgebiete von Tracking im Internet sind: Kriminalitätsbekämpfung, Website-Analyse und User-Profiling bzw. Online-Marketing. Es wird eine kurze Übersicht über die derzeit bekanntesten Tracking-techniken, wie zum Beispiel HTTP-Cookies, Etags, Web Bugs, History Sniffing, Fingerprinting oder Tracking mittels Social-Media-Buttons, gegeben und auf die Gefahren wie etwa Preismanipulation, Personenscoring oder die Entwicklung einer Filterblase hingewiesen.

Kapitel 3 beschäftigt sich mit den gesetzlichen, organisatorischen und technischen Schutzmaßnahmen zur Wahrung der Privatsphäre und der Einhaltung des Datenschutzes im Internet. Es werden das österreichische Datenschutz-, Telekommunikations- und E-Commerce-Gesetz, Datenschutzbestimmungen der Europäischen Union und das kontrovers gesehene "Safe Harbor"-Abkommen und dessen Nachfolger, das "EU-US Privacy Shield", behandelt. Weiters wird die Bedeutung von Nutzungsbedingungen und Allgemeinen Geschäftsbedingungen, Datenschutz- bzw. E-Commerce-Gütesiegel und Selbstregulierungssysteme und die Problematik von Opt-Out-Mechanismen erörtert. Abschließend werden technische Hilfsmittel gegen Tracking wie konkrete Browsereinstellungen und nützliche Browsererweiterungen vorgestellt.

In Kapitel 4 werden zehn der beliebtesten, österreichischen Websites auf ihre Tracking- und Profilingtechniken hin analysiert. Es wird untersucht, welche First- und Third-Party-Cookies gesetzt werden, welche zusätzlichen Tracking-Elemente aktiv sind, wie transparent und verständlich die jeweiligen Allgemeinen Geschäftsbedingungen und Datenschutzerklärungen sind, welche Social-Media-Plug-ins im Einsatz sind und wie Werbeanzeigen gehandhabt werden.

---

In Kapitel 3 und 4 werden die Ergebnisse des Interviews mit ao. Univ.-Prof. Dr. Markus Haslinger an der Technischen Universität Wien eingearbeitet. Das Gespräch dient einerseits zum Verständnis der vorliegenden österreichischen Gesetzestexte aus Kapitel 3 und andererseits der kritischen Hinterfragung der AGBs und Datenschutzbestimmungen der untersuchten österreichischen Webauftritte in Kapitel 4. Der verwendete Fragenkatalog ist im Anhang der Diplomarbeit zu finden.

In den abschließenden Bemerkungen von Kapitel 5 werden die Schlussfolgerungen der Diplomarbeit und ein Best Practice Beispiel präsentiert.

Nicht Gegenstand dieser Diplomarbeit sind Cross-Device-Tracking<sup>1</sup> und Internet-Tracking beim Gebrauch von Tablets, Smartphones oder zusätzlich installierter mobiler Apps bzw. entsprechender Desktop-Varianten. Für diese wissenschaftliche Arbeit wurden ein Personal Computer, ein Notebook und entsprechende Browser eingesetzt. Unter diesem Aspekt werden Internet-Tracking und die darauf aufbauenden Themen eingehend behandelt.

---

<sup>1</sup>Cross-Device-Tracking bezeichnet grundsätzlich das Verfolgen von Daten über mehrere Geräte hinweg. Es kann festgestellt werden, welches Equipment wie Personal Computer, Notebook, Tablet, Smartphone oder Smart-TV, zu welchem User gehört und von diesem verwendet wird.

## 2 Tracking im Internet

*“On the Internet, nobody knows you’re a dog.”<sup>1</sup>*

Das Cartoon von Peter Steiner, das am 5. Juli 1993 im The New Yorker publiziert wurde, wo zwei Hunde vor einem Computer sitzen und einer zum anderen sagt: *“On the Internet, nobody knows you’re a dog.”*, hat sich zu einer Bild-Ikone und Redensart für Privatsphäre im Internet entwickelt.

Heutzutage hat das Cartoon an Gültigkeit verloren, denn aufgrund ausgereifter Trackingtechniken ist es Unternehmen mittlerweile möglich zu eruieren, welche Person welches Gerät zum Surfen im Internet einsetzt und welche Websites damit aufgerufen werden.

Im folgenden Kapitel wird erklärt, was man unter Internet-Tracking versteht, welche personenbezogenen und technischen Daten beim Internetsurfen von Anwendern in Erfahrung gebracht werden können, was der Unterschied zwischen First- und Third-Party-Tracking ist und welche grundlegenden Einsatzgebiete es für Tracking gibt: Kriminalitätsbekämpfung, Website-Analyse und User-Profilung bzw. Online-Marketing. Es wird ein Überblick über die Entwicklung der gegenwärtig bekanntesten Tracking-Technologien, unter anderem HTTP-Cookies, Fingerprinting oder Tracking über Social-Media-Plug-ins, gegeben. Am Ende des Kapitels wird auf konkrete Risiken, die durch Tracking entstehen können, wie etwa Preismanipulation, Personenscoring oder die Entwicklung einer Filterblase, aufmerksam gemacht.

---

<sup>1</sup>Zitat von [Peter Steiner 1993], Cartoon in The New Yorker

## 2.1 Was ist Internet-Tracking und wofür wird es eingesetzt?

Die englische Phrase "to track somebody" bedeutet übersetzt "jemanden verfolgen/ folgen/ rückverfolgen". Unter Internet-Tracking versteht man grundlegend das Verfolgen des Surfverhaltens eines Internetusers mit anschließendem Speichern, Analysieren und Auswerten der Daten. Das Tracking muss dabei nicht auf eine einzelne Website begrenzt sein, sondern es ist vielmehr üblich, einen User über mehrere Websites hinweg zu "tracken", sprich zu verfolgen, um Daten über ihn und seine Surfgewohnheiten zu sammeln. Die Surfgewohnheiten lassen wiederum auf die Vorlieben einer Person schließen. Interessen, Konsumverhalten, Lebensumstände, Alter, familiäre Situation, Wohnsitz, Arbeitsplatz, Bildungsgrad, soziales Umfeld, Religionszugehörigkeit, sexuelle Orientierung oder politische Einstellung können erfasst werden. Daraus werden detaillierte Personenprofile erstellt, die anschließend monetarisiert werden können.

Tracking findet unbemerkt vom Benutzer im Hintergrund statt und steht oft nicht im Kontext mit der eigentlichen Anwendung des Users. Dieser ist sich selten bewusst, dass seine Handlungen im Internet dazu verwendet werden, um zusätzliche Daten über ihn zu generieren.

Durch die Verwendung einer Suchmaschine erhält der Anwender passend zu seiner Suchanfrage eine Ergebnisliste mit relevanten Links. Die Suchmaschine wiederum kann die eingegeben Suchbegriffe für eigene Zwecke auswerten und zum Beispiel Werbung passend zur abgesetzten Suche anzeigen. Mit dem Einblenden von Werbeanzeigen verdient die Suchmaschine Geld, zusätzlich, wenn der User die Werbung anklickt. Beim Öffnen der Suchtreffer oder der Werbeanzeigen werden weitere Informationen über den User gesammelt. Einerseits vom Erstanbieter, der Suchmaschine, andererseits von einem Drittanbieter, jenem Unternehmen, das die Werbeanzeige schaltet. Die Unterscheidung zwischen "First-Party-Tracking" und "Third-Party-Tracking" wird im übernächsten Absatz erklärt.

Social-Media-Plattformen dienen unter anderem zur Vernetzung und zum Informationsaustausch der Nutzer. Wenn sich eine Person bei einer Social-Media-Plattform registriert, erhält diese Grunddaten zur Person, wie Geburtsdatum oder Klarnamen, sofern Echt-daten angegeben werden. Durch die Benutzung der Plattform entstehen weitere Daten, die dazu beitragen, dass genaue Details über Mitglieder in Erfahrung gebracht werden können. Außerhalb der Plattform kann diese Datenmenge über integrierte Social-Media-Plug-ins auf fremden Websites, wie etwa Facebooks Like-Button, vermehrt werden.

Es ist zu unterscheiden, ob ein User freiwillig Daten zur Verfügung stellt, weil er diese aktiv preisgibt oder ohne sein Wissen Daten erfasst werden.

Zum Beispiel werden beim Registrieren, beim Ausfüllen von Online-Formularen, bei der Beteiligung an Gewinnspielen oder beim Online-Shopping Personendaten bewusst mitgeteilt.

Mittels Tracking können mitunter folgende technische Daten unbemerkt von einem Internetbenutzer erfasst werden, ohne dass diese durch dessen selbstständige Dateneingabe bekannt gegeben wurden:

- IP-Adresse, Internetanbieter
- Browsertyp und -version, Browsersprache, installierte Browser-Plug-ins
- Betriebssystem, Hardwaredaten, Geräte-ID, Bildschirmauflösung
- Gerätestandort bzw. genaue GPS-Daten, Datum, Uhrzeit, Zeitzone
- HTTP-Referrer (URL, der zuvor besuchten Webseite) oder gesamte Browser-Chronik
- Verweildauer, welche Unterseiten geöffnet werden, welche Anzeigen/ Artikel/ Inhalte angeklickt wurden, von welcher Seite aus die Website verlassen wird

Es wird zwischen "First-" und "Third-Party-Tracking" unterschieden. First-Party-Tracking wird von der vom User initial aufgerufenen Website ausgeführt. Dabei untersucht der Website-Betreiber ausführlich, wie sich ein Besucher auf dessen Webseiten verhält bzw. sein Online-Angebot nutzt.

Ein Online-Shop wird zum Beispiel Informationen darüber sammeln, wie sich ein Kunde in seinem "Geschäft" bewegt, welche Produkte angesehen werden, welche davon am häufigsten verkauft werden, welche Subseiten des Online-Shops bevorzugt aufgerufen werden oder welche Preis-Aktionen erfolgreich sind. Mit Hilfe dieser Daten kann der Online-Shop versuchen sein Angebot zu verbessern und dadurch im Best-Case-Szenario größere Umsätze erzielen. Anhand der Analysen kann er sich dazu entschließen Artikel anders zu platzieren, um deren Verkaufschancen zu erhöhen oder er kann seinen Kunden ihren Interessen entsprechende Newsletter mit Angeboten zusenden. Ein Kunde, der zum Beispiel hauptsächlich Sportartikel aufruft bzw. einkauft wird eher auf Werbemails zu Sportprodukten reagieren, als auf jene, die etwa Babywaren bewerben.

Ein konkreteres Beispiel ist Google, dessen Kernkompetenz die Auswertung seiner Userdaten ist. Ein Ergebnis davon ist etwa der Dienst "Google-Trends". "*Google Trends analysiert einen prozentualen Anteil der Suchanfragen in der Google Websuche, um die Anzahl der Suchanfragen in einem bestimmten Zeitraum zu ermitteln.*"<sup>2</sup> Dadurch werden aktuelle Such-Trends und Interessen zu bestimmten Themen sichtbar.

Third-Party-Tracking wird von Drittanbietern, die innerhalb der eigentlich besuchten Internetseite ("First-Party") eingebettet sind, durchgeführt. Zum Beispiel über einen auf den einzelnen Seiten integrierten Code eines Website-Analyse-Dienstes, der Daten über die Benutzung dieser Seiten sammelt, wie es etwa bei Google Analytics der Fall ist. Details zur Verbreitung von Google Analytics weltweit, zu Konkurrenz-Anbietern und zur Website-Analyse im Allgemeinen, werden im Unterkapitel *2.1.2 Website-Analyse* auf Seite 11 dargestellt.

Ein weiteres Beispiel für einen integrierten Code ist das Einbetten von Social-Media-Plug-ins, wie es im Unterkapitel *2.2.12 Tracking durch Social-Media-Buttons* ab Seite 41 beschrieben wird.

Neben dem integrierten Code geht Third-Party-Tracking auch von referenzierten Inhalten aus, die Teil der eigentlich geladenen Webseite sind, wie zum Beispiel Bilder, Videos, Spiele oder Werbeanzeigen, die wiederum von externen Quellen auf der ursprünglichen Seite geladen und angezeigt werden. Diese externen Inhalte können Tracking-Mechanismen enthalten, welche zwar über die Erstanbieter-Seite initialisiert wurden, aber von Drittanbietern stammen und von diesen ausgewertet werden.

Bei Werbeanzeigen kann der Drittanbieter zum Beispiel messen wieviele eindeutige User diese Anzeige angeklickt oder gesehen haben und berechnet daraus den Verdienst des Erstanbieters.<sup>3</sup>

Drittanbieter können durch Third-Party-Tracking die Aktivitäten von Internetbenutzern über alle Websites hinweg, die den Drittanbieter einsetzen, verfolgen und Daten sammeln. Anhand von Tracking-Merkmalen, wie etwa gesetzten Cookies oder das Auslesen von Geräte-IDs, können Drittanbieter Internetuser individualisieren und auf unterschiedlichen Websites wiedererkennen, wodurch sie deren Surfverhalten mitverfolgen und analysieren können. Die gesammelten Daten werden zur Erstellung ausführlicher Benutzerprofile herangezogen, welche für verschiedene Zwecke, wie zum Beispiel dem Platzieren personalisierter Werbeanzeigen, vermarktet werden.

---

<sup>2</sup>vgl. [Google 2016d]

<sup>3</sup>vgl. [McKinley Kate 2008]

Es wird nicht ausschließlich First- oder Third-Party-Tracking eingesetzt. Meistens werden beide Varianten kombiniert, oftmals sind mehrere verschiedene Drittanbieter gleichzeitig aktiv. Besonders lukrativ können Daten gesammelt werden, wenn ein Dienstleister einerseits First- und andererseits Third-Party-Tracking betreibt. Hier ist es für Firmen von Vorteil, wenn sie als Erstanbieter eine Dienstleistung anbietet, wo zur Anwendung ein Konto erstellt werden muss. So werden bereits bei der anfänglichen Registrierung durch den User viele interessante Personendaten preisgegeben und vom jeweiligen Dienstleister in Erfahrung gebracht. Je mehr Mitglieder dieses Unternehmen für sich gewinnen kann, umso besser. Weiters muss es zusätzliche Services bereitstellen, die auf zahlreichen externen Webangeboten integriert werden können. So kann das Unternehmen über das ursprüngliche Angebot im Internet hinaus weitere Daten ermitteln.<sup>4</sup>

Facebook sammelt zum Beispiel als Erstanbieter Daten über seine Mitglieder, die bei Facebook angemeldet sind und das Netzwerk nutzen. Als Drittanbieter aggregiert es Daten mittels aller Websites, die Facebooks Social-Plug-ins, wie den Facebook-Like-Button, installiert haben.

Google bietet mehrere Dienste als Erstanbieter an, wie Google Mail oder Google-Plus, wo das Anlegen eines Kontos notwendig ist. Als Drittanbieter ist Google zum Beispiel durch Google Analytics, den Google-Plus-Button oder Googles Werbedienst AdSense bei einer Vielzahl von Google unabhängigen Websites integriert und kann so sein Datenmonopol stetig ausbauen.

Ein Internetnutzer muss sich bewusst sein, dass im Prinzip sein gesamtes Surfverhalten protokolliert und ausgewertet werden kann. Die Recherche zu dem Thema Internet-Tracking hat gezeigt, dass folgende drei Bereiche wesentlich sind:

- Kriminalitätsbekämpfung im Internet zum Schutz des Users
- Website-Analysen, die auswerten, welche Inhalte für Besucher interessant sind, welche Beiträge angeklickt werden oder welche Produkte Gefallen finden. So können Webauftritte benutzerfreundlicher gestaltet bzw. verbessert werden.
- User-Profiling und Online-Marketing: Detaillierte Benutzerprofile dienen dazu personalisierte Werbung zu platzieren und helfen bei der Vermarktung von Produkten und deren Verkauf.

---

<sup>4</sup>vgl. [Schneider et al. 2014]



### 2.1.1 Bekämpfung von Internet-Kriminalität

Wie Geheimdienste oder Behörden Tracking zur Kriminalitätsbekämpfung einsetzen, ist nicht Teil dieser Diplomarbeit. Daher werden Themen wie die Aufdeckungen von Edward Snowden oder die Vorratsdatenspeicherung in Österreich oder im Allgemeinen nicht weiter erläutert.

Daten, die durch Web-Tracking generiert werden, finden im Risikomanagement Verwendung. Sie dienen zum Beispiel dazu, Online-Betrug aufzudecken oder Kunden zu authentifizieren. Banken setzen Tracking-Techniken ein, um die Datensicherheit bei Transaktionen zu gewährleisten oder um Kunden wiederzuerkennen und sicherzustellen, dass sich Betrüger nicht als bereits vorhandene Kunden ausgeben. Diese Vorgehensweise kann bei allen Dienstleistungen zur Anwendung kommen, wo ein Login benötigt wird. So können etwa IP-Adressen oder Geräte-IDs als gefährlich eingestuft und von Unternehmen blockiert werden.<sup>5</sup>

Facebook protokolliert etwa von welchem Standort, mit welchem Gerät, welchem Browser und welchem Betriebssystem auf ein Facebook-Konto zugegriffen wird. Untypische Logins meldet Facebook beim User und fordert eine Bestätigung des Zugriffs. Einerseits ist dies ein praktisches Feature und schützt vor unerlaubten Zugriffen auf Facebook-Konten und vor Identitätsdiebstahl. Bei kritischer Betrachtung zeigt es andererseits deutlich auf, welche zusätzlichen Merkmale von einem Mitglied gespeichert und ausgewertet werden. Datenschutzfreundlicher wäre es, es dem User zu überlassen, ob er eine Sicherheitsvorkehrung dieser Art aktivieren oder lieber das Risiko einer fremden Nutzung seines Kontos eingehen möchte.

---

<sup>5</sup>vgl. [Ramirez et al. 2014]

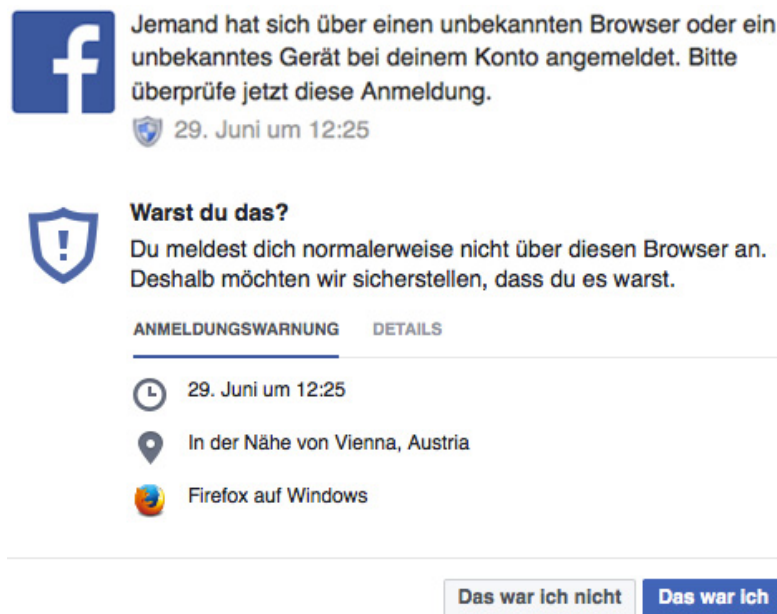


Abbildung 2.1: Die Grafik zeigt einen Screenshot der User-Authentifizierung bei Facebook.

Bildquelle vgl. [Facebook 2016][Mitteilung bei einem privaten Facebook-Konto]

### 2.1.2 Website-Analyse

Im Allgemeinen wird bei der Website-Analyse das Surfverhalten einer Person während des Besuchs einer Website untersucht. Dabei können unter anderem folgende Daten vom Website-Betreiber ermittelt und statistisch ausgewertet werden<sup>6</sup>:

- Einstiegsseite, Ausstiegsseite, Referrer
- IP-Adresse, Browser, installierte Add-ons
- Betriebssystem, Bildschirmauflösung, Geräte-ID
- Sprache, Land, Datum, Uhrzeit
- Aufenthaltsdauer auf einzelnen Webseiten und gesamt, welche Subseiten geöffnet werden, Ladezeiten
- bei Websites mit Suchfunktionen die eingegebenen Suchbegriffe, welche Suchen Null Treffer erzielen
- neue oder wiederkehrende User, Anzahl der Besucher pro Seite/ pro Tag

<sup>6</sup>vgl. [Google Analytics 2016]

- Downloads, Klickraten, welche Werbeanzeigen/ Artikel/ Inhalte geöffnet werden, welche Social-Media-Plug-ins genutzt werden, welche Inhalte geteilt werden
- Mausbewegungen, Tastatureingaben, Usernavigation auf der Website
- Konversionsraten, zum Beispiel wie viele Interessenten registrierte Kunden oder Käufer werden
- Abbruchraten, zum Beispiel wieviele Kunden Produkte in einen Warenkorb legen, aber keine Bestellung tätigen bzw. den Bestellvorgang abbrechen

Statistiken über die Nutzung einer Website helfen den Betreibern dabei, so viel wie möglich über seine Benutzer bzw. Kunden zu erfahren. Durch die gesammelten Informationen kann der Webauftritt verbessert und die Zugriffsraten erhöht werden. Es kann in Erfahrung gebracht werden, wofür sich Besucher im Detail interessieren und welche Inhalte besonders beliebt sind. Das Zielpublikum kann so wirksamer angesprochen, Inhalte/ Produkte/ Werbeanzeigen können besser platziert und somit gewinnbringender vermarktet werden. Der Erfolg oder Misserfolg von Marketingkampagnen kann gemessen werden. Probleme, zum Beispiel beim Aufbau oder Laden der Website, bei der Navigation oder bei Bestellprozessen, können rascher erkannt und dementsprechend behoben werden.<sup>7</sup>

Analyse-Tools können vom Websitebetreiber eigenständig entwickelt oder mittels Code von Drittanbietern in den Webauftritt integriert werden, wie es zum Beispiel bei der Verwendung des weltweit erfolgreichsten Dienstleisters, Google Analytics, der Fall ist. Laut einer Statistik von W3Techs<sup>8</sup> verwenden 34,5% der laut Alexa zehn Millionen weltweit meistbesuchten Websites keine Drittanbieter zur Analyse ihrer Website. Ungefähr 54% aller untersuchten Websites setzen Google Analytics zur Website-Traffic-Analyse ein, womit Google weltweit einen Marktanteil von ca. 83% erreicht. Wie in der anschließenden Grafik zu sehen ist, lässt Google Analytics seine Konkurrenten weit hinter sich. Nur ca. 1-5% der geprüften Websites verwenden andere Anbieter unter den Top 10. Das einzige Open Source Website-Analyse-Tool Piwik befindet sich auf Platz 7 der Top 10 und hält einen Marktanteil von 2%.<sup>9</sup>

---

<sup>7</sup>vgl. [Google Analytics 2016]

<sup>8</sup>W3Techs ist ein Dienstleistungsangebot des österreichischen Unternehmens Q-Success, das Informationen über derzeit eingesetzte Internettechnologien sammelt, auswertet und die Ergebnisse online zur Verfügung stellt. Dazu analysiert W3Techs zehn Millionen, der laut Alexa meistbesuchten Websites weltweit in einem Zeitraum der jeweils letzten drei Monate. Die Berichte werden täglich aktualisiert.

<sup>9</sup>vgl. [W3Techs 2016b]

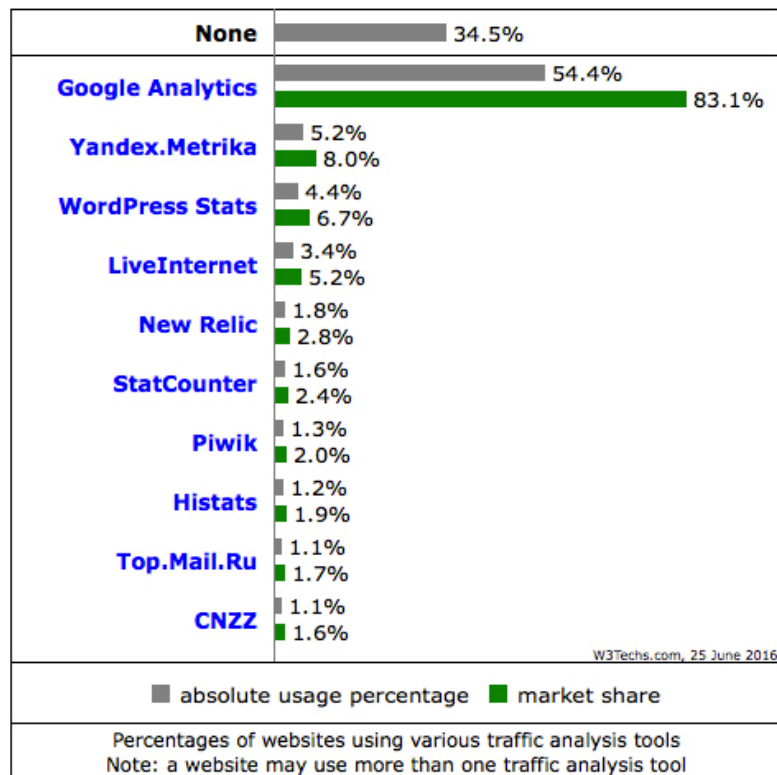


Abbildung 2.2: Die Grafik zeigt eine Statistik von W3Techs von der weltweiten Verbreitung der Top 10 Anbieter von Website-Analyse-Tools.

Bildquelle vgl. [W3Techs 2016b]

Laut Datenschutzgesetz müssen User über den Einsatz von Trackingtechniken, wozu auch eine Website-Analyse zählt, informiert werden. Datenschutzkonforme Website-Analyse-Tools anonymisieren automatisch die IP-Adresse des Besuchers, bieten ein Opt-Out von der Analyse an und ermöglichen das Speichern aller generierten Daten und Statistiken auf eigenen, vom Tool unabhängigen Servern.

Das deutsche Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein veröffentlichte im März 2011 eine Empfehlung für den Einsatz des Open Source Website-Analyse-Tools Piwik.<sup>10</sup> Wohingegen Google Analytics 2008<sup>11</sup> und 2009<sup>12</sup> als *„datenschutzrechtlich unzulässig“* beurteilt wurde.

<sup>10</sup>vgl. [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2011]

<sup>11</sup>vgl. [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2008]

<sup>12</sup>vgl. [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2009]

Seit Mai 2010 bietet Google Analytics die Anonymisierung von IP-Adressen und ein Browser-Add-on, das ein persistentes Opt Out ermöglicht, an.<sup>13</sup> Alle generierten Daten werden jedoch auf Google Servern in den USA gespeichert. Die rechtlichen Rahmenbedingungen bezüglich Internet-Tracking werden detailliert im Unterkapitel 3.1 *Gesetzliche Maßnahmen* ab Seite 67 erörtert.

Welche der in dieser Diplomarbeit untersuchten, österreichischen Websites Drittanbieter zur Website-Traffic-Analyse installiert haben, wird im Unterkapitel 4 *Tracking-beispiele in Österreich* ab Seite 130 aufgelistet.

### 2.1.3 User-Profiling und Online-Marketing

User-Profiling bedeutet das Erstellen möglichst detaillierter Persönlichkeitsprofile. Dazu werden einerseits verschiedene Tracking-Technologien eingesetzt, die das Surfverhalten einer Privatperson im Internet erfassen, und daraus so viele Daten wie möglich lukrieren. Andererseits werden dafür konkrete Personendaten herangezogen, die User selbst angeben, zum Beispiel bei einer Registrierung auf einem Webportal.

Ein Hintergrund zur Profilbildung ist, dass je genauer ein Unternehmen seine Kunden kennenlernt, umso effektiver kann zielgruppenorientiertes bzw. personenbezogenes Marketing durchgeführt werden. Je besser eine Werbung dem potentiellen Kunden entsprechend platziert werden kann, umso höher ist ihre Wahrnehmung und Wirkung, und desto größer ist die Wahrscheinlichkeit, dass eine Werbeanzeige angeklickt, eine Produktseite aufgerufen, ein Kauf vollzogen und somit Umsatz erzielt wird.

Google und Facebook sind die prominentesten Datenmonopole, die umfangreiche Userprofile generieren und diese bekanntermaßen vermarkten und monetarisieren. Weniger geläufig sind sogenannte Data Broker. Das sind Unternehmen, die sich darauf spezialisiert haben, Datensätze über einzelne Personen in größtmöglichen Mengen zusammenzutragen, daraus aussagekräftige Profile erstellen und diese profitbringend verkaufen. Einer der größten Dienstleister in diesem Bereich ist die amerikanische Firma Acxiom, die global tätig und seit 2013 auch ein Marketingpartner von Facebook ist. Das bedeutet, dass Facebook seine Daten mit jenen von weiteren Drittanbietern zusammenführt, um Zielgruppen noch genauer anzusprechen und Werbeanzeigen noch besser zu platzieren.<sup>14</sup>

---

<sup>13</sup>vgl. [Amy Chang 2010]

<sup>14</sup>vgl. [Facebook 2013]

Die New York Times berichtet 2012 in einem umfassenden Artikel über Acxiom, dass das Unternehmen weltweit Daten von über 500 Millionen Konsumenten mit ca. 1.500 Einträgen pro Person besitzt und mehr über Einzelpersonen weiß, als etwa die zentrale amerikanische Sicherheitsbehörde, das FBI. So lieferte Acxiom zum Beispiel nach den Terroranschlägen in den USA am 11. September 2001 hilfreiche Informationen zu 11 der 19 Flugzeugentführer und arbeitete diesbezüglich eng mit der Regierung zusammen.<sup>15</sup>

Die 1.500 Einträge pro Person sind eine Kombination aus Offline- und Online-Daten und enthalten beispielsweise Angaben zu folgenden Parametern: Adresse, Haushalt (ob Miete oder Eigentum), Alter, Geschlecht, Gewicht, Größe, Beruf, Arbeitsplatz, Einkommen, Kapital, Schulden, Kredite, Zahlungsfähigkeit, Bildung, Akademischer Titel, Sprachkenntnisse, politische Einstellung, freiwilliges Engagement, Religion, Familienstand, Beziehungsstatus, Kinder, Gesundheitszustand, Krankenversicherung, andere Versicherungen, Konsumverhalten, Kundenkarten, tätigt Online-Einkäufe, Hobbys, Interessen, Vorlieben, Zeitschriftenabonnements, Lebensstil, ausgeübte Sportarten, Radfahrer, Autofahrer, E-Mailadresse, IP-Adresse, Geräte-ID, Telefonnummer, Browser, Betriebssystem, Besitzer eines Computers/Laptops/Tablets/Smartphones, installierte Apps, Facebook-/Twitterprofil.<sup>16</sup> Es ist davon auszugehen, dass die Gesamtdatenmenge und die einzelnen Datensätze pro Person seit 2012 stark zugenommen haben und weiterhin laufend anwachsen.

Die anschließende Grafik zeigt eine zweiseitige Werbeanzeige von Acxiom für Direktmarketing, die speziell für den amerikanischen Markt im Sommer ausgerichtet ist. Sie lässt erahnen, auf welche Datenvielfalt Acxiom und seine Kunden Zugriff haben.

---

<sup>15</sup>vgl. [Natasha Singer 2012]

<sup>16</sup>vgl. [Acxiom 2016a]

# AMERICANS ARE PACKING UP. ARE YOU CASHING IN?

Reach a huge market with summertime audiences from Acxiom. Summer travel and purchases for related activities represent billions in spending. Precisely target your client's message at the right time and in the right place.



To find out how these targeted groups can pay off big this summer, contact [dataguru@acxiom.com](mailto:dataguru@acxiom.com) or call 888.3ACXIOM.



### Camping/Glamping

Families that love to camp and hike are often big spenders when it comes to summer travel and spending. Connect directly with an audience as high as 5 million that camp or have an RV with this segment.

### Waterparks and Swimming

Want to know who is going to dive into the local pool or pack up and head to the nearest waterpark. As many as 16 million Americans will do just that this summer. Help them make the right choices on destination and supplies.

### Stay-cation

A recent survey about summer travel indicated that 1/3 of the respondents are planning on enjoying summertime fun a little closer to home. If you represent a client with local attractions, this audience of over 8 million Americans is the perfect match.

### Beach Travelers

As many as 66% of summer vacationers will head to the beach during the months of June to August. But before they put their toes in the sand, they'll be busy researching the best condos, hotels and airfares, as well as stocking up on essentials for their vacation. Let us help you get your message directly in front of this group that numbers over 11 million.

### Space and Specialty Kids Camps

Space camp and other special interest camps for kids are a large and growing market. With counts as high as 8 million, our data helps you reach this prime pool of parents.

### Active Kids Camps

Kids and their parents are still making important decisions about choosing a summer camp to attend. If your client is looking to reach this market with counts as high as 3 million, with information about camps or gear that kids will take to camps, this segment is a great fit.

### International Travelers

A huge number of Americans will actually venture outside our borders for their summer getaway this year. But before they do, they'll not only research and purchase airfare and book accommodations but they also fill their suitcases with apparel and accessories vital to their plans. Connect with this audience of over 15 million.

### Outdoor Family Fun

In addition to what will be spent on travel, a huge amount of money will be used by families on grills, cookouts and other outdoor activities. This market is ideal for clients interested in selling seasonal items related to outdoor fun.

### Boating and Sailing

When the temperatures rise, so does the number of customers interested in hitting the water in a boat or sailboat. Reach those ready to make a major purchase this summer.

### Gardening and Home Improvement

Lots of Americans embark on major garden and home improvement projects during the summertime. Reach avid gardeners and DIYers looking for tools, plants and other supplies.



Abbildung 2.3: Die Grafik zeigt eine Werbeanzeige von Acxiom. Diese beschreibt, welche Daten für amerikanische Zielgruppen im Sommer genutzt werden können.

Bildquelle vgl. [Acxiom 2016b]



Wie Unternehmen wie etwa Acxiom durch Online-Tracking das Surfverhalten von Personen ausspionieren und anschließend für Werbezwecke nutzen, beschreibt die anschließende Grafik des Wall Street Journals aus der investigativen Artikelserie "What They Know".<sup>17</sup>

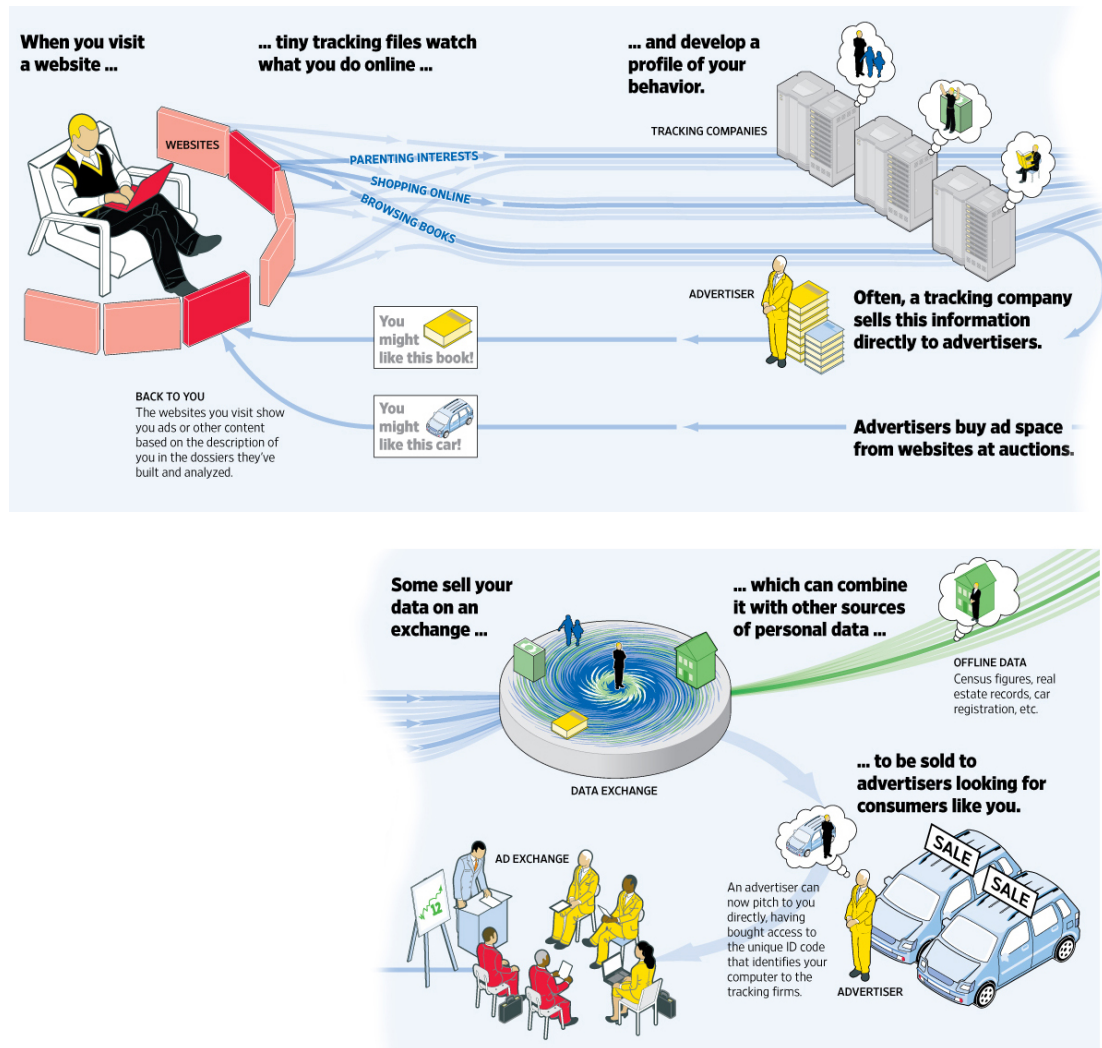


Abbildung 2.4: Die Grafik des Wall Street Journals aus der Reihe "What They Know" beschreibt den Kreislauf des Trackings zwischen Internetanwender, Tracking-Unternehmen und der Werbeindustrie.

Bildquelle vgl. [The Wall Street Journal 2010]

<sup>17</sup>Die amerikanische Tageszeitung The Wall Street Journal recherchierte von 2010-2012 ausgiebig zum Thema Tracking und brachte dazu eine eigene Serie von zahlreichen, informativen Artikeln mit dem Übertitel "What They Know" heraus. 2012 war das ausführende Team des Wall Street Journals für ihre herausragende Leistung der Hintergrundberichterstattung unter den Finalisten des Pulitzer Preises.

So wie sich Offline-Medien wie Fernsehen, Radio und Print mit Werbeschaltungen finanzieren, finanzieren sich auch Webauftritte mittels Werbung. Oft ist Werbung die einzige Einnahmequelle. Aufgrund der Einnahmen über Werbeanzeigen steht ein Großteil beliebter Internetdienste gratis zur Verfügung. Dabei sollte die Formulierung "gratis" kritisch hinterfragt werden. Webdienstleister sammeln im Gegenzug zur freien Nutzung ihres Angebots Userdaten, die zur umfangreichen Profilerstellung und anschließenden Vermarktung herangezogen werden. Im Unterschied zu Offline-Werbung, wo je nach Sendezeit, Art der Ausstrahlung oder Form des Printmediums ein bestimmtes Zielpublikum angesprochen wird, ist es online möglich, Reklame zu individualisieren und auf potentielle Kunden genau anzupassen.

Verteidiger personenbezogener Werbung befürworten den Umstand, dass Einzelpersonen relevantere und ansprechendere Werbeinformationen erhalten, sich weniger von der Werbung belästigt fühlen, die Wahrscheinlichkeit des Anklickens und eines potentiellen Kaufs steigt und der Werbekonsum das jeweilige Webportal besser unterstützt.<sup>18</sup>

Gegner kritisieren die Praktiken des Online-Profilings und -Marketings an sich und sehen den Vorgang als einen massiven Eingriff in die Privatsphäre. Nicht die Kundenanfragen nach einem bestimmten Produkt sind ausschlaggebend für die Darstellung einer Werbeanzeige, sondern aufgrund von zuvor gesammelten Informationen über eine Person werden Waren angeboten.<sup>19</sup>

Ein Beispiel, wo Profiling und das Vorschlagen weiterer Produkte teilweise nicht wie gewünscht funktioniert, ist Amazon. Der Algorithmus kann noch nicht erkennen, ob man Waren für sich selbst oder als Geschenk für andere Personen erwirbt. Alle Einkäufe werden jedoch für neue Empfehlungen herangezogen. Ein Amazonkunde kann darauf keinen Einfluss nehmen, indem er zum Beispiel sein Amazonprofil editiert.

Aussagen der Art *"Wenn schon Werbung, dann lieber eine, die auf mich zurechtgeschnitten ist und nicht nervt."* bzw. *"Es ist ja nur Werbung!"* sind zu relativieren. Detaillierte Personenprofile werden nicht nur für Werbezwecke eingesetzt (siehe Kapitel 2.3 *Gefahren durch Tracking* ab Seite 54). Durch die Auswertung gesammelter Userdaten können Unternehmen weit mehr in Erfahrung bringen, als Einzelpersonen zunächst bewusst ist.

---

<sup>18</sup>vgl. [Network Advertising Initiative 2016]

<sup>19</sup>vgl. [Constanze Kurz und Frank Rieger 2011]

Ein Artikel des Wall Street Journals aus 2009 berichtet zum Beispiel über Google, das versucht mittels einer Auswertung von gespeicherten Mitarbeiterdaten vorherzusagen, welche Angestellten demnächst das Unternehmen verlassen möchten. Aufgrund der Ergebnisse werden von Google konkrete Gegenmaßnahmen gesetzt, um kein vielversprechendes Mitarbeiterpotential zu verlieren.<sup>20</sup>

## 2.2 Tracking-Technologien

*“We’ve lost the technology fight.  
There are just too many ways to track people.”<sup>21</sup>*

Da es eine große Anzahl an Trackingtechniken gibt, die laufend erweitert und weiterentwickelt werden, kann in der vorliegenden Arbeit keine vollständige Liste an Technologien angeführt werden. Im Anschluss wird daher eine grobe Übersicht über die derzeit bekanntesten Trackingpraktiken im Internet gegeben. Die meisten Methoden können von Erst- und/ oder Drittanbietern praktiziert werden.

### 2.2.1 HTTP-Cookie

HTTP-Cookies sind kleine Dateien, die geringe Zeilen Text enthalten, welcher spezifisch für den User und die geladene Internetseite ist. Sie werden beim Aufrufen einer Webseite clientseitig auf dem jeweiligen Rechner des Users gespeichert und beim neuerlichen Laden jener Seite wieder erkannt. Cookies wurden ursprünglich kreiert, um den Inhalt des Warenkorbs über die Dauer des Einkaufs in einem Web-Shop zu speichern und einem bestimmten User zuzuordnen. Diese sogenannten ”Session-Cookies” werden weiters zur Speicherung von Login-Informationen verwendet und werden nach dem Verlassen der Website bzw. dem Schließen des Browsers vom Computer entfernt, da sie nicht mehr benötigt werden. ”Persistent-Cookies” dienen zum Hinterlegen von persönlichen Einstellungen, die dauerhaft angelegt werden und langfristig abrufbar sein sollen. Zum Beispiel kann bei Suchmaschinen die Such- oder Anzeigesprache konfiguriert werden oder es werden automatische Logins mit ihrem Einsatz ermöglicht.

---

<sup>20</sup>vgl. [Scoot Morrison 2009]

<sup>21</sup>Zitat von [Mayer Jonathan 2011c], What You Can Do About the New Web Tracking Tools

Cookies sind das älteste, einfachste und am weitest verbreitete Grundelemente für Web-Tracking. Bei Webanalysen lässt sich beispielsweise mit ihrer Hilfe feststellen, wie frequentiert eine Website ist, wieviele Besucher sie hat, welche Unterseiten geöffnet werden und welche Links angeklickt werden. Dies dient nicht nur der Verbesserung des Online-Auftritts einer Website. Mit den gesammelten Informationen kann das Surfverhalten eines Internetusers nachvollzogen werden, womit wiederum detaillierte Benutzerprofile erstellt werden können. Jede geöffnete Seite, jeder Mausklick, wie zum Beispiel das Anklicken einer Werbeanzeige, kann mittels Cookies identifiziert, archiviert und ausgewertet werden.<sup>22</sup> Mittels Einstellungen im jeweiligen Browser<sup>23</sup> kann ein Anwender das Verhalten von Cookies beeinflussen. Aufgrund der EU-Richtlinie 2002/58/EG, die in Österreich durch das Telekommunikationsgesetz 2003 umgesetzt wurde<sup>24</sup>, sind Betreiber von Websites oder anderen Online-Angeboten dazu verpflichtet, auf den Einsatz von Cookies aufmerksam zu machen und genaue Informationen dazu anzubieten.

Eine Studie aus 2015 hat ergeben, dass Google die Vorherrschaft hat, wenn es um die Verbreitung von Tracking-Cookies geht. Zählt man alle Unternehmen bzw. Dienste des Google-Universums wie Google Analytics, DoubleClick, Google Mail, Google Maps, Google Plus oder etwa YouTube zusammen, so erlangt Google eine Tracking-Flächendeckung von 92% auf den laut Quantcast<sup>25</sup> 100 und 1.000 meistbesuchten, us-amerikanischen Interneteiten, und 73,5% auf den 25.000 populärsten Websites. Somit kennt Google das Surfverhalten eines Users fast genau so detailliert wie der jeweilige Internetprovider.<sup>26</sup>

Im Zuge der Diplomarbeit wurde die Version der Google-Datenschutzbestimmungen vom 19. August 2015 auf eingesetzte Trackingtechniken und etwaige Opt-Out-Möglichkeiten hin untersucht. Die Datenschutzerklärung ist sehr umfangreich und wird auf Dauer durch das Laden mehrerer Unterseiten unübersichtlich, der Leser verliert den Überblick. Sie bezieht sich hauptsächlich auf Daten in Verbindung mit einem angemeldeten Google Konto, wo es detaillierte Kontrollmöglichkeiten gibt. Nutzt der User Google-Dienste unangemeldet, hat er kaum Einfluss auf selbst generierte Daten. Die Datenschutzbestimmungen gelten für alle Google-Produkte, manche, wie zum Beispiel Google Chrome, haben zusätzliche Anforderungen, die vom Anwender separat berücksichtigt

---

<sup>22</sup>vgl. [Verbraucher sicher online 2011]

<sup>23</sup>Siehe Kapitel 3.3.1 *Einstellungen im Browser* ab Seite 111.

<sup>24</sup>Siehe Kapitel 3.1.2 *Telekommunikationsgesetz* auf Seite 71.

<sup>25</sup>Quantcast ist ein internationales Technik-Unternehmen mit Sitz in San Francisco, USA, das sich auf die Analyse von Internet-Datenverkehr auf konkreten Websites und darauf aufbauend auf zielgerichtete Werbeplatzierung spezialisiert hat.

<sup>26</sup>vgl. [Altaweel et al. 2015]

werden müssen. Es ist für den User nicht ersichtlich, für welche Google-Dienste die Datenschutzregeln ausdrücklich gelten, es gibt dazu keine genaue Auflistung. Google speichert Daten mittels Cookies oder ähnlicher Technologien. Es wird nicht näher darauf eingegangen, was genau ähnliche Technologien sind. Mögliche Privatsphäre-Einstellungen außerhalb des Google-Kontos werden mittels Cookies gespeichert, die hinfällig werden, wenn zum Beispiel der Browser beim Beenden alle Cookies löscht. Google bietet Browser-Add-ons für Google Analytics (für Google Chrome, Firefox, Internet Explorer, Safari und Opera) und DoubleClick (nur für Google Chrome, Firefox und Internet Explorer) an, welche die jeweiligen Opt-Out-Cookies dauerhaft speichern. Google zeigt keine Versionshinweise bei den Add-ons an, wodurch unklar ist, wie aktuell sie sind.<sup>27</sup>

Es bestehen drei Möglichkeiten sich von durch Google personalisierter Werbung abzumelden: als Einstellung innerhalb eines angemeldeten Google-Kontos, mittels Opt-Out-Cookie auf Websites, wo mittels Google Werbeanzeigen platziert werden oder mittels Opt-Out-Cookie bei der Anwendung der Google-Suche. Damit die letzteren zwei Varianten dauerhaft beibehalten werden können, dürfen Cookies vom Browser nicht gelöscht werden.<sup>28</sup> Die dadurch entstehende Problematik wird im Kapitel *3.2.3 Selbstregulierungs-Systeme* ab Seite 103 beschrieben.

### 2.2.2 Flash-Cookie

Flash-Cookies, auch "Local Shared Objects (LSOs)" genannt, werden durch den Adobe Flash Player generiert, der bei den meisten Benutzern im jeweiligen Browser als Plug-in installiert ist, um Flash-Inhalte wie Animationen, Filme oder Spiele auf Internetseiten anzuzeigen.<sup>29</sup>

Eine Studie der Berkeley Universität hat ergeben, dass Flash-Cookies gegenüber HTTP-Cookies einige Vorteile besitzen, die es vereinfachen, die Aktivitäten der Interneter im Netz zu verfolgen. Sie besitzen kein Ablaufdatum, weshalb sie, wenn man sie nicht manuell löscht, permanent am Computer gespeichert bleiben. Sie können eindeutige User-IDs erzeugen. Zum Speichern von Informationen stehen 100KB zur Verfügung, bei einem Standard-Cookie sind nur 4KB Speicherplatz vorhanden. Sie werden vom Browser unabhängig, clientseitig am Rechner des Nutzers hinterlegt. Somit können Websites auch

---

<sup>27</sup> vgl. [Google 2015b]

<sup>28</sup> vgl. [Google 2016a]

<sup>29</sup> vgl. [EPIC 2005]

von unterschiedlichen Webbrowsern aus auf bereits gesetzte Flash-Cookies zugreifen. Beim Laden einer Internetseite werden die gleichen Daten in beide Cookie-Arten, HTTP und Flash, gespeichert. So kann ein Flash-Cookie als eine Art Reservekopie fungieren, um bereits gelöschte HTTP-Cookies wiederherzustellen und die Bemühung des Users zu ignorieren, Cookies nicht zu akzeptieren. Flash-Cookies ermöglichen so ein lückenloses Usertracking. "Wiederauferstandene" Cookies werden auch als "Zombie-Cookies" bezeichnet, da sie, obwohl bereits einmal gelöscht, vom System erneut angelegt werden.<sup>30</sup> Diese vorteilhaften Eigenschaften nutzen auch andere Tracking-Technologien wie Evercookies<sup>31</sup> oder unterschiedliche Fingerprinting-Methoden<sup>32</sup>.

Ursprünglich konnten, im Gegensatz zu HTTP-Cookies, Flash-Cookies nicht über den Browser verwaltet werden. Es war somit nicht möglich, mit den üblichen Browsereinstellungen Flash-Cookies zu verhindern, denn diese bezogen sich nur auf HTTP-Cookies. Ebenso kamen Konfigurationen, die im Privatmodus des Browsers<sup>33</sup> vorgenommen wurden, bei Flash-Cookies nicht zum Greifen. Seit der Flash Player Version 10.1, die im Juni 2010 erschien, werden die Einstellungen des Privatmodus der vier gängigen Browser (Google Chrome, Mozilla Firefox, Microsoft Internet Explorer und Apple Safari) eingebunden und alle entsprechenden Flash-Elemente beim Beenden gelöscht.<sup>34</sup> Im Jänner 2011 wurde am "Flash Platform Blog" von Adobe ein Beitrag veröffentlicht, dass eine neue API (Progammierschnittstelle) spezifiziert wurde, die es ermöglicht, LSOs analog zu HTTP-Cookies über den Browser zu löschen.<sup>35</sup>

Auf der Flash-Player-Hilfeseite von Adobe gelangt man zum Menü des Einstellungsmanagers, worin zusätzliche Einträge bezüglich des Verhaltens von LSOs erstellt werden können. Unter dem Menüpunkt "Globale Speichereinstellungen" kann man die standardmäßig aktive Funktion "Zulassen, dass Flash-Inhalte von Drittanbietern Daten auf dem Computer speichern" deaktivieren.<sup>36</sup>

Über die Plug-in-Liste des Browsers kann das Menü des Flash-Players nicht erreicht werden. Der Anwender muss aktiv die Hilfeseite des Adobe-Produkts aufsuchen. Es kann davon ausgegangen werden, dass sich die wenigsten User darüber bewusst sind bzw. sie im Einstellungsmanager tatsächlich aktiv Einträge vornehmen. Das Plug-in lässt sich

---

<sup>30</sup>vgl. [Soltani et al. 2009]

<sup>31</sup>Siehe Kapitel 2.2.5 *Evercookie* auf Seite 28

<sup>32</sup>Siehe Kapitel 2.2.9 *Browser Fingerabdruck* ab Seite 32

<sup>33</sup>Siehe Kapitel 3.3.1 *Einstellungen im Browser* auf Seite 114.

<sup>34</sup>vgl. [Xu Jimson und Nguyen Tom 2010]

<sup>35</sup>vgl. [Emmy Huang 2011]

<sup>36</sup>vgl. [Adobe Systems 2016]

jedoch über den Browser gänzlich deaktivieren bzw. ermöglicht eine "Click to Play"-Einstellung, woraufhin der Browser jedesmal nachfragt, ob das Flash-Plug-in ausgeführt werden darf.

Adobe Flash leidet regelmäßig unter massiven Sicherheitslücken, weshalb Firefox<sup>37</sup> und Chrome<sup>38</sup> das Plug-in wiederholt blockieren und vermehrt auf die Unterstützung von HTML5 setzen. Adobe hat selbst, mit seinem im November 2015 präsentierten Produkt "Adobe Animate CC", sein Angebot um HTML5-Entwicklertools und einem HTML5-Video-Player erweitert und ruft Webentwickler auf, verstärkt mit neuen Standards zu arbeiten.<sup>39</sup> Auch andere große Internet-Plattformen steigen vermehrt auf HTML5 um: Der Videoanbieter YouTube spielt seit Jänner 2015 Filme automatisch in HTML5 ab, ursprünglich waren sie im Flash-Format.<sup>40</sup> Auch Facebook wechselte Ende 2015 bei der Videodarstellung von Flash auf HTML5.<sup>41</sup> Google erlaubt auf seinen beiden Online-Werbe- und Marketinganbietern AdWords und DoubleClick Digital Marketing ab Juli 2016 kein Hochladen von Flash-Werbeanzeigen mehr und stellt mit Jänner 2017 die gesamte Unterstützung von Flash auf Google's Display Network und DoubleClick ein.<sup>42</sup>

### 2.2.3 HTML5-Cookie

HTML5 ist eine Weiterentwicklung der Seitenbeschreibungssprache HTML4, die zum Aufbau und zur Strukturierung von Webseiten dient. Die vollständige Spezifikation wurde am 28. Oktober 2014 vom World Wide Web Consortium (W3C) freigegeben. HTML5-Elemente wurden bereits mehrere Jahre davor teilweise von den verbreitetsten Browsern unterstützt und von Webentwicklern eingesetzt.<sup>43</sup>

Besonders die Eigenschaften der lokalen HTML5-Speicherelemente sind für Tracking-Zwecke interessant. Eine Studie<sup>44</sup>, die ebenfalls über den Einsatz von Etags<sup>45</sup> berichtet, hat schon im Juli 2011 auf das Vorhandensein von HTML5-Cookies, als Flash-Cookie-Alternative, aufmerksam gemacht. Sie verfügen über eine Speicherkapazität von min-

---

<sup>37</sup> vgl. [Mozilla Corporation 2016]

<sup>38</sup> vgl. [Porter Felt et al. 2015]

<sup>39</sup> vgl. [Adobe Corporate Communications 2015]

<sup>40</sup> vgl. [Richard Leider 2015]

<sup>41</sup> vgl. [Daniel Baulig 2015]

<sup>42</sup> vgl. [AdWords 2016]

<sup>43</sup> vgl. [W3C 2014]

<sup>44</sup> vgl. [Ayenson et al. 2011]

<sup>45</sup> Details dazu im anschließenden Kapitel 2.2.4 *Etags*.

destens 5MB, werden per Default permanent clientseitig gespeichert und benötigen im Gegensatz zu Flash-Cookies kein zusätzliches Plug-in, um zu funktionieren. Der Speicher kann zum Ablegen eindeutiger Identifikatoren und weiteren zusätzlichen Informationen dienen. Weiters kann ein HTML5-Cookie zum Abgleichen von herkömmlichen HTTP-Cookies und zum Erstellen von Zombie-Cookies<sup>46</sup> benutzt werden. Diese Eigenschaften machen ihren Einsatz zu einer bedeutenden Tracking-Technik.

Samy Kamkar macht sich HTML5 für sein entwickeltes Evercookie<sup>47</sup> zu Nutze. Eine weitere hartnäckige Tracking-Alternative, Canvas Fingerprinting<sup>48</sup>, bedient sich ebenfalls an HTML5-Elementen.

Wie im vorigen Kapitel bereits erwähnt, wurde 2009 auf den Einsatz von Flash-Cookies aufmerksam gemacht und deren Verbreitung erstmals untersucht<sup>49</sup>. Diese Recherche wurde 2011 um HTML5-Cookies erweitert und erneut durchgeführt<sup>50</sup>. Um die Entwicklung des Einsatzes von HTTP-, Flash- und HTML5-Cookies zu beobachten, wurde die Studie 2012 und 2015 abermals wiederholt. Dabei wurden die, laut Quantcast, 100, 1.000 und 25.000 meistbesuchten, us-amerikanischen Websites überprüft. Nur durch das Aufrufen der Homepage der 100-Top-Websites, wurden bei dem Durchlauf in 2015, 6.280 HTTP-Cookies gesetzt, davon 83% Third-Party-Cookies von 275 unterschiedlichen Anbietern. Drei Websites setzten auf ihrer Startseite bereits 300 oder mehr HTTP-Cookies. Nach zwei weiteren Klicks innerhalb der selben Domain wurden 12.857 HTTP-Cookies, davon 90% von Drittanbietern, erzeugt. 2012 waren es nur halb so viele Cookies. Beim initialen Besuch der 1.000-Top-Websites wurden 80.821 HTTP-Cookies generiert, bei den 25.000-Top-Websites 1.065.076. Der Einsatz von Flash-Cookies ist im Vergleich ebenfalls angestiegen. Besonders verstärkt hat sich der Gebrauch von HTML5-Cookies und die Anzahl der darin gespeicherten Informationen. So konnten 2015 auf den 100-Top-Websites, wenn zusätzlich zur Homepage zwei Unterseiten geladen wurden, 76 HTML5-Cookies mit 877 Werten ausgelesen werden. Bei den 1.000-Top-Websites stieg die Anzahl auf 649 HTML5-Cookies mit 6.309 gespeicherten Informationen und bei den 25.000-Top-Websites wurden 8.688 HTML5-Cookies mit 48.949 Elementen angelegt. Verglichen mit 2012 hat der generelle Gebrauch von Cookies stark zugenommen und es kann davon ausgegangen werden, dass die steigende Entwicklung andauern wird.<sup>51</sup>

---

<sup>46</sup>Wurde im vorigen Kapitel 2.2.2 *Flash-Cookies* beschrieben.

<sup>47</sup>Siehe Kapitel 2.2.5 *Evercookie* auf Seite 28

<sup>48</sup>Siehe Kapitel 2.2.10 *Canvas Fingerprinting* auf Seite 34.

<sup>49</sup>vgl. [Soltani et al. 2009]

<sup>50</sup>vgl. [Ayenson et al. 2011]

<sup>51</sup>vgl. [Altaweel et al. 2015]



### 2.2.4 Etags

Entity Tags (Etags) sind Teil des Caching-Prozesses zwischen Browser und Webserver im Internet. Sie werden eigentlich als Merkmal eingesetzt, um festzustellen, ob eine Webseite oder einzelne Elemente davon, sich seit dem letzten Aufruf verändert haben. Hat es kein Update gegeben, ist es nicht notwendig, diese Elemente erneut zu laden, sondern der Browser kann die bereits vorhandenen aus dem Cache verwenden. Somit wird der Seitenaufbau beschleunigt und Downloadlasten verringert.<sup>52</sup> Die Einsatzmöglichkeit von Etags für Tracking ist bereits seit 2003 bekannt<sup>53</sup>.

Dieselben Wissenschaftler, die 2009 auf den Einsatz von "Local Stored Objects" von Flash als Tracking-Elemente aufmerksam gemacht haben<sup>54</sup>, haben im Juli 2011 eine weitere Studie<sup>55</sup> veröffentlicht, wo sie den Einsatz von Etags als neues Tracking-Mittel beschreiben. Bei ihrer Recherche haben sie festgestellt, dass KISSmetrics, ein Web-Analyse-Dienstleister, als erstes Unternehmen Etags dafür eingesetzt hat, um eindeutige IDs für Tracking-Zwecke zu vergeben. Die ID wird beim ersten Aufruf einer Website mit KISSmetrics integriertem Code generiert und neben dem Etag auch in den HTTP-, Flash- und HTML5-Cookies des Users gespeichert. Dies bedeutet, dass selbst ein Anwender, der sich mit den Privatsphäre-Einstellungsmöglichkeiten seines Browsers auseinandergesetzt hat, Cookies blockiert und den privaten Browser-Modus verwendet, gegen die Tracking-Leistung eines KISSmetrics-Identifikators nichts ausrichten kann. Denn das Etag ist von diesen Einstellungen nicht betroffen und bleibt so lange erhalten, bis der Browser-Cache gelöscht wird. Der User müsste zwischen jedem Website-Aufruf den Cache löschen, um das Etag zurückzusetzen und ein durchgehendes Tracking zu verhindern. Hinzu kommt, dass der KISSmetrics-Code ein und dasselbe Erkennungsmerkmal nicht nur auf der ersten besuchten Website erstellt, sondern auf allen folgenden, die die Dienste von KISSmetrics verwenden. Das Merkmal ist immer identisch. Dies versetzt einerseits alle KISSmetrics-Kunden in die Lage ihre Analysedaten untereinander auszutauschen, auch ohne dem aktiven Mitwirken von KISSmetrics. So könnten sich zum Beispiel eine beliebige Firma A und Firma B, aufgrund des Wissens, das beide KISSmetrics einsetzen, gegenseitig kontaktieren und gesammelte Daten weitergeben. KISSmetrics selbst gelangt andererseits, aufgrund ihres Identifikators, in die Position, Individuen über verschiedene Websites hinweg eindeutig zu erkennen und ihre Aktivitäten im Netz zu speichern und auszuwerten.<sup>56</sup>

---

<sup>52</sup>vgl. [Clausen Lars R. 2004]

<sup>53</sup>vgl. [Gaudet Dean 2003]

<sup>54</sup>Siehe voriges Unterkapitel 2.2.2.

<sup>55</sup>vgl. [Ayenson et al. 2011]

<sup>56</sup>vgl. [Soltani Ashkan 2011]

Aufgrund der Ergebnisse dieser Studie, einer eingereichten Klage gegen KISSmetrics und mehreren Medienberichten darüber, hat das Unternehmen 2011 sein Geschäftsmodell geändert. Laut einem Blogeintrag durch Hiten Shah, dem Geschäftsführer von KISSmetrics, wurden folgende Änderungen durchgeführt: ein Opt-Out<sup>57</sup>, Wahrung des "Do Not Track"-Headers, sowie kein weiterer Einsatz von Etags oder anderen persistenten Trackingelementen.<sup>58</sup>

Im Rahmen der Diplomarbeit wurde die aktuelle Privacy Policy (Stand Jänner 2016) des Unternehmens, die seit 10. März 2014 gültig ist, auf Trackingtechniken hin untersucht. KISSmetrics verlangt von ihren Kunden, dass sie auf den Einsatz von KISSmetrics-Technologie und der Möglichkeit zum Opt-Out in ihren Datenschutzbestimmungen hinweisen. Der "Do Not Track"-Header wird nur über ihre Kunden berücksichtigt, wenn diese "Do Not Track" akzeptieren. KISSmetrics setzt weiterhin keine Etags oder andere Trackingelemente ein, ausgenommen von Zählpixel<sup>59</sup> und HTTP-Cookies.<sup>60</sup> Über eine Suchmaschinenabfrage nach "Kissmetrics Datenschutzbestimmungen" oder "Kissmetrics Privacy Policy" innerhalb österreichischer Websites konnte u.a. das Red Bull Media House gefunden werden, die KISSmetrics einsetzen.<sup>61</sup>

Wie bereits beschrieben, war, laut der im Juli 2011 publizierten Studie<sup>62</sup>, KISSmetrics das erste Unternehmen, das Etags für Tracking-Zwecke eingesetzt hat. Jonathan Mayer hat im August 2011 in einem Online-Artikel<sup>63</sup> einen weiteren Einsatz von Etags durch Microsoft veröffentlicht. Microsoft verwendete einen JavaScript-Code zur Erstellung einer eindeutigen Cookie-Kennung. Etags erhielten ebenfalls einen eindeutigen Parameter. Wurden die Cookies gelöscht, aber nicht der Cache des Browsers, war der zuerst erstellte Identifikator innerhalb des Etags immer noch vorhanden. Der Identifikator konnte mit dem eines neu erstellten Cookies assoziiert werden, wodurch die Erkennung des Users und die Tracking-Möglichkeit erhalten blieb. Der Autor des Beitrags konnte nicht feststellen wie Microsoft diese Daten verwendet und bei wievielen Internetbenutzern eine solche ID existiert. Von Microsoft betriebene Internetseiten zählen jedoch zu den hochfrequentiertesten im Web.

---

<sup>57</sup>Siehe im Kapitel 3.2.3 *Selbstregulierungs-Systeme* ab Seite 103.

<sup>58</sup>vgl. [Hiten Shah 2011]

<sup>59</sup>Siehe Unterkapitel 2.2.7 *Zählpixel* auf Seite 29.

<sup>60</sup>vgl. [Kissmetrics Privacy Office 2014]

<sup>61</sup>vgl. [Red Bull Media House 2015]

<sup>62</sup>vgl. [Ayenson et al. 2011]

<sup>63</sup>vgl. [Mayer Jonathan 2011b]

Beispielsweise befinden sich die zum Microsoft Universum gehörenden Webportale [www.live.com](http://www.live.com), [www.msn.com](http://www.msn.com) oder [www.bing.com](http://www.bing.com) unter den TOP 20 (Stand Jänner 2016) der weltweit meistbesuchtesten Websites<sup>64</sup>. Es wird davon ausgegangen, dass die Logfiles mit den entsprechenden Informationen von Microsoft nicht ohne weitere Auswertung gelöscht werden.

Im Umfang der Diplomarbeit wurden die aktuellen Datenschutzbestimmungen (Stand Jänner 2016) von Microsoft, die seit Oktober 2015 gültig sind, dahingehend untersucht, ob Etags im Einsatz sind. Dies konnte weder bestätigt noch widerlegt werden, da Microsoft die Begriffe "Cookies und ähnliche Technologien" verwendet und es unterlässt zu erklären, was mit "ähnlichen Technologien" im Detail gemeint ist.<sup>65</sup>

### 2.2.5 Evercookie

Das im Oktober 2010 veröffentlichte Evercookie wurde von dem IT-Sicherheitsexperten Samy Kamkar programmiert, um zu verdeutlichen, welche technischen Möglichkeiten es zum Erzeugen persistenter Tracking-Daten gibt.<sup>66</sup> Dabei werden mittels einer Javascript-Programmierschnittstelle verschiedene Speicherelemente des Browsers genutzt, um initial gesetzte Cookie-Informationen auf mehrere Speicherplätze verteilt zu hinterlegen. Sobald eines der Elemente gelöscht wird, regeneriert das Evercookie die Daten. Zu diesen Instanzen gehören u.a. HTTP-Cookies, Flash-Cookies, Etags, HTML5-Cookies oder die Chronik des Browsers. Es ist aufwendig und schwierig ein Evercookie bzw. alle seine Bestandteile zu löschen. Laut Samy Kamkar können mittels dem "Privaten Surfen"-Modus von Safari und einem anschließenden Safari-Neustart alle Evercookie-Varianten vernichtet werden.<sup>67</sup>

2014 wurde eine Studie veröffentlicht, die den Einsatz von Evercookies auf 10.000 der weltweit meistbesuchten Websites untersucht hat. Unter den Top 200 Seiten befanden sich zehn, die Flash-Cookies zur Wiederherstellung von gelöschten HTTP-Cookies einsetzten, zum Beispiel [www.yandex.ru](http://www.yandex.ru), die führende Suchmaschine in Russland. Das Flash-Cookie "bbcookie.sol" der Domain "bbcdn-bbnaut.ibillboard.com" belebte bei der Untersuchung die meisten Cookies wieder, 69 auf 24 Websites.

---

<sup>64</sup>vgl. [Alexa Internet, Inc. 2016b]

<sup>65</sup>vgl. [Microsoft 2015]

<sup>66</sup>vgl. [Tanzina Vega 2010]

<sup>67</sup>vgl. [Kamkar Samy 2010]

Die Forscher der Studie kommen zu dem Schluß, dass es selbst für Technik versierte User, die einen hohen Wert auf ihre Online-Privatsphäre legen und sich mit der Thematik vertraut gemacht haben, eine große Herausforderung darstellt, Tracking durch Evercookies zu verhindern.<sup>68</sup>

Unabhängig von der Studie kann davon ausgegangen werden, dass Evercookies im Einsatz sind. Die GitHub-Seite<sup>69</sup> des Informatikers Samy Kamkar zeigt, dass laufend an der Weiterentwicklung und Verbesserung des Evercookies gearbeitet wird.<sup>70</sup>

### 2.2.6 Supercookie

Der Begriff Supercookie wird regelmäßig in Berichten über Tracking-Verfahren erwähnt und soll deshalb kurz erklärt werden. Supercookies stellen keine weitere Cookie-Alternative dar, sondern dienen als Überbegriff für Tracking-Technologien, die nicht ausschließlich auf HTTP-Cookies aufbauen. Jede Technik, die bereits gelöschte Cookies wiederherstellen und somit Zombicookies generieren kann, gilt als ein Supercookie. Dazu gehören die bereits beschriebenen Evercookies, Etags, HTML5-Cookies und Flash-Cookies.<sup>71</sup>

### 2.2.7 Web Bugs

Web Bugs, auch Zählpixel, Web Beacons, Tracking-Pixel oder Clear GIFs genannt, sind neben HTTP-Cookies, die am längsten bekannte Tracking-Variante im Internet. Ein Web Bug besteht hauptsächlich aus einer 1x1-Pixel großen Grafik, die nicht als solche erkennbar auf einer Webseite platziert wird. Beim Aufruf der jeweiligen Internetseite wird diese Grafik mitgeladen und kann folgende Informationen, die vom Browser automatisch beim Aufrufen einer Seite mitgesendet werden, an den Webserver, von wo die Datei stammt, übermitteln: die IP-Adresse, der verwendete Browser, die Uhrzeit des Aufrufs, von welcher Seite die Pixelgrafik geladen wurde und, wenn bereits vorhanden, ein zuvor gesetzter Cookie-Wert. Web Bugs werden daher überwiegend als Third-Party-Tracking-Mittel eingesetzt.

---

<sup>68</sup>vgl. [Acar et al. 2014a]

<sup>69</sup>GitHub ist ein Online-Dienst für Softwareentwicklung.

<sup>70</sup>vgl. [Kamkar Samy 2016]

<sup>71</sup>vgl. [Mayer Jonathan 2011b]

Die Daten können zu Webanalyse-Zwecken eingesetzt werden, um beispielsweise festzustellen, wieviele Personen eine bestimmte Seite besucht haben. Die Werbebranche nutzt die Angaben, um die Surfgewohnheiten eines Internetusers zu protokollieren und damit Benutzerprofile zu ergänzen.<sup>72</sup>

Das Laden von Web Bugs kann mittels direkter Browsereinstellungen nicht verhindert werden, außer man würde dem Browser generell das Laden von Grafiken untersagen. Zählpixel können auch nicht einfach gelöscht werden, weil sie im HTML-Code der Webseite integriert sind. Eine Zwischenlösung wäre, keine Cookies und vor allem keine Drittanbieter-Cookies zu akzeptieren und somit zumindest das Senden von Cookie relevanten Daten zu unterbinden. Um Web Beacons vollständig zu blockieren, benötigt man ein passendes Browser-Add-on, wie zum Beispiel "Ghostery"<sup>73</sup>.

### 2.2.8 History Sniffing

History Sniffing basiert auf einer über mehrere Jahre bekannte Sicherheitslücke in der Browser-Software, die einen Zugriff auf die hinterlegte Chronik des Users zulässt. Ein Browser speichert in der Chronik nicht nur die besuchten Webseiten, sondern auch welche Hyperlinks angeklickt wurden und welche nicht, indem diese unterschiedlich farblich hinterlegt werden. Üblicherweise werden Links in blau angezeigt, nach einem Aufruf werden sie violett oder in einer anderen als der Ausgangsfarbe dargestellt. Besuchte Websites können mittels History Sniffing anhand von einer beliebigen Liste an URLs überprüfen, welche davon ein User aufgerufen hat und welche nicht, je nachdem, wie sie in der Chronik des Anwenders hinterlegt sind. Ohne dass der Internetbenutzer etwas davon merkt, kann problemlos auf diese Daten zugegriffen und Informationen über die Surfgewohnheiten des Users gesammelt werden.<sup>74</sup>

"History Sniffing" wäre beispielsweise für folgende Szenarien anwendbar:

- Die Erstellung eines ausführlichen Benutzerprofils anhand der besuchten Webseiten und geöffneten Hyperlinks wäre realisierbar. Dadurch könnte man die Platzierung von Werbeanzeigen auf die Chronik abstimmen.

---

<sup>72</sup>vgl. [Smith Richard M. 1999]

<sup>73</sup>Siehe Kapitel 3.3.2 *Browsererweiterungen* auf Seite 119.

<sup>74</sup>vgl. [Jackson et al. 2006]

- Ein Webshop könnte nur jenen Usern spezielle Sonderangebote oder Ermäßigungen anzeigen, der zuvor eine Konkurrenzseite besucht hat.
- Internetbetrüger wären in der Lage Informationen über aufgerufene Bank- oder Kreditkartenseiten für Phishing-Attacken einzusetzen. Auch Identitätsdiebstahl wäre mittels der Daten denkbar.

Im Oktober 2010 wurde eine Studie<sup>75</sup> veröffentlicht, die erstmals untersucht hat, ob "History Sniffing" zum Einsatz kommt. Es wurde festgestellt, dass von 50.000 Websites, die laut Alexa<sup>76</sup> weltweit am häufigsten besucht wurden, 46 davon "History Sniffing" in Verwendung hatten. Darunter das Webportal "YouPorn", das sich unter den Top 200 (Stand Jänner 2016) befindet und mittlerweile dessen Einsatz eingestellt hat.

Eine im Mai 2010 veröffentlichte Studie<sup>77</sup> verwendet "History Sniffing" um Nutzerdaten aus bekannten sozialen Netzwerken, wie Xing, Facebook und LinkedIn, auszulesen. Soziale Netzwerke verfügen über große Datenbanken mit persönlichen Angaben und stellen daher ein beliebtes Angriffsziel dar. Voraussetzung des Angriffversuchs war, dass auf Mitgliedszugehörigkeiten zu Benutzergruppen innerhalb des Netzwerks zugegriffen werden konnte. Meistens ist die Teilnahme an einer Gruppe ausreichend, um einen User eindeutig identifizieren zu können. Der Besuch einer Gruppe ist wie ein Seitenaufruf, der in der Chronik des Mitglieds gespeichert wird und so mittels "History Sniffing" zugänglich ist. Die Wissenschaftler konnten 42% der registrierten Xing-Benutzer ermitteln. Auch andere Plattformen, wie Facebook oder LinkedIn, sind in dieser Weise angreifbar. Die Studie ergab, dass um eine Person eindeutig identifizieren zu können "History Sniffing" alleine nicht ausreicht, aber es in Verbindung mit Informationen aus sozialen Netzwerken wesentlich einfacher wird.

---

<sup>75</sup>vgl. [Jang et al. 2010]

<sup>76</sup>Alexa Internet, Inc. ist ein Internetservice-Anbieter mit Sitz in San Francisco, USA, das sich auf Datenverkehr und Website-Ranglisten spezialisiert hat. Anhand von einer Kombination aus täglichen Besuchern und Seitenzugriffen des letzten Monats werden die am häufigsten aufgerufenen Internetseiten berechnet.

<sup>77</sup>vgl. [Wondracek et al. 2010]

Im März 2010 veröffentlichte David Baron, ein Entwickler bei Mozilla, eine Lösung des Problems<sup>78</sup>, woraufhin im Firefox Browser die Sicherheitslücke geschlossen wurde<sup>79</sup>. Auch in den anderen Browsern kann über die ursprüngliche Java-Script-Abfrage der CSS-Style-Sheets kein History Sniffing mehr betrieben werden. Eine Studie vom Juli 2015 zeigt in einem Überblick bekannter Trackingtechniken, dass seit 2010 andere Varianten des History Sniffing entwickelt wurden, die teilweise auf den Webcache bzw. Fingerabdruck des Browsers<sup>80</sup> oder auf Userinteraktion zurückgreifen.<sup>81</sup>

### 2.2.9 Browser-Fingerabdruck

Eine Studie von Peter Eckersley von der amerikanischen Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) aus 2010 hat ergeben, dass das Auslesen von Informationen, die der verwendete Browser eines Internetnutzers beim Aufrufen einer Webseite zur Verfügung stellt, einen ziemlich eindeutigen "Fingerabdruck" erzeugt. Dabei wurde ein Algorithmus eingesetzt, der folgende Browsermerkmale erfasst: User Agent, HTTP\_ACCEPT Headers, Browser-Plug-in-Details, Zeitzone, Bildschirmauflösung, Bildschirmfarbtiefe, System-Schriftarten, ob Cookies aktiviert sind und vorkommende Supercookies. Das Forschungsergebnis zeigte auf, dass 83,6% der Browser eindeutig identifizierbar und somit wiedererkennbar waren. Jene Browser, die entweder Adobe Flash oder eine Java Virtual Machine implementiert hatten, sogar zu 94,2%. User, die auf ihre Privatsphäre achteten und dementsprechende Plug-ins anwandten, generierten dadurch sogar eine noch größere Einmaligkeit. Der verwendete Algorithmus und wie einzigartig die eigene Browserkonfiguration ist, kann unter <https://panopticlick.eff.org> getestet werden.<sup>82</sup>

2015 wurde Panopticlick dahingehend erweitert, dass Browser-Add-ons wie Adblock Plus, Ghostery oder Disconnect<sup>83</sup> auf ihre Blockierfähigkeiten gegenüber Trackingelementen überprüft werden. Mit dem Test auf <https://panopticlick.eff.org> wird also einerseits ermittelt, wie individuell der Browser Fingerabdruck ist und andererseits wie gut der User gegen verbreitete Trackingtechniken geschützt ist.

---

<sup>78</sup>vgl. [David Baron 2010]

<sup>79</sup>vgl. [Sid Stamm 2010]

<sup>80</sup>Siehe nächstes Kapitel

<sup>81</sup>vgl. [Bujlow et al. 2015]

<sup>82</sup>vgl. [Eckersley Peter 2010]

<sup>83</sup>Siehe Kapitel 3.3.2 *Browsererweiterungen* ab Seite 119.

Seit 2015 wird auch kontrolliert, ob der Browser ein "Do Not Track"-Signal<sup>84</sup> sendet und ob Canvas Fingerprinting<sup>85</sup> zugelassen wird.<sup>86</sup>

Die Identifizierungsmöglichkeiten durch einen Browser Fingerabdruck stellen eine bedeutende Tracking-Variante dar, denn sie ist weder transparent noch leicht zu verhindern. Im Gegensatz zu den bisherigen Trackingverfahren, wird hier nicht das Verhalten des Users, sondern die Eigenschaften des eingesetzten Browsers analysiert.<sup>87</sup>

Eine weitere Studie über JavaScript-Anwendungen hat ergeben, dass die Einstellungen, welche das Firefox-Add-on "NoScript" auszeichnen, ausgewertet werden können. Den Autoren gelang der Zugriff auf die Positivliste und konnten aufgrund dessen das Surfverhalten bzw. jene Webseiten, denen der Benutzer vertraut, in Erfahrung bringen. Diese Daten ermöglichen wiederum das Erstellen eines genauen Profils des Users, das für personalisierte Online-Werbung eingesetzt werden kann.<sup>88</sup> Dies deutet darauf hin, dass es selbst für Webanwender, die sich mit Datenschutz und Wahrung der Privatsphäre auseinandersetzen, schwierig ist einen Browser-Fingerabdruck zu verhindern.

Ein weiteres negatives Beispiel der Möglichkeiten zur Personenerkennung zeigt das "Fingerprintr Projekt". Dem Schweizer Sicherheitsexperten Walter Sprenger ist es im Mai 2011 gelungen, anhand eines Browser-Fingerabdrucks, Benutzerdaten von Facebook zu evaluieren. Er hat mit einem seiner Studenten eine Applikation namens "Fingerprintr" entwickelt. Sie besteht aus einer Website, die, ähnlich wie Panopticlick, einen Browser-Fingerabdruck erzeugt. Weiters haben sie eine Facebook-Applikation implementiert, bei deren Aufruf im Hintergrund ebenfalls ein Browser-Fingerabdruck erstellt wird. Durch die Kombination der beiden "Fingerabdrücke" ist es ihnen gelungen, außerhalb des sozialen Netzwerks die Identität eines Users zu ermitteln. Voraussetzung dafür ist, dass die Einträge auf Facebook keine Pseudonyme oder erfundene Informationen sind, sondern echte Personendaten registriert wurden. Techniken dieser Art könnten in beliebigen Facebook-Erweiterungen versteckt integriert sein. Diese Funktionalität kann u.a. für Tracking-Zwecke eingesetzt werden, um personalisierte Benutzerprofile zu generieren.<sup>89</sup>

---

<sup>84</sup>Siehe Kapitel 3.3.1 *Einstellungen im Browser* auf Seite 112.

<sup>85</sup>Siehe übernächstes Kapitel 2.2.10 *Canvas Fingerprinting* auf Seite 34.

<sup>86</sup>vgl. [Electronic Frontier Foundation 2015]

<sup>87</sup>vgl. [Electronic Frontier Foundation 2015]

<sup>88</sup>vgl. [Mowery et al. 2011]

<sup>89</sup>vgl. [Sprenger Walter 2011]



### 2.2.10 Canvas Fingerprinting

Eine spezielle Form des Browser-Fingerabdrucks ist jene, die mittels Canvas Fingerprinting generiert wird. Diese Art des Trackings wurde erstmals in einer Studie 2012 publik gemacht. Der Canvas Fingerabdruck baut darauf auf, dass der Browser immer mehr Zugriff auf Funktionen des zugrundeliegenden Betriebssystems und der Hardware hat, im Speziellen auf die Grafikkarte und das Rendern von Schriftarten. Websites mit installierter Canvas-Fingerprinting-Methode greifen auf das HTML5 Canvas-Element zu, worin im Hintergrund Text oder Grafiken generiert werden. Da die Systemvoraussetzungen von Benutzer zu Benutzer sehr individuell sind, wird dadurch ein eindeutiges Bild erzeugt, aus dessen Darstellung und Pixelanalyse eine eindeutige ID gewonnen werden kann, die wiederum für Tracking einsetzbar ist. Der Vorteil eines Canvas-Fingerabdrucks ist vor allem seine Konsistenz, er kann unbemerkt vom User und einfach erstellt werden.<sup>90</sup>

In der selben Studie<sup>91</sup>, in der 2014 der Einsatz von Evercookies<sup>92</sup> nachgewiesen wurde, konnte auch die Verwendung von Canvas Fingerprinting aufgezeigt werden. Im Mai 2014 untersuchten die Wissenschaftler die laut Alexa 100.000 weltweit meistbesuchten Websites und konnten auf 5,5% aktive Canvas-Fingerprinting-Mechanismen von 20 unterschiedlichen Domains feststellen. Deren Ursprung gehörte zu 95% zu AddThis<sup>93</sup>, einem amerikanischen Unternehmen, das unter anderem Widgets für Websites zur Verfügung stellt, um gesammelt mehrere Social-Media-Buttons auf einmal einzubetten, Website-Analysen durchführt und bei der Platzierung von Werbeanzeigen hilft.

AddThis äußerte sich im Juli 2014 zu der Studie und gab bekannt, dass es sich dabei nur um einen mehrmonatigen Test gehandelt hatte, um Cookie-Alternativen auszuprobieren. Der Canvas-Fingerprinting-Code würde von AddThis seitdem nicht mehr eingesetzt werden.<sup>94</sup>

---

<sup>90</sup> vgl. [Mowery et al. 2012]

<sup>91</sup> vgl. [Acar et al. 2014a]

<sup>92</sup> Siehe Kapitel 2.2.5 *Evercookies* auf Seite 28.

<sup>93</sup> vgl. [AddThis Privacy Office 2014]

<sup>94</sup> vgl. [Rich LaBarca 2014]

Ihre Privacy Policy wurde jedoch zuletzt am 7. April 2014 aktualisiert (Stand Jänner 2016), darin steht zum Beispiel, dass eine eindeutige Browser-ID vergeben wird. Welche Technik dafür im Einsatz ist, wird im Detail nicht beschrieben.

*”We also assign your web browser a unique identifier. This ID doesn’t, and can’t, say anything about you, it’s just a random series of numbers and letters we use to distinguish users from each other.”*<sup>95</sup>

AddThis bietet auf ihrer Website eine Opt-Out-Möglichkeit<sup>96</sup> an, jedoch bezieht sich diese nur darauf, dass keine Daten des Users gesammelt werden, um für ihn passende Werbung zu platzieren. In der Studie aus 2014 wurde die Wirkung des AddThis-Opt-Outs untersucht und dargelegt, dass beim Aufrufen von Webseiten mit integriertem AddThis-Code und gesetztem AddThis-Opt-Out-Cookie trotzdem Canvas-Fingerprinting durchgeführt wurde.<sup>97</sup> Auch hier soll auf die Problematik von Opt-Outs<sup>98</sup> hingewiesen werden. Ein Enduser kann mittels Opt-Out nicht bestimmen, dass generell keine Daten von ihm gesammelt oder weiterverarbeitet werden. AddThis behält sich weiters das Recht vor, nicht personenbezogene Daten, dazu zählen u.a. die IP-Adresse oder die eindeutige Browser-ID, die AddThis setzt, mit Daten von anderen Dienstleistern zusammenzuführen und zu analysieren.<sup>99</sup>

Unter den 100.000 von der Studie untersuchten Websites, wurden auch zehn österreichische Domains gefunden: jene der ÖBB, von Kika, Conrad, NudeVista, Parents.at, RestaurantTester, Eversport, haude electronica, dem Wifi Wien und meinKauf. Davon wurde 2014 bei allen der AddThis-Code mit dem Canvas-Fingerprinting-Mechanismus festgestellt, außer meinKauf, die einen eigenen verwendeten.<sup>100</sup> AddThis war beim Besuch der ÖBB-, Kika-, Conrad-, Wifi-, Eversport- und haude-electronica-Homepage während der Begutachtung als Teil der Diplomarbeit im Jänner 2016 nicht mehr integriert. Bei NudeVista, Parents.at und RestaurantTester ist AddThis weiterhin aktiv, wird in den AGBs oder Datenschutzbestimmungen der jeweiligen Seite aber nicht angegeben.

<sup>95</sup>Zitat von [AddThis Privacy Office 2014], Privacy - What you should know

<sup>96</sup>vgl. [AddThis Privacy Office 2016]

<sup>97</sup>vgl. [Acar et al. 2014a]

<sup>98</sup>Siehe im Kapitel 3.2.3 *Selbstregulierungs-Systeme* ab Seite 103.

<sup>99</sup>vgl. [AddThis Privacy Office 2014], Privacy - Privacy Policy

<sup>100</sup>vgl. [Acar et al. 2014b]

Die beiden Mitarbeiter der Studie aus 2014, Steven Englehardt und Arvind Narayanan, haben die Tracking-Messung im Jänner 2016 wiederholt und weiter ausgebaut. Dabei wurden die laut Alexa 1 Million weltweit meistbesuchten Websites auf unterschiedliche Tracking-Techniken untersucht. Damit haben sie die bisher umfangreichste Tracking-Analyse durchgeführt. Bei der Kontrolle, ob der Canvas-Fingerprinting-Code von AddThis weiterhin eingesetzt wird, konnten 72 Websites ausfindig gemacht werden, die den Code integriert haben. 14 österreichische Domains (zalando.at,groupon.at,home24.at,jochen-schweizer.at,expedia.at,meinkauf.at,automobile.at,kochrezepte.at,bruttonetto-rechner.at,autonet.at,tarifecheck.at,homeaway.at,salzkammergut-rundblick.at und du-bist-der-teamchef.at) setzen von fünf Drittanbietern (metrigo.com,dzheqstlbt4e.cloudfront.net,edgesuite.net,cdn-net.com,doubleverify.com) Canvas Fingerprinting ein.groupon.at und meinkauf.at verwenden dafür eigenständige Entwicklungen.<sup>101</sup>

Medien berichteten mehrfach über die Studie aus 2014, u.a. das Online-Nachrichtenportal ProPublica, deren Artikel einen Canvas-Fingerprinting-Test anbietet.<sup>102</sup> Im Rahmen der Diplomarbeit wurde im Jänner 2016 mit einem MacBook Pro mit installiertem Betriebssystem OS X 10.9.5 mit vier der gängigen Browser der Test durchgeführt. Anschließend sollen die unterschiedlich generierten Bilder und die daraus erstellte, jeweils für den Browser individuelle ID dargestellt werden:



Abbildung 2.5: Die Grafik zeigt einen Canvas Fingerabdruck mit dazu generierter, eindeutiger ID. Das Bild wurde mittels Firefox Version 44.0 auf einem MacBook Pro mit OS X 10.9.5 aufgerufen.

Bildquelle vgl. [Mike Tigas 2014]

<sup>101</sup>vgl. [Englehardt et al. 2016]

<sup>102</sup>vgl. [Mike Tigas 2014]



Abbildung 2.6: Die Grafik zeigt einen Canvas Fingerabdruck mit dazu generierter, eindeutiger ID. Das Bild wurde mittels Google Chrome Version 48 auf einem MacBook Pro mit OS X 10.9.5 aufgerufen.

Bildquelle vgl. [Mike Tigas 2014]



Abbildung 2.7: Die Grafik zeigt einen Canvas Fingerabdruck mit dazu generierter, eindeutiger ID. Das Bild wurde mittels Safari Version 9.0.3 auf einem MacBook Pro mit OS X 10.9.5 aufgerufen.

Bildquelle vgl. [Mike Tigas 2014]



Abbildung 2.8: Die Grafik zeigt einen Canvas Fingerabdruck mit dazu generierter, eindeutiger ID. Das Bild wurde mittels Opera Version 9.0.3 auf einem MacBook Pro mit OS X 10.9.5 aufgerufen.

Bildquelle vgl. [Mike Tigas 2014]

### 2.2.11 Geräte-Fingerabdruck

*"I think cookies are a joke. The system is archaic and was invented by accident. We've outgrown it, and it's time for the next thing."*<sup>103</sup>

Nicht nur der Browser kann einen individuellen, digitalen Fingerabdruck hinterlassen. Jedes Gerät (zum Beispiel: Laptop, PC, Mobiltelefon, Tablet-Computer, Spielkonsole, TV-Set-Top-Box, Auto-Navigationsgerät), das über eine Internetverbindung verfügt, kann unverwechselbar und auf Dauer anhand seiner spezifischen Eigenschaften erkannt werden.<sup>104</sup> Laut Peter Eckersley von der Electronic Frontier Foundation stellt die Langlebigkeit und die Tracking-Möglichkeit eines Geräte-Fingerabdrucks im Vergleich zu herkömmlichen Cookies eine große Gefahr für den Datenschutz und die Privatsphäre dar. Andererseits betonen Befürworter dieser Technologie, dass durch einen Geräte-Fingerabdruck auch ein resistentes Opt-Out geschaffen wird. Im Gegensatz zu der Lebensdauer eines Opt-Out-Cookies, das eventuell beim Beenden des Browsers gelöscht wird, bleibt ein Opt-Out-Fingerabdruck für die Nutzungsdauer des jeweiligen Geräts erhalten.<sup>105</sup>

Als Teil dieser Diplomarbeit wurde das Geschäftsmodell der amerikanischen Firma BlueCava, deren Technik auf der Erstellung von Geräte-Fingerabdrücken basiert, untersucht. Das erklärte Ziel dieses Unternehmens ist es, alle Geräte weltweit, die mit dem Internet verbunden sind, zu ermitteln und zu kennzeichnen. Die Firma wirbt mit ihrer eindeutigen BlueCava-ID, die besonders langlebig, "selbstheilend" und um 2500% effizienter als herkömmliche Cookies sein soll, was auf den Einsatz von Evercookies<sup>106</sup> hindeutet. BlueCava hat mit seiner Technologie, die sie als "cross-screen mapping" anpreisen, ebenfalls die Möglichkeit auszuwerten, welche unterschiedlichen Geräte zueinander in Beziehung stehen, zum Beispiel innerhalb eines Haushalts, oder ob ein Mobiltelefon, Tablet und Computer im Besitz von ein und derselben Person sind. BlueCava wertet weiters das Surf- und Einkaufsverhalten des Benutzers der indizierten Geräte aus, um Interessen, Standort und demographische Informationen zuzuweisen. Darauf aufbauend können Kunden von BlueCava ihre Zielgruppen auswählen und zum Beispiel Werbung passend zur jeweiligen Person auf allen Geräten, die mit ihr assoziiert werden, platzieren.<sup>107</sup>

<sup>103</sup>Zitat von [Norris David, CEO von BlueCava 2010], Race Is On to 'Fingerprint' Phones, PCs

<sup>104</sup>vgl. [Marshall Jack 2011a]

<sup>105</sup>vgl. [Marshall Jack 2011b]

<sup>106</sup>Siehe Kapitel 2.2.5 *Evercookie* auf Seite 28.

<sup>107</sup>vgl. [BlueCava, Inc. 2016a]

Die Website von BlueCava wurden im Laufe der Diplomarbeit erstmals 2011 besucht. Zu dieser Zeit häufte sich auf den Seiten des Unternehmens wiederholt die Aussage, "BlueCava wäre nicht an Personen, sondern ausschließlich an Maschinen interessiert":

*"Device identification at BlueCava strips out all PII (personally identifiable information) so that you can target machines not people."*<sup>108</sup>

*"What a device has done is a pretty interesting way to look at things because we are targeting device behavior, not people."*<sup>109</sup>

*"We remove names, physical addresses and email addresses from the data we collect. So this means that the companies that use our services are targeting machines rather than people."*<sup>110</sup>

*"But we want you to know that we don't collect any personal information (or PII as it's called in the industry). We strip it out. At BlueCava, we focus on devices, not people."*<sup>111</sup>

*"These pieces of information are used to uniquely identify a device. Of course we do not collect any personal information, just boring stuff that most people couldn't care less about."*<sup>112</sup>

*"At BlueCava we are interested in machines, not people."*<sup>113</sup>

2016 sieht die Unternehmensstrategie anders aus, Personen und Maschinen werden nicht mehr verglichen, stattdessen wird hauptsächlich von Bildschirmen gesprochen:

*"BlueCava's Platform enables our Clients to recognize Screens when their Users visit Sites."*<sup>114</sup>

*"Our Platform utilizes cookies. [...] This allows us to identify a Screen faster and more efficiently."*<sup>115</sup>

<sup>108</sup>Zitat von [BlueCava, Inc. 2011], What we do - Device Identification

<sup>109</sup>Zitat von [BlueCava, Inc. 2011], What we do - Device Reputation

<sup>110</sup>Zitat von [BlueCava, Inc. 2011], Privacy Policy

<sup>111</sup>Zitat von [BlueCava, Inc. 2011], Privacy Policy

<sup>112</sup>Zitat von [BlueCava, Inc. 2011], Privacy Policy

<sup>113</sup>Zitat von [BlueCava, Inc. 2011], Privacy Policy

<sup>114</sup>Zitat von [BlueCava, Inc. 2016a], Privacy Policy

<sup>115</sup>Zitat von [BlueCava, Inc. 2016a], Privacy Policy

*"We may combine our data with the data of others to make us even better at recognizing Screens."*<sup>116</sup>

*"Additionally, BlueCava does not track users as they move from one publisher to another, only recognizing a user at a specific moment in time when they interact with a site or ad that includes our technology."*<sup>117</sup>

Direkt im Footer der Firmen-Website, als auch über die Privacy Policy, gelangt man zur Opt-Out-Möglichkeit von BlueCava. Weiters hat man die Option die BlueCava-ID zurückzusetzen. Das Unternehmen informiert darüber, dass es den "Do Not Track"-Header akzeptiert, aber keinen Einfluss darauf hat, ob ihre Kunden "Do Not Track" berücksichtigen.<sup>118</sup> Die Problematik von Opt-Outs wird im Detail in Kapitel 3.2.3 *Selbstregulierungs-Systeme* ab Seite 103 beschrieben. Hier soll darauf hingewiesen werden, dass ein User nicht weiß, dass eventuell beim Besuch einer Website mittels Technologie von BlueCava ein Geräte-Fingerabdruck gemacht wird. In der Privacy Policy von BlueCava konnte kein Eintrag dazu gefunden werden, dass BlueCava seine Kunden auffordert, den Einsatz ihrer Technologie bekannt zu geben.

BlueCava informiert darüber keine personenbezogenen Daten zu sammeln. Es ist fraglich, ob ihre Behauptung stimmt, dass persistente IDs in Kombination mit analysierten Bildschirmdaten und die Möglichkeit zielgerichtete Werbung auf ausgewählte Geräte zu platzieren, nicht personenbezogen sind und keinen Eingriff in die Privatsphäre darstellen? Werden Name, Postanschrift, Emailadresse, Alter oder Geschlecht noch benötigt, wenn man ein Gerät eindeutig im Internet identifizieren kann und man weiß, welche Webinformationen damit gerne bzw. regelmäßig aufgerufen werden? Stellt in diesem Fall der Begriff Gerät oder Bildschirm nicht ein Synonym für Person oder User dar?

BlueCava ist eine Tochtergesellschaft von Uniloc, ein australisches Softwareunternehmen, das seine Technologie ursprünglich ausschließlich zur Bekämpfung von Raubkopien von Software eingesetzt hat. Mittlerweile hat es sein Geschäftsfeld um zusätzliche Einsatzvarianten, wie zum Beispiel in der Werbewirtschaft und der generellen Prävention von Internet-Kriminalität, erweitert. Das 2010 gegründete BlueCava dient zu dessen Vermarktung.

<sup>116</sup>Zitat von [BlueCava, Inc. 2016a], Privacy Policy

<sup>117</sup>Zitat von [BlueCava, Inc. 2016a], Cross-Screen University, White Paper

<sup>118</sup>vgl. [BlueCava, Inc. 2016b]

Das Wall Street Journal berichtet in seinem Artikel "Race Is On to 'Fingerprint' Phones, PCs"<sup>119</sup> der "What They Know"-Serie<sup>120</sup>, dass immer mehr Firmen, die sich auf die Identifizierung von Geräten spezialisiert haben, um diese gegen illegales Vervielfältigen von Software und Online-Betrug einzusetzen, erkennen, dass sie auch in anderen Wirtschaftsbereichen, wie der Online-Werbung, Geld verdienen können. Selbst innerhalb dieser Industrie ist man sich uneinig, wie man Fingerabdrücke von Geräten am besten anwenden soll und wie man zwischen ehrlichen Kunden, die nicht getrackt werden wollen und Online-Betrügnern abgrenzen kann.<sup>121</sup>

Eine Studie aus 2013, die den verbreiteten Einsatz von webbasierten Fingerprinting untersucht und nachgewiesen hat, behandelt ebenfalls die Frage bezüglich der Begrifflichkeit von "Gerät" und "User". Die Autoren haben festgestellt, dass Unternehmen, die Geräte- oder Browser-Fingerabdrücke für Sicherheitsabfragen zur Abwehr von Online-Betrug einsetzen, oft ausdrücklich darauf hinweisen, Geräte und nicht Personen zu protokollieren. Die Unternehmen würden nicht personenbezogene, sondern gerätespezifische Daten speichern und auswerten. Weiters konnte die Studie aufzeigen, dass die Fingerprinting-Technik damit legalisiert wird, dass sie zum Schutz des Anwenders diene. Die Forscher sehen den Datenschutz des Benutzers vor allem dadurch gefährdet, dass eindeutige Geräte-IDs als nicht personenbezogen vermarktet werden, obwohl sie ihrer Meinung nach mit ihnen gleichwertig sind.<sup>122</sup>

### 2.2.12 Tracking durch Social-Media-Buttons

Websites haben bei ihren Beiträgen meistens Schaltflächen der populären Social-Media-Plattformen wie Facebook ("Gefällt mir", "Like", "Teilen", "Share", "Login", etc.), Twitter ("Twittern", "Tweet") oder Google-Plus ("+1") integriert. Sie ermöglichen es dem Internetbenutzer direkt von der besuchten Seite aus einen Beitrag innerhalb des gewählten Netzwerks zu veröffentlichen. Indem man zum Beispiel den "Gefällt mir"-Button von Facebook anklickt gelangt man, bei voriger Anmeldung, direkt auf seine Facebook-Profilseite, wo automatisch ein dementsprechender Eintrag mit einem Link auf diesen Beitrag erstellt wird. Ist man nicht angemeldet, gelangt man zuerst auf die Login-Seite von Facebook. Der User kann so einfach Informationen, die ihn interessieren, mit seinen Freunden teilen.

<sup>119</sup>vgl. [Norris David, CEO von BlueCava 2010]

<sup>120</sup>vgl. [The Wall Street Journal 2010 - 2012]

<sup>121</sup>vgl. [Valentino-DeVries Jennifer 2010]

<sup>122</sup>vgl. [Acar et al. 2013]



Für Websites hat das Einbetten der Schaltflächen den Vorteil, dass dadurch die Besucherzahlen und somit die Zugriffe auf ihre Seiten erhöht werden.

Datenschützer kritisieren diese Funktionalität, denn die Surfgewohnheiten der Nutzer können dadurch vom jeweiligen Social-Media-Anbieter protokolliert werden. Jedesmal wenn eine dieser Schaltflächen angeklickt wird erfahren Facebook, Twitter, Google und Co. welche Internetseite von ihrem User besucht bzw. welches Webangebot genutzt wurde. Alleine das Laden der Seite reicht aus um Daten mittels Cookies an den entsprechenden Dienst zu übermitteln. Dazu ist es nicht einmal notwendig den entsprechenden Button zu betätigen. Dies ist zum Beispiel bei dem von Facebook bereitgestellten Code der Fall. Ist der User zum Zeitpunkt des Seitenaufrufs bei Facebook angemeldet, erhält Facebook über gesetzte Cookies Informationen zu den Internetaufrufen und kann diese personalisiert speichern und verwalten. Auch von Personen, die noch keine Facebook-Mitglieder sind, kann das Surfverhalten dadurch übermittel werden und das Netzwerk kann diese in einer separaten Datenbank aufzeichnen und zu einem späteren Zeitpunkt einem neuen Mitglied zuweisen.<sup>123</sup>

Heise online hat 2011 eine Alternative entwickelt, um Buttons von sozialen Netzwerken ohne dem sofortigen Senden von Daten in eine Webseite zu integrieren. Dabei haben sie folgenden "Zwei Klick"-Mechanismus entwickelt: Alle Social-Media-Schaltflächen auf einer Webseite sind zunächst einmal inaktiv. Möchte der User einen Button verwenden, muss er im ersten Schritt diesen zuerst anklicken, damit er auf aktiv gesetzt wird. Ab diesem Zeitpunkt werden von dieser Webseite Daten, aber nur an das zum Button gehörige soziale Netzwerk, kommuniziert. Um einen Beitrag auf jenem Netzwerk zu integrieren muss in einem zweiten Schritt der Button erneut angeklickt werden und man wird zur betreffenden Plattform verbunden. Das Verfahren ist so konzipiert, dass bei jeder weiteren besuchten Seite alle Buttons wieder inaktiv sind, auch wenn zuvor eine Verbindung erlaubt wurde. Benutzer, die den "Zwei-Klick-Button" nicht verwenden möchten, haben die Möglichkeit die defaultmäßige Einstellung so zu ändern, dass die Schaltflächen von einzelnen oder allen Netzwerken immer aktiv sind. Heise bietet den Code unter einer Open-Source-Lizenz für andere Website-Betreiber zur Weiterverwendung an.<sup>124</sup>

---

<sup>123</sup>vgl. [Roosendaal Arnold 2010]

<sup>124</sup>vgl. [Jürgen Schmidt 2011]



Abbildung 2.9: Die Grafik zeigt die inaktiven Schaltflächen von Facebook, Twitter und Google-Plus auf heise online. Über dem Twitter-Button wird ein Informationstext eingeblendet.

Bildquelle vgl. [Jürgen Schmidt 2011]



Abbildung 2.10: Die Grafik zeigt die geänderte Darstellung des aktivierten Twitter-Buttons nach dessen einmaligen Anklicken und eine Erklärung zur möglichen Datenübertragung.

Bildquelle vgl. [Jürgen Schmidt 2011]

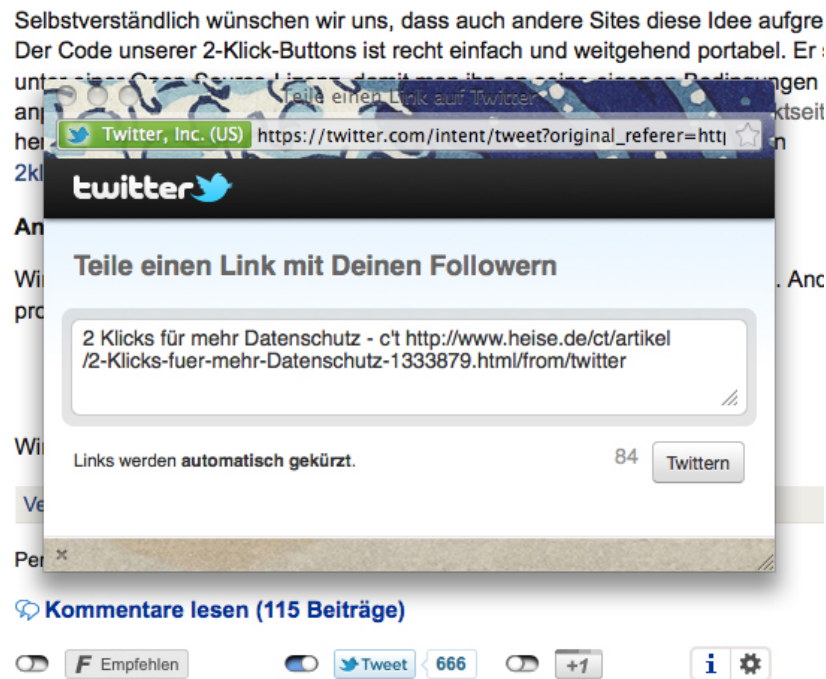


Abbildung 2.11: Die Grafik zeigt den geöffneten Twitter-Dialog, nachdem der Twitter-Button ein zweites Mal angeklickt wurde.  
Bildquelle vgl. [Jürgen Schmidt 2011]

2014 wurde die ursprüngliche Zwei-Klick-Methode von heise online weiterentwickelt. Die neue Variante namens Shariff ist einfacher gestaltet, spart den Aktivierungsklick ein, ist im Design der Buttons freier und sendet weiterhin erst Daten an das entsprechende soziale Netzwerk, wenn der Button vom User aktiv angeklickt wird.<sup>125</sup>



Abbildung 2.12: Die Grafik zeigt die mit Shariff integrierten Schaltflächen von Facebook, Twitter und Google-Plus auf heise online.  
Bildquelle vgl. [Daniel Berger 2014]

<sup>125</sup>vgl. [Daniel Berger 2014]

In Österreich setzte 2011 u.a. der Informationsdienst "futurezone.at" die "Zwei-Klick-Lösung" ein, wie man im folgenden Screenshot anhand der Mouse-Over-Informationen bei den entsprechenden Schaltflächen und dem hinzugefügten Informationsbutton erkennen kann. In der Zwischenzeit (Stand Jänner 2016) wurde die "Zwei-Klick-Lösung" auf futurezone.at mit einem Sammel-Social-Media-Button von AddThis ersetzt.

The screenshot shows the website 'futurezone.at' with a search bar and navigation menu. The main article is titled 'Datenschützer erhöht Druck gegen Like-Button' (Data protection officer increases pressure against Like button) and is dated 05.10.11, 13:00. The article discusses the German data protection officer Thilo Weichert's concerns about Facebook's 'Gefällt mir' button. A red box highlights a text box that explains the 'Zwei-Klick-Lösung' (two-click solution): 'ZWEI KLICKS für mehr Datenschutz! Der 1. KLICK stellt die Verbindung zu Facebook her. Für die Empfehlung ist ein 2. KLICK notwendig. So können ohne Ihre Zustimmung keine Daten an Facebook übertragen werden. Details siehe i-Button.' Below the text box are social media sharing buttons for Google Plus, Twitter, Facebook, and a printer icon.

Abbildung 2.13: Die Grafik zeigt die inaktiven Buttons von Google-Plus, Twitter und Facebook auf futurezone.at 2011. Der Facebook-Button und der entsprechende Informationstext zur "Zwei-Klick-Lösung" werden rot umrandet dargestellt.

Bildquelle vgl. [dpa 2011a]

DEUTSCHLAND

## Datenschützer erhöht Druck gegen Like-Button

Letztes Update am 05.10.11, 13:58 [Mail an die Redaktion](#)

DEUTSCHLAND

E-Mail  
Jappy Ticker  
Favoriten  
Reddit  
Drucken  
Blogger  
Mehr... (274)

DEUTSCHLAND

Datenschützer erhöht Druck gegen Like-Button

KOMMENTARE

MEHR ZUM THEMA

Die Datenschützer Thilo Weichert wendet sich an öffentliche Stellen wie die Landeszentrale für Medien und Kommunikation (LMK), FACEBOOK, PRIVATSPHÄRE

Steins Datenschützer Thilo Weichert erhöht den Druck im Kampf gegen Facebooks „Gefällt mir“-Button. Er hat noch sollten Briefe an öffentliche Stellen wie die Landeszentrale für Medien und Kommunikation (LMK) herausgehen, die einen „Gefällt mir“-Knopf oder die Facebooks weltweit größten Online-Netzwerk nutzen, teilte das Unabhängige Landeszentrum für Datenschutz (ULD) auf Anfrage mit.

Weichert kritisiert, bei den Buttons oder Fanseiten würden auch solche Daten übermittelt, die nicht in der Einwilligungserklärung von Facebook stünden. Insofern werde gegen den Datenschutz verstoßen. Auch Unternehmen sollen in diesen Tagen erneut ermahnt werden, Buttons und Fanseiten zu löschen oder zu deaktivieren. Noch in dieser Woche werde Weichert ein Gespräch in der Staatskanzlei über das Problem führen.

### Mehr zum Thema

- [Datenschützer weiter gegen "Gefällt mir"-Knopf](#)

[DPA] ERSTELLT AM 05.10.2011, 13:00

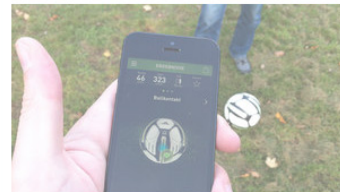
Computer installieren?

futurezone

tech-service

POWERED BY extendIT

### FEATURED



FUSSBALL-TRAINER  
Adidas Smart Ball im Test: Gute Tipps für satte Schüsse

Abbildung 2.14: Die Grafik zeigt rot umrandet den Sammel-Social-Media-Button von AddThis auf futurezone.at 2016.

Bildquelle vgl. [dpa 2011b]

AddThis stand aufgrund des Einsatzes von Canvas Fingerprinting unter Kritik<sup>126</sup>. Das Unternehmen verlangt laut seinen "Terms of Service" von seinen Kunden, dass sie auf ihrer Website über die Nutzung von AddThis-Diensten aufmerksam machen.<sup>127</sup> In den AGBs von futurezone.at wird unter dem Punkt "IV. Registrierung und Datenschutz" aber nicht darauf hingewiesen. Im Gegenteil, unter Artikel 8 steht sogar, Social-Media-Buttons wären erst nach Anklicken aktiv und würden davor keine Daten an das jeweilige soziale Netzwerk schicken:

*"[...] Programme/Plug-ins sozialer Netzwerke wie Facebook, Twitter etc. werden erst durch Anklicken des jeweiligen graphischen Symbols (zB "Gefällt mir"-Button von Facebook) aktiviert. Die Verbindung zum Anbieter des jeweiligen sozialen Netzwerks wird daher nicht automatisch, sondern erst infolge Anklickens des betreffenden Symbols hergestellt. Sofern der Nutzer zu diesem Zeitpunkt in seinem Benutzerkonto auf der Dritt-Website eingeloggt ist (zB Facebook-Konto), kann letztere den Besuch des Nutzers auf den Portalen des Betreibers dem externen Benutzerkonto zuordnen. [...]"<sup>128</sup>*

Sowohl der aktivierte "Schutz vor Aktivitätenverfolgung" durch den Firefox Browser, wie auch das Firefox-Add-on "Ghostery"<sup>129</sup> blockieren Trackingelemente von u.a. Facebook, Google, Twitter und AddThis auf den Seiten von futurezone.at. Im Gegensatz zu der Datenschutzerklärung in den AGBs werden sehr wohl alleine durch das Laden einer Webseite von futurezone.at Daten an soziale Netzwerke übermittelt.

---

<sup>126</sup>Siehe Kapitel 2.2.10 *Canvas Fingerprinting* auf Seite 34.

<sup>127</sup>vgl. [AddThis 2014]

<sup>128</sup>Zitat von [Futurezone GmbH], Registrierung und Datenschutz

<sup>129</sup>Technische Maßnahmen gegen Tracking Technologien werden im Detail im Kapitel 3.3.1 *Einstellungen im Browser* und im Kapitel 3.3.2 *Browsererweiterungen* ab Seite 111 besprochen.

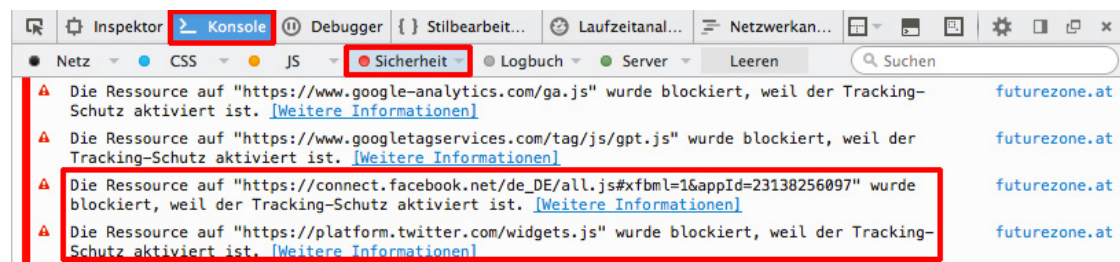


Abbildung 2.15: Die Grafik zeigt rot umrandet die Sicherheitseinträge in der Firefox Web-Entwickler Konsole zu Facebook und Twitter auf der Homepage von futurzone.at, die vom Schutz vor Aktivitätenverfolgung von Firefox blockiert wurden.

Bildquelle vgl. [Futurezone GmbH ]



Abbildung 2.16: Die Grafik zeigt rot umrandet die Ersatzbuttons durch Ghostery von Facebook und Twitter auf der Homepage von futurzone.at und den Infotext des Mouseovers beim blockierten Facebook-Button.

Bildquelle vgl. [Futurezone GmbH ]

Facebook, Google-Plus und Co. setzen einerseits First-Party-Tracking bei ihren eigenen Webdienstleistungen ein und fungieren andererseits als Third-Party-Tracker auf anderen Websites, die sich ihrer Elemente bedienen oder mit ihnen kooperieren. Facebook verwendet zum Beispiel auf seinem eigenen Portal ausschließlich "First-Party-Tracking". Abgesehen davon, dass man beim Registrieren auf Facebook Personendaten angibt und Facebook alle Daten auswerten kann, die ein User freiwillig über das Netzwerk mitteilt, wird bei jedem Login protokolliert, wie und wofür man den Dienst in Anspruch nimmt. Zum Beispiel welche anderen Personenprofile oder Fanseiten besucht werden, welche Werbeanzeigen angeklickt werden oder mit welchen anderen Facebook-Mitgliedern man interagiert. Dies wird dazu benutzt, um Facebook zu verbessern und benutzerfreundlicher zu machen, und mit den Daten wird ein detailliertes Userprofil erstellt, das zur Vermarktung und Platzierung personalisierter Werbung dient.

Facebook fungiert wie zuvor beschrieben mittels seiner "sozialen Plug-ins" ("Gefällt mir", "Teilen", "Login", etc.) auch als Drittanbieter und kann so außerhalb des Netzwerks weitere relevante Informationen in Erfahrung bringen und seine Benutzerprofil-Datenbank erweitern.<sup>130</sup>

Unter dem Menü "Einstellungen" beim jeweiligen Profil des eingeloggten Users gibt es Anpassungsmöglichkeiten für "Werbeanzeigen". Hier kann der auf Facebook registrierte Benutzer zum Beispiel bestimmen, dass er keine personenbezogene Werbung auf Facebook sehen möchte, die auf dessen Surfverhalten außerhalb von Facebook beruht. Weiters kann der User Einfluss darauf nehmen, welchen Werbekategorien er von Facebook zugeordnet wurde. Alle vorgenommenen Einstellungen haben nur Einfluss darauf, ob der Anwender auf sich zugeschnittene oder allgemeine Werbung eingeblendet bekommt. Der User hat keine Möglichkeit Werbung vollständig zu unterbinden oder Facebook zu untersagen Profiling zu betreiben.

Die Electronic Frontier Foundation hat 2013 einen Artikel<sup>131</sup> veröffentlicht, worin sie beschreiben, wie Facebook durch die Zusammenarbeit mit Datenhändlern indirekt noch mehr Geld verdient. Es gibt Unternehmen, die sich darauf spezialisiert haben, Offline- sowie Online-Daten von Personen zu sammeln und mit diesen Daten, wie mit einer Ware oder einem Produkt, zu handeln. Facebook arbeitet mit mehreren großen Datenhändlern zusammen, neben wie bereits erwähnt Acxiom, befindet sich darunter auch die Firma "BlueKai". BlueKai fungiert selbst als Drittanbieter auf Websites und platziert Werbeanzeigen, die wiederum dazu dienen das Surfverhalten der Website-Besucher zu protokollieren. Durch die Kooperation von Facebook und BlueKai werden die Daten beider Unternehmen miteinander verknüpft. Durch Geschäftsbeziehungen dieser Art kann Facebook über sein eigenes Tracking hinaus, noch besser angepasste Werbung platzieren und dadurch auch mehr erwirtschaften. BlueKai wurde im Februar 2014 von Oracle aufgekauft<sup>132</sup>, ob Oracle weiterhin mit Facebook kooperiert ist offen.

---

<sup>130</sup>vgl. [Facebook 2015a]

<sup>131</sup>vgl. [Opsahl et al. 2013]

<sup>132</sup>vgl. [Oracle 2014]



### 2.2.13 Tracking mittels Internetdienstanbieter

Im Februar 2008 wurde bekannt, dass die drei größten britischen Internetprovider mit der Firma "Phorm" einen Vertrag abgeschlossen hatten, der dieser erlaubte, alle Online-Aufrufe über den jeweiligen Internetanbieter kundenspezifisch zu analysieren. Die von Phorm eingesetzte Technologie ermöglichte die Erstellung detaillierter Kundenprofile anhand unter anderem aller besuchten Webseiten oder gesetzten Suchabfragen. Diese Profile wurden von Phorm weitervermarktet, indem sie mit den gewonnenen Informationen eine bestmögliche Platzierung von personalisierter Werbung anbot.<sup>133</sup>

Die Internetdienstanbieter profitierten davon, dass sie einer außenstehenden Firma erlaubten, über ihr Netzwerk das Onlineverhalten ihrer Kunden zu überwachen, zu analysieren und die daraus generierten Daten an Dritte weiterzuverkaufen. Die Kunden bezahlten nicht nur für die Internetverbindung, sondern indirekt auch dafür, dass sie sich unwissentlich ausspionieren ließen.<sup>134</sup> Der Unterschied zwischen der Technologie von Phorm und anderen Drittanbietern ist, dass diese den User nur über jene Onlinedienste verfolgen können, wo zum Beispiel ihre Werbeanzeigen platziert sind und der User diese besucht. Diese Drittanbieter können Userprofile nur anhand der besuchten Webseiten erstellen, die ihre Trackingelemente integriert haben. Phorm hingegen konnte, dadurch dass es direkt mit dem Internetprovider kooperierte, das gesamte Userverhalten analysieren.<sup>135</sup>

Nach dem Bekanntwerden der Vorgehensweise, kam es in Großbritannien seitens der Datenschützer zu heftiger Kritik, bezüglich der Kooperation zwischen Internet Providern und Phorm und deren Eingriff in die Privatsphäre der User. Das ursprüngliche System ermittelte Daten ohne dem Wissen oder dem Einverständnis der Kunden. Weiters wurde publik, dass einer der Internetdienstanbieter bereits in den Jahren 2006 und 2007 die Leistung des Phorm-Systems aktiv an seinen Kunden getestet hatte, ohne diese darüber zu informieren, dass ihr Surfverhalten analysiert wurde. Auch die Europäische Kommission blieb in diesem Fall nicht tatenlos und forderte eine Untersuchung zur Einhaltung des EU-Datenschutzrechts an.<sup>136</sup>

<sup>133</sup>vgl. [derstandard.at Redaktion 2008]

<sup>134</sup>vgl. [Gibson Research Corporation 2008a]

<sup>135</sup>vgl. [Gibson Research Corporation 2008b]

<sup>136</sup>vgl. [Die Presse, Oliver Grimm 2009]

Auf die Klage der EU gegen die Britische Regierung, aufgrund mangelnder Umsetzung europäischer Privatsphäre-Gesetze, reagierte im Juli 2009 der größte britische Internetanbieter mit der Bekanntgabe, die Zusammenarbeit mit Phorm zu beenden und dessen Technologie nicht weiter einzusetzen. Ihm folgten ebenfalls die anderen zwei Dienstleister, die ihre Kooperation mit Phorm lösten.<sup>137</sup>

2012 informierte Phorm über seine Privacy Policy, dass das Unternehmen ein Opt-In-System anböte und seine Geschäftspartner dazu verpflichtete, Kunden über den Einsatz von Phorm-Technologie zu informieren und eine Zustimmung für deren Verwendung einzuholen.<sup>138</sup> In der aktuellen Version (Stand Jänner 2016) wurde das Opt-In-System mit einem Opt-Out ersetzt und eine Weitergabe von Informationen oder das Einholen einer Zustimmung werden nicht mehr erwähnt.<sup>139</sup>

2008 erhielten die beiden österreichischen Internetprovider UPC und Telekom Austria einen Big Brother Award in den Kategorien "Kommunikation und Marketing" (UPC) und "Publikumspreis" (Telekom Austria) wegen Weitergabe von Kundendaten. Die Big Brother Awards wurden erstmals 1998 in London vergeben und von Simon Davies, dem Direktor der internationalen Organisation Privacy International, erfunden. In Österreich werden sie seit 1999 jährlich am 25. Oktober an jene Personen, Firmen, Organisationen oder Behörden vergeben, die sich negativ im Bereich Datenschutz und Wahrung der Privatsphäre hervorgetan haben. 2011 erhielt UPC eine weitere Nominierung in der Kategorie "Kommunikation und Marketing" aufgrund ihrer Änderungen der Allgemeinen Geschäftsbedingungen. 22 von 24 Klauseln wurden in erster Instanz als gesetzwidrig angesehen.<sup>140</sup>

In der vorliegenden Diplomarbeit wurde die seit 13. Juni 2014 gültige AGB<sup>141</sup> von UPC kontrolliert und festgestellt, dass die von den Big Brother Awards beanstandeten Klauseln aus 2011 weiterhin enthalten sind. Besonders hervorzuheben sind dabei die AGB-Punkte 19.6 bis 19.8, die die Zustimmung zur Weiterverarbeitung von Kundendaten ( Stammdaten wie Name, Adresse oder Kontaktangaben, Verkehrsdaten, weitere personenbezogene Daten wie Geburtsdatum, Beruf oder Bankverbindung) behandeln. Diese werden unter anderem für Dienste mit Zusatznutzen (um welche Dienste es sich dabei handelt wird nicht definiert), zur Markt- und Meinungsforschung oder zur Bonitätsprüfung an Drittunternehmen weitergegeben.

<sup>137</sup> vgl. [unwatched.org , sac 2009]

<sup>138</sup> vgl. [Phorm 2012]

<sup>139</sup> vgl. [Phorm 2015]

<sup>140</sup> vgl. [quintessenz 2015a]

<sup>141</sup> vgl. [UPC Austria Services GmbH 2014]

Dabei beinhalten alle drei Klauseln folgende Angabe:

*”Sie können diese Zustimmung jederzeit schriftlich, mittels Telefax oder E-Mail uns gegenüber widerrufen.”<sup>142</sup>*

Auf die Problematik der Zustimmung mittels einer AGB bzw. deren Widerspruch wird genauer im Kapitel *3.2.1 Nutzungsbedingungen* auf Seite 86 eingegangen.

In diesem Unterkapitel wurde eine Vielzahl an Trackingtechniken vorgestellt und ihr Einsatz anhand von praktischen Beispielen illustriert. Als erstes wurde das grundlegendste, älteste und einfachste Tracking-Element, das HTTP-Cookie, beschrieben. User haben die Möglichkeit mittels Einstellungen im Browser oder zusätzlich installierten Add-ons diese Art von Cookies, egal ob als First- oder Third-Party gesetzt, einfach zu kontrollieren. Dies wird in dem späteren Unterkapitel *3.3 Technische Maßnahmen* ab Seite 110 im Detail erklärt. Anschließend wurden Weiterentwicklungen des HTTP-Cookies, Flash-Cookies, HTML5-Cookies, Etags, Evercookies und Supercookies, bei denen es ein Anwender schon schwieriger hat sie zu umgehen, dargestellt. Weiters wurden Trackingvarianten mittels Web Bugs, History Sniffing, unterschiedlichen Formen von Fingerprinting, Social-Media-Buttons und Internetprovider aufgezeigt.

Es hat den Anschein, dass für jede publik gemachte Trackingart, bereits eine neue, noch invasivere Form im Einsatz ist und längst an der Entwicklung eines weiteren Nachfolgers gearbeitet wird. Die Industrie ist bemüht Trackingtechnologien kontinuierlich weiterzuentwickeln, zu verbessern und neue Mechanismen zu erarbeiten. Wünsche der User, nicht getrackt zu werden, werden von Unternehmen oft ignoriert bzw. werden sogar stärkere Tracking-Elemente konstruiert, die Blockiermechanismen bewusst umgehen sollen. Datenschützer und Forscher liegen stets hinter den technischen Entwicklungen zurück und neue Datenschutzbestimmungen sind immer eine verspätete Reaktion auf bereits vorhandene Tracking-Techniken.

---

<sup>142</sup>Zitat von [UPC Austria Services GmbH 2014], AGB für Kabelprodukte - Klausel 19.6, 19.7, 19.8

Unabhängig von den eingesetzten Technologien stellt Tracking einen Eingriff in die Privatsphäre der Internetuser dar. Denn es wird versucht, so viel wie möglich über eine Person zu erfahren. Dabei findet das Sammeln, Analysieren und Auswerten der Daten größtenteils intransparent im Hintergrund ohne das Wissen des Benutzers statt. Dieser kann bei bestimmten Techniken weder Einfluss auf das Tracking an sich, noch auf das resultierende Ergebnis zu seiner Person nehmen und hat keine Kontrolle darüber, wofür die gespeicherten Daten verwendet werden und welche benachteiligenden Auswirkungen sie auf ihn haben können. Das anschließende Kapitel demonstriert einige bekannte Tracking-Risiken.

## 2.3 Gefahren durch Tracking

*“Personalization’s evil twin is manipulation.”*<sup>143</sup>

Firmen geben meistens bekannt, Trackingmaßnahmen zur Prävention von Internetkriminalität, zur Platzierung maßgeschneiderter Werbeanzeigen, zur Durchführung weiterer Marketingaktionen bzw. zur Meinungsforschung oder zur Analyse der Websitenutzung und der darauf aufbauenden Verbesserung ihrer Services einzusetzen. Was könnte sich eventuell hinter der Aussage ”Verbesserung der Services” verstecken? Wofür können die Ergebnisse der Useranalysen noch eingesetzt werden? Dieses Kapitel soll auf einige bekannte Risiken hinweisen, die durch Usertracking entstehen können. Im Detail wird auf drei konkrete Beispiele eingegangen: Preismanipulation, Personenscoring und Filterblasen.

### 2.3.1 Preismanipulation

Schon wenige Informationen reichen aus, um Websitebesucher unterschiedlich zu behandeln, wie etwa das installierte Betriebssystem (Microsoft Windows versus Apple OS X) oder der eingesetzte Browser (zum Beispiel Safari).

Das Wall Street Journal veröffentlichte im August 2012 einen Online-Artikel, der bekannt machte, wie das Online-Reiseportal orbitz.com das Buchungsverhalten seiner Kunden daraufhin analysierte, ob es sich um einen PC- oder Mac-Anwender handelte und dementsprechend unterschiedliche Reiseangebote empfahl. Das Unternehmen konnte feststellen, dass Apple-Benutzer ca. 30% mehr für Nächtigungen ausgeben und ca. 40% Vier- oder Fünfsternehotels bevorzugen. Das Reiseportal fing daraufhin an, diesen Kunden teurere Reiseoptionen anzuzeigen als im Vergleich PC-Anwendern. Zum Beispiel wurden Hotelangebote unterschiedlich sortiert, wobei Apple-Usern kostspieligere Übernachtungsmöglichkeiten an erster Stelle gereiht wurden.<sup>144</sup>

Angebote oder Produkte unterschiedlich anzuordnen scheint eine harmlose Manipulation zu sein, solange der Kunde die Möglichkeit hat, die Sortierung von ”Relevanz” oder ”beste Ergebnisse” auf ”ab- bzw. aufsteigende Preise” zu ändern.

<sup>143</sup>Zitat von [Nicholas Carr 2010], Tracking Is an Assault on Liberty, With Real Dangers

<sup>144</sup>vgl. [Dana Mattioli 2012]

Es ist gebräuchlich Kosten aufgrund von Nachfrage, Verfügbarkeit, Stückzahl, Lieferanten, saisonalen Schlussverkäufen, Sonderangeboten oder Angeboten von Mitbewerbern zu variieren und laufend anzupassen. Auch personenbezogene Rabatte wie etwa für Kinder, Schüler, Studenten, Senioren oder Gruppen sind regulär und werden akzeptiert. Usertracking ermöglicht eine spezifischere und für den Verbraucher undurchsichtige Art der Preismanipulation. Variablen wie Standort (zum Beispiel: wohnt der Kunde in einem armen oder reichen Viertel), Kreditwürdigkeit (zum Beispiel: Höhe des Einkommens des Kunden) oder Konsumverhalten können in die Preiskalkulation miteinbezogen werden und dazu führen, dass Kunden für das gleiche Produkt unterschiedliche Preise angezeigt bekommen.<sup>145</sup>

Userprofile können sich auch auf das reale, analoge Leben auswirken. Ein weiterer Bericht des Wall Street Journals informiert darüber, wie die Online-Recherche nach einem neuen Auto Auswirkungen auf die Preisverhandlungen mit einem Autohändler haben können. Die folgende Infografik erklärt anhand des Unternehmens Dataium im Detail wie dies ermöglicht wird.<sup>146</sup>

Dataium ist ein amerikanisches Unternehmen, das sich darauf spezialisiert hat, das Online-Kaufverhalten in der Fahrzeugindustrie auszuwerten. Dabei werden monatlich 20 Millionen Konsumenten auf über 10.000 KFZ-Websites getrackt. Die Firma wirbt damit, zukünftige Verkäufe vorhersagen zu können.<sup>147</sup>

---

<sup>145</sup>vgl. [Wolfie Christl 2014]

<sup>146</sup>vgl. [Valentino-DeVries et al. 2012]

<sup>147</sup>vgl. [IHS Automotive 2016]

## HOW THEY KNOW

Dataium, which tracks more than 10,000 car websites, can tie an analysis of online browsing to people's names. Here's how it works.

**1** When you visit certain car-selling websites, Dataium places a tracking file on your computer, called a 'cookie,' that contains a unique ID number.



**2** As you visit more sites, Dataium builds a profile of your shopping behavior.

This is possible because Dataium has computer code on car sites across the Web.

**3** If you have provided your name or email to a car dealer, Dataium can sometimes link its analysis of your Web-surfing to your identity.

If you click on a link in certain emails from the car dealer ...

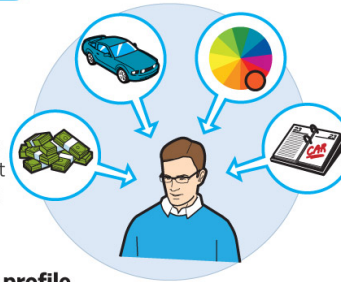
... or if you fill out a form on a dealership site to inquire about a car or get a coupon



**4** When you fill out the form or click the link, Dataium can see that the cookie on your machine is actually tied to you.

The profile that Dataium builds of your online car-shopping might specify, for instance, what cars you have looked at, or whether you are a serious buyer or just window-shopping.

**5** Dataium can provide that car dealership with an analysis of your profile, based on your Web-surfing behavior.



**6** Armed with this information on you, the dealer can know what emails to send you, or how to approach you if you come to the dealership.



Illustrations by Jason Lee The Wall Street Journal

Abbildung 2.17: Die Grafik beschreibt den Prozess, wie das Unternehmen Dataium ein Tracking-Cookie setzt, damit Informationen über das Suchverhalten eines möglichen Kunden sammelt, die Daten mit Echtnamen kombinieren kann und die Datenauswertung potentieller Neukunden an Autohändler vermarktet.

Bildquelle vgl. [Jason Lee 2012]

Die Kammer für Arbeiter und Angestellte für Wien hat im November 2015 vom Österreichischen Institut für angewandte Telekommunikation eine Studie über "Dynamic Pricing - die Individualisierung von Preisen im E-Commerce" durchführen lassen. Dynamic Pricing beschreibt den Prozess, den Preis eines Produkts nicht festzusetzen, sondern ihn variabel zu halten, um rasch auf Veränderungen am Markt reagieren zu können und den Wert dynamisch anzupassen.

Wie weiter oben bereits aufgelistet, ist Dynamic Pricing aus vielen Gründen gelebte Wirtschaftspraxis und vom Kunden akzeptiert. Problematisch stellt sich das dynamische Preismanagement dar, wenn sich Preise individuell am Konsumenten und dessen Kaufverhalten ausrichten. Bestmögliche Gewinnmaximierung stellt den Hauptvorteil für den Einsatz von dynamischer bzw. personenbezogener Preisgestaltung dar. Das Unternehmen riskiert gleichzeitig durch die intransparente Art der Preispolitik Kunden zu verlieren, die sich dadurch zu Recht hintergangen fühlen.

Die Studie kommt zu dem Schluss, dass sich "Personalized Pricing" noch in einer Anfangsphase mit Zukunftspotential befindet. Konsumenten wird geraten Preisentwicklungen über mehrere Tage hinweg zu beobachten, Onlineshops von verschiedenen Endgeräten aus zu besuchen und regelmäßig im Browser den Verlauf und gesetzte Cookies zu löschen, um etwaige Preismanipulationen vorzubeugen.<sup>148</sup>

### 2.3.2 Personenscoring

Als Weiterführung der Preismanipulation kann das sogenannte Kunden- bzw. Personenscoring gesehen werden. Dabei werden detaillierte Userprofile herangezogen, um jemanden einerseits anhand gespeicherter Personendaten zu evaluieren und sogenannte Kundenscores zu ermitteln, andererseits wird versucht konkrete Vorhersagen über eine Person zu treffen und Wahrscheinlichkeiten zu ihrem zukünftigen Verhalten zu berechnen. Enthält das Ergebnis einen Risikofaktor, kann dies zu einer negativen Bewertung und dementsprechenden Auswirkungen für die jeweilige Person führen.<sup>149</sup>

---

<sup>148</sup> vgl. [Österreichisches Institut für angewandte Telekommunikation 2015]

<sup>149</sup> vgl. [ULD 2010]



Bekannte Einsatzbereiche, wo Unternehmen Personenscoring heranziehen, sind zum Beispiel:

- Banken, bedienen sich unter anderem dem Kundenscoring, um anhand des ermittelten Wertes die Kreditwürdigkeit festzulegen und wägen damit die Wahrscheinlichkeit einer vollständigen Kreditrückzahlung eines Bankkunden ab. Dementsprechend können Konditionen eines Kredits bzw. Kreditzinsen individuell angepasst oder gänzlich verweigert werden. Dabei berücksichtigte Merkmale sind etwa die Wohngegend des Kunden, zum Beispiel kann der Bezirk alleine schon ausschlaggebend sein, ob ein Kredit abgelehnt wird oder nicht. Auch bestimmte Vornamen können bei der Vergabe eine Rolle spielen. Wie werden Kunden bewertet, die nach Begriffen wie Schuldenberg, Schuldenberatung oder bankrott auf einer Suchmaschine gesucht haben?<sup>150</sup>

Facebook erhielt 2015 den österreichischen Big Brother Award in der Kategorie "Weltweiter Datenhunger" für die Anmeldung eines Patents zum Kreditscoring seiner Mitglieder. Die Social-Media-Plattform hat vor anhand der verknüpften Daten der jeweiligen Freunde und Kontakte eines Mitglieds dessen Kreditwürdigkeit zu berechnen und den resultierenden Kreditscore zu vermarkten.<sup>151</sup>

- Der Online-Handel setzt Personenscoring zur Prüfung der Zahlungsfähigkeit seiner Kunden ein und erlaubt infolgedessen bestimmten Konsumenten nur eine Bezahlung mittels Vorkasse oder per Nachnahme anstatt der Verwendung einer Kreditkarte.
- Krankenversicherungen könnten anhand des "Wertes" einer Person unterschiedliche Vertragsklauseln oder Preise festlegen. Ausschlaggebende Merkmale können hier zum Beispiel sein, wie oft im Jahr eine Person krankgeschrieben wird, Häufigkeit von Arztbesuchen, welche Ärzte aufgesucht werden, allgemeiner Gesundheitszustand, gesunder/ ungesunder Lebensstil, Ausübung von Sport oder Betreiben von Extremsportarten. Hier kann ebenfalls der Suchverlauf einer Suchmaschine von Relevanz sein. Welchen Score erhält eine Person, die sich über Diabetes, Depressionen, Schlaflosigkeit, Schwangerschaft, Krebs oder ähnliche Gesundheitszustände informiert?

---

<sup>150</sup> vgl. [Fabian Schmid 2015]

<sup>151</sup> vgl. [quintessenz 2015b]

Dazu passend soll ein kurzer Exkurs zu Online-Tracking durch den internationalen Marktführer von Fitness-Armbändern, Fitbit, und dem damit verbundenen Bewegungs-/Aktivitäts-/Schlaf- und Ernährungstracking gegeben werden. Fitbit wirbt etwa mit Gesundheitsprogrammen für Firmen und ihre Angestellten oder Auswertungen für Versicherungen.<sup>152</sup>

**Verbessere die Gesundheit deiner Mitarbeiter. Das wirkt sich auf das ganze Unternehmen aus.**

“ Das Aktivitätsniveau ist rasant gestiegen. Mit diesem Fitbit-Tracker sieht man gleich, wie wenig man sich bewegt. Das motiviert enorm.”  
Janice Barker – PEGASYSTEMS

88% MEHR SCHRITTE MIT FITBIT  
FITNESS MIT FITBIT UM 69% GESTEIGERT

**Jetzt Infos anfordern**

**Angebote für Fitbit @ Work**  
Flexible, skalierbare Lösungen für dein Budget und zur Verbesserung der Gesundheit deiner Mitarbeiter. Das Programm "Fitbit @ Work" beinhaltet Folgendes: Berichte über Mitarbeiterteilnahme, Support vor und nach dem Kauf, Pauschalpreise und bewährte Vorgehensweisen bei der Programmgestaltung.

**Arbeitgeber**  
Lösungen, die sich in deine aktuellen Gesundheitsangebote einbinden lassen oder eigenständig umgesetzt werden können. Motiviere deine Mitarbeiter mit einer anwenderfreundlichen integrierten Plattform und hilf ihnen, ihre Gesundheitsziele zu erreichen.

**Versicherungsunternehmen und Gesundheitsbranche**  
Umfassende und dennoch anwenderfreundliche Tools, die sich in bestehende Programme einbinden lassen und diese ergänzen. Erzielte Fortschritte im Laufe der Zeit anhand zuverlässiger Daten messen.

**Vorteile des Gesundheitsangebots für Unternehmen: Gesundere und damit zufriedenere Mitarbeiter**  
Verbessere die Teilnahme der Mitarbeiter mit einem Gesundheitsprogramm, das funktioniert.

**Weniger** Krankheitstage

**Weniger** gesundheitsbezogene Kosten

**Höhere** Mitarbeiterproduktivität

Abbildung 2.18: Die Grafik zeigt einen Screenshot der Fitbit-Website, die mit Gesundheitsangeboten für Unternehmen und ihre Mitarbeiter und Auswertungsmöglichkeiten für Versicherungen wirbt.

Bildquelle vgl. [Fitbit, Inc. 2016]

<sup>152</sup>vgl. [Fitbit, Inc. 2016]

In Deutschland wurden bereits am 22. April 2016 die diesjährigen Big Brother Awards verliehen.<sup>153</sup> In der Kategorie Verbraucherschutz wurde die Generali Versicherung für ihr Bonuspunkteprogramm mit einem Negativpreis ausgezeichnet. Versicherungsnehmer, die die Versicherung regelmäßig über ihren Gesundheitszustand und ihr Fitnesslevel bzw. sportliche Aktivitäten informieren, erhalten dementsprechende Punkte, die ab einer bestimmten Summe bei Partnerunternehmen der Generali Versicherung eingetauscht werden können. Der spielerische Ansatz verharmlost das eigentliche Datensammeln und den Eingriff in die Privatsphäre der Kunden.<sup>154</sup>

In Österreich bietet unter anderem das Versicherungsunternehmen UNIQA in der Kategorie Gesundheit mit dem VitalPlan und dem VitalPlan PLUS konkrete Vorsorge- und Fitnesspakete zusätzlich zur Krankenversicherung an. Versicherungsnehmer, die den VitalPlan absolvieren und gesetzte Ziele erreichen, werden mit Prämien belohnt. Es ist auf der Website nicht ersichtlich, welche Auswirkungen das Verfehlen der Vorgaben auf die Versicherung hat.<sup>155</sup>

Andere Versicherungsbereiche sind ebenfalls an zusätzlichen Daten ihrer Kunden interessiert, zum Beispiel jene der KFZ-Versicherungen. Die SafeLine-Autoversicherung der UNIQA wurde 2015 in Österreich mit dem Big Brother Award für Business und Finanzen ausgezeichnet. Dabei wird ein GPS-Gerät in das jeweilige Fahrzeug des Versicherungsnehmers eingebaut, welches als Notfall-Knopf, Notrufauslöser bei einem Unfall oder Ortungsgerät bei einem gestohlenen Fahrzeug dienen soll.<sup>156</sup> Das Auswahlkriterium für den Negativpreis der Jury der Big Brother Awards war, dass das Auswerten des Fahrverhaltens des Versicherungsnehmers zu unterschiedlichen Tarifmodellen führt.<sup>157</sup>

Personen, die aus Datenschutzgründen oder anderen Motiven nicht an derartigen Versicherungsprogrammen teilnehmen wollen, könnten als Risiko eingestuft werden und aufgrund dessen schlechtere Konditionen erhalten.

---

<sup>153</sup>In Österreich finden die Big Brother Awards jedes Jahr am 25. Oktober statt.

<sup>154</sup>vgl. [Digitalcourage e.V. 2016]

<sup>155</sup>vgl. [UNIQA 2016b]

<sup>156</sup>vgl. [UNIQA 2016a]

<sup>157</sup>vgl. [derstandard.at 2015]

- Der Personenscore könnte für den Erfolg eines Bewerbungsgesprächs und die Zusage zu einem Stellenangebot ausschlaggebend sein. Es ist mittlerweile üblich, dass das Online-Leben bzw. Social Media Einträge eines Jobbewerbers ausgewertet werden und als Kriterium bei der Stellenvergabe miteinfließen.

Problematisch am Personenscoring sind die zugrundeliegenden statistischen Berechnungen großer Datenmengen. Personen werden dabei häufig auf Stereotype reduziert und individuelle Begebenheiten werden nicht berücksichtigt. Weiters müsste bei diesen Prozessen dafür gesorgt werden, dass die Daten laufend aktualisiert und auf Korrektheit und Vollständigkeit geprüft werden.<sup>158</sup>

Opfer von falschen bzw. schlecht errechneten Scores können eigenständig oder mit Hilfe von Konsumentenschutzorganisationen versuchen in Erfahrung zu bringen, ob Bewertungen der eigenen Person bei einer Entscheidung hinzugezogen wurden und von welchem Urheber, um diesen dann zu kontaktieren und Daten gegebenenfalls korrigieren zu lassen.<sup>159</sup>

Da Data Broker jedoch als Drittanbieter fungieren, führt die fehlende Transparenz dazu, dass Personen meistens nicht wissen, dass außenstehende Firmen Daten über sie sammeln, auswerten, weiter verkaufen und bei Entscheidungsfindungen involviert sind. Die zugrundeliegenden Algorithmen werden als Betriebsgeheimnis angesehen und stehen gesetzlich über den Rechten von Einzelpersonen. Dieser Umstand erschwert zusätzlich das Eingreifen und Korrigieren von fehlerhaften Scores.<sup>160</sup>

### 2.3.3 Filterblase

Der Begriff Filterblase wurde von dem amerikanischen Aktivisten und Autor Eli Pariser geprägt. In seinem 2011 erschienen Buch "The Filter Bubble - What the Internet Is Hiding from You" beschreibt er, wie nicht nur Produkte oder Werbung, sondern auch Informationen für jeden User maßgeschneidert werden.<sup>161</sup>

---

<sup>158</sup>vgl. [Peissl et al. 2014]

<sup>159</sup>vgl. [ULD 2010]

<sup>160</sup>vgl. [Peissl et al. 2014]

<sup>161</sup>vgl. [Eli Pariser 2011]

Google passt seit 2009 seine Suchtreffer an die Person an, die die Suche absetzt. Dazu verwendet der Algorithmus der Suchmaschine über 200 Angaben wie etwa Standort, verwendeter Browser, vorherige Suchen, bereits besuchte Webseiten, PageRank, Tagesgeschehen, um vorherzusagen, welche Treffer am relevantesten für den jeweiligen User sein könnten. Relevant bedeutet für Google, welche Links werden am wahrscheinlichsten angeklickt. Eli Pariser nennt in seinem Buch dazu ein Beispiel, wo zwei seiner Freunde unterschiedliche Treffer für die Suche nach "BP" erhielten. Der Eine sah Nachrichtenartikel zu BP und der Ölpest im Golf von Mexiko aus 2010, dem Anderen wurden wirtschaftliche Kennzahlen zu Investmentmöglichkeiten bei BP angezeigt.

Derstandard.at führte im August 2011 eine Aktion durch, um die Filterblase bei Google Österreich zu veranschaulichen. Über hundert Standard-Leser nahmen daran teil und suchten am selben Tag, zur selben Uhrzeit nach dem Begriff "Hitze" und sendeten einen Screenshot der ersten Trefferseite an die Redaktion. Die Auswertung zeigt, dass sich vor allem Anzahl und Sortierung der Treffer und im Abschnitt News, die ausgewählten Medien, unterscheiden.<sup>162</sup>

Auch Facebook verwendet einen Algorithmus, der die Meldungen im Newsfeed vorsortiert. Dies ist abhängig vom eigenen Userverhalten, den Freunden, geteilten Inhalten, Like-Angaben oder anderen Interaktionen auf der Social Media Plattform. Eli Pariser stellte bei seinem Facebookkonto fest, dass Einträge von konservativen Freunden, deren Beiträge er weniger bzw. gar nicht "teilte" oder mit "gefällt mir" markierte, aus seinem Newsfeed verschwanden und er nur mehr Meldungen angezeigt bekam, die inhaltlich ähnlich zu seinen eigenen waren. Er sieht durch Algorithmen, die dazu dienen, die für uns relevanteren Informationen herauszupicken, die Gefahr einer Einschränkung der objektiven Wahrnehmung und Erzeugung eines Tunnelblicks.

Durch Filterblasen im Internet befürchtet Eli Pariser unter anderem eine Bedrohung des demokratischen Diskurs. Social Media Plattformen werden verstärkt als Nachrichtenquellen herangezogen. Der Newsfeed-Algorithmus von Facebook bestätigt permanent die eigene Meinung, indem jene Meldungen angezeigt werden, die am besten die eigenen Interessen widerspiegeln. So sehen User verstärkt jene Überzeugungen, die sie ohnehin schon vertreten, erfahren keine Gegenargumente und verlieren andere Blickwinkel auf Themen.

---

<sup>162</sup>vgl. [Tatjana Rauth 2011]

Seit knapp einem Jahr beschäftigt unter anderem die Flüchtlingspolitik internationale Medien. Das Thema ist ein gutes Beispiel, wie es durch die Auswahl von Informationsquellen zu Polarisierung und Radikalisierung kommen kann. Spiegel Online berichtet im Jänner 2016 über den Einfluss sozialer Medien auf die Gesellschaft und nennt als Beispiel ein auf Facebook gepostetes, zwei Jahre altes Video mit dem Titel "Muslimischer Asylant schneidet Frau den Kopf ab und ruft Allahu akbar".

Anfängliche Kommentare, die versuchen den Sachverhalt kritisch zu hinterfragen, rücken schnell in den Hintergrund und die Meldung wird mit Entrüstung als real und aktuell wahrgenommen. Das Video ist jedoch zwei Jahre alt, steht mit der derzeitigen Flüchtlingssituation in keinen Zusammenhang, aus dem Video gehen weder die religiöse Angehörigkeit, noch ob es sich um einen Asylanten handelt hervor, "Allahu akbar" wird nicht gerufen.

Meldungen dieser Art schüren Ängste, verbreiten Gerüchte, bestätigen radikale Ansichten und vermehren diese auch. Es ist einfacher, Meldungen zu glauben, die die eigenen Ansichten bekräftigen, als jene, die ihnen widersprechen. Sortieralgorithmen sozialer Medien tragen ihren Teil dazu bei, indem jene Beiträge von Freunden oder abonnierten Seiten und Gruppen vorgereicht werden, die ähnlich denen des Users sind. Dieser sieht seine Einstellung wiederum untermauert und fühlt sich nicht alleine damit.<sup>163</sup>

Filter sind nützlich und wichtig, um in der Informationsflut des Internets nicht unterzugehen. Eli Pariser beschreibt dennoch drei grundsätzliche Probleme von Filterblasen:

- Jede Person besitzt eine individuelle, auf sie zurechtgeschnittene Filterblase. Sie kann mit niemanden geteilt werden.
- Anwender wissen nicht, dass sie sich in einer Filterblase befinden und nach welchen Kriterien die Filter agieren. Es kann kein Einfluss darauf genommen werden, welche Informationen gefiltert werden und welche nicht.
- Filterblasen werden weder aktiv aufgerufen, noch können sie verlassen werden.

---

<sup>163</sup>vgl. [Christian Stöcker 2016]

Anwender gehen davon aus, dass Suchresultate, Informationen, Newsfeeds, etc. neutral erzeugt bzw. gereiht werden und jeder die gleichen Treffer erhält. Der Internetsurfer bemerkt meistens nicht, dass Ergebnisse auf ihn zugeschnitten und Webseiten für unterschiedliche User, verschieden aufgebaut werden. Für Eli Pariser ist es von großer Bedeutung, Filterblasen sichtbar zu machen. Seiner Einschätzung nach täuschen sie unsere Wahrnehmung, gefährden unsere Meinungsvielfalt und Kreativität, manipulieren uns, neue Impulse, divergente Ideen und Alternativen gehen verloren und unpopuläre, aber wichtige Informationen werden verdrängt. Die Präsentation gleicher Inhalte vermehrt sich, wohingegen der Blick über den Tellerrand verloren geht.

Durch die vollständige Personalisierung des Internets und das ununterbrochene Vorhandensein einer individuellen Filterblase, wird es zusehends schwieriger, seinen eigenen Horizont zu erweitern. Für jede Person wird vorausgewählt, welche Informationen und Online-Angebote sie sieht, liest oder hört, ohne dass sie auf die für sie ausgerichtete Selektion Einfluss nehmen kann.

Um Filterblasen teilweise entgegenzuwirken, hilft es regelmäßig im Browser den Suchverlauf und hinterlegte Cookies zu löschen. Weiters ist es ratsam Alternativen zur Google-suche bzw. abwechselnd unterschiedliche Suchmaschinen einzusetzen. Nachrichten sollten nicht via soziale Netzwerke oder herkömmliche Blogs, sondern von journalistisch qualitativen und redaktionell betreuten Presseportalen bezogen werden. Wichtig ist, dass sich der Anwender darüber bewusst ist, dass Filterblasen und ein auf verschiedenen Ebenen auf ihn personalisiertes Internet existieren.

Preismanipulationen, Personenscoring und Filterblasen sind nur drei Beispiele der möglichen Risiken und negativen Auswirkungen von Online-Tracking. Der User hat keine Kontrolle über die von ihm gesammelten und ausgewerteten Daten und welche Konsequenzen daraus für ihn entstehen können. Informationen, die für einen bestimmten Grund eruiert wurden, können leicht zweckentfremdet, missbraucht und mit Werten aus anderen Datenbanken verknüpft werden. Datenskandale, wo Unternehmen gehackt und personenbezogene, sowie sensible Daten gestohlen werden, sind keine Seltenheit. Anfangs anonyme Angaben können dadurch oft deanonymisiert werden.

Diese Hintergründe sollen dazu beitragen die negativ und kriminell behaftete Aussage *"Ich habe nichts zu verbergen."* zu relativieren. Dabei geht es nicht darum, dass Internetuser etwas vor dem Gesetz verheimlichen oder ein Verbrechen begehen möchten. Zu jeder Person existieren Informationen, die nicht geteilt werden möchten bzw. die Entscheidung darüber bei der Person selbst liegen soll. Web-Tracking und daraus resultierende, weit umfassende Persönlichkeitsprofile entbinden Einzelpersonen von dieser Entscheidung, wie auch von der Selbstbestimmung über die eigenen, mitunter sensiblen Daten.

In diesem Kapitel wurde eine Einführung in das Thema Internet-Tracking gegeben. Dabei wurde aufgezeigt welche Datenvielfalt von einem Internetuser gespeichert werden kann, und wie sie zur Kriminalitätsbekämpfung, Website-Analyse und zum User-Profiling bzw. Online-Marketing eingesetzt werden kann. Weiters wurde der Unterschied zwischen First- und Third-Party-Tracking erklärt und die derzeit verbreitetsten Tracking-mechanismen vorgestellt. Abschließend wurde auf die Gefahren von Online-Tracking, Profiling und Personalisierung im Web anhand drei konkreter Beispiele aufmerksam gemacht.

Im nächsten Abschnitt werden gesetzliche, organisatorische und technische Schutzmaßnahmen dargestellt, die dazu beitragen die Privatsphäre im Internet zu sichern und Perspektiven für einen angemessenen Datenschutz zu schaffen.



## 3 Schutzmaßnahmen

*”If users don’t want to be tracked and there is a problem with tracking, then we should regulate tracking, not regulate cookies.”*<sup>1</sup>

Die Studie ”Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning”<sup>2</sup> und deren Folgeartikel ”RESPAWN REDUX”<sup>3</sup> zeigen auf, dass Firmen Tracking-Technologien einsetzen, um bewusst Anti-Tracking-Versuche ihrer User zu umgehen. Wie in Kapitel 2.2 *Tracking-Technologien* ab Seite 20 beschrieben ist es möglich bereits gelöschte Cookies neu zu erstellen oder Tracking relevante Informationen aus anderen Elementen wie zum Beispiel Etags oder anhand des Browser- bzw. Geräte-Fingerabdrucks auszulesen. Es herrscht ein andauernder technischer Wettkampf zwischen Datenschützern und Privatpersonen, die einen Wert auf Online-Privatsphäre legen und Unternehmen, die Trackingtechniken entwickeln und einsetzen. Diesen Schluss ziehen auch die Forscher der Studie ”Web Privacy Census: HTML5 Storage Takes the Spotlight As Flash Returns”.<sup>4</sup>

---

<sup>1</sup>Zitat von [Soltani Ashkan 2009], You Deleted Your Cookies? Think Again

<sup>2</sup>vgl. [Ayenson et al. 2011]

<sup>3</sup>vgl. [Soltani Ashkan 2011]

<sup>4</sup>vgl. [Altaweel et al. 2014]

In diesem Kapitel werden die Grundlagen zum Schutz der Privatsphäre und dem Datenschutz im Internet erörtert. Diese sind in drei Bereiche gegliedert:

- Die gesetzlichen Maßnahmen befassen sich mit den österreichischen Gesetzen zu Datenschutz, Telekommunikation und E-Commerce. Weiters werden Datenschutzbestimmungen in der Europäischen Union und im internationalen Umfeld anhand des umstrittenen "Safe Harbor"-Abkommens und dessen Nachfolger, dem "EU-US Privacy Shield" dargelegt. Um den gesetzlichen Rahmen besser zu verstehen wurde mit ao. Univ.-Prof. Dr. Markus Haslinger an der Technischen Universität Wien ein Gespräch geführt.<sup>5</sup> Der zugrundeliegende Fragenkatalog ist im Anhang dieser Diplomarbeit ab Seite 161 zu finden.
- Die organisatorischen Maßnahmen behandeln die Relevanz von Nutzungsbedingungen und Allgemeinen Geschäftsbedingungen, Datenschutz- bzw. E-Commerce-Gütesiegel und Selbstregulierungssysteme wie zum Beispiel das "Self-Regulatory Program for Online Behavioral Advertising" und dem Platzieren des "Advertising Option Icon (AdChoice)" als Kennzeichnung für interessensbasierte Werbung, sowie etwaige Opt-Out-Varianten.
- Die technischen Maßnahmen geben einen Überblick über die gängigen, in Österreich eingesetzten Browser und beschreiben die Möglichkeiten, wie anhand von Browsereinstellungen oder Erweiterungen die Privatsphäre besser geschützt und allgemein der Datenschutz verbessert werden kann. Dabei werden dementsprechende Browserkonfigurationen aufgezeigt und verschiedene wirksame Browser-Add-ons vorgestellt, wie zum Beispiel Adblock Plus und Ghostery.

### 3.1 Gesetzliche Maßnahmen

Datenschutz liegt einerseits in der Eigenverantwortung eines jeden Einzelnen, wie er mit seinen für ihn schutzwürdigen Daten umgeht. Andererseits ist es die Aufgabe des Staates für einen gesetzlichen Rahmen zu sorgen, um eine missbräuchliche Verarbeitung von Daten, insbesondere jene, die personenbezogen sind, zu verhindern.

---

<sup>5</sup>Ao. Univ.-Prof. Dr. Markus Haslinger unterrichtet an der Technischen Universität Wien im Fachbereich Rechtswissenschaften. Seine Arbeitsschwerpunkte setzen sich aus Öffentliches Recht, Daten- und Informatikrecht, Rechtsfragen des Internet, Rechtsinformationswesen, Vergaberecht, eLearning und Plagiatsproblematik zusammen.

Es existiert kein allgemein gültiges Universalgesetz für den Datenschutz im Internet, nach dem sich der Anwender richten kann. Eine Anzahl von verschiedenen nationalen und internationalen Gesetzen bzw. Richtlinien spielen dabei eine wichtige Rolle. Als österreichischer Internetuser besucht man selten Webseiten, die rein aus dem Heimatland stammen und daher nicht ausschließlich den österreichischen Gesetzen unterliegen. Die grenzenlose Vielfalt an Informationsmöglichkeiten im Internet und deren geschätzter internationaler Charakter tragen dazu bei, dass Anwender beim Surfen im Web mit Datenschutzbestimmungen aus unterschiedlichen Ländern in Berührung kommen.

In Österreich sind die relevantesten Bestimmungen das Österreichische Datenschutzgesetz, das Telekommunikationsgesetz und das E-Commerce-Gesetz. Auf Europaebene sind EU-Gesetze und EU-Richtlinien, die in nationale Gesetze umgewandelt werden von Bedeutung. International ist besonders das "Safe Harbor"-Abkommen zwischen der EU und den USA und dessen Nachfolger, das "EU-US Privacy Shield" entscheidend. Die juristischen Definitionen können für den Laien verwirrend und schwer verständlich sein, weshalb in dieser Diplomarbeit im Anschluss nur ein grober Überblick über die derzeitige Rechtslage gegeben werden kann.

### 3.1.1 Das Österreichische Datenschutzgesetz

In Österreich trat zum Jahresbeginn von 1980 erstmals mit dem Bundesgesetz BGBl. Nr. 565/1978 ein Datenschutzgesetz in Kraft. Dieses wurde von dem überarbeiteten Datenschutzgesetz 2000 (DSG 2000) mit 1. Jänner 2000 abgelöst.<sup>6</sup> Mit dem aktuellen Gesetz wurde die Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates in Österreich realisiert. Diese Richtlinie ist ein EU-weiter Mindeststandard "*zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*".<sup>7</sup>

Das Grundrecht auf Datenschutz des DSG 2000 besagt:

*"Jedermann hat, [...], Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, [...]."*<sup>8</sup>

<sup>6</sup> vgl. [Bundeskanzleramt Österreich 1978]

<sup>7</sup> vgl. [Bundeskanzleramt Österreich 2015a]

<sup>8</sup> Zitat von [Bundeskanzleramt Österreich 2015a], Artikel 1, §1, Absatz (1)

Das DSGVO 2018 definiert personenbezogene Daten wie folgt: *„Angaben über Betroffene [...], deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten [...] dann, wenn der Personenbezug der Daten derart ist, daß [...] die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;“*.<sup>9</sup> Dabei unterscheidet das Gesetz zwischen sensiblen und nicht-sensiblen personenbezogenen Daten, wobei sensible Personendaten einen höheren Schutzwert besitzen.

Nicht-sensible Angaben zu einer Person können zum Beispiel sein:

- Name, Adresse, Telefonnummer, E-Mail-Adresse, Standortdaten eines Mobiltelefons, IP-Adresse
- Geburtsdatum, Alter, Familienstand, Geschlecht
- Staatsangehörigkeit, biometrische Daten (z.B.: Fingerabdruck)
- Sozialversicherungsnummer, Versicherungsdaten
- Kontodaten, Ausgaben, Einkaufsverhalten
- Ausbildung, Titel, Beruf, Einkommen, Arbeitsplatz
- Freizeitverhalten, Kontakte, Interessen, Hobbys

Zu den sensiblen und besonders schutzwürdigen Daten eines Individuums gehören:

- Ethnische und rassische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, Religion, Gesundheit, Sexualleben<sup>10</sup>

Der Autor Rainer Knyrim beschreibt in seinem Datenschutzrecht-Buch die Bedeutung der bestimmten oder bestimmaren Identität: Sie ist bestimmt, wenn Daten eindeutig mit einer Person in Zusammenhang gebracht werden können, zum Beispiel der Name in Verbindung mit dem Geburtsdatum. Die Identität ist bestimmbar, wenn der Anwender Zugriff auf den Schlüssel kodierter Daten erlangen und diese dadurch dekodieren kann bzw. wenn anonyme Daten deanonymisiert werden können.<sup>11</sup>

---

<sup>9</sup>Zitat von [Bundeskanzleramt Österreich 2015a], Artikel 2, §4, Absatz (1)

<sup>10</sup>vgl. [Bundeskanzleramt Österreich 2015a], Artikel 2, §4, Absatz(2)

<sup>11</sup>vgl. [Knyrim Rainer 2003], Seite 15

Die Verarbeitung von Personendaten, egal ob elektronisch oder manuell, ist laut Grundrecht generell untersagt. Das DSG 2000 beschreibt jedoch weiters, dass die Datenverwendung in besonderen Fällen erlaubt und somit auch der Anspruch auf Geheimhaltung aufgehoben werden kann. Einer dieser Gründe ist die Zustimmung durch die jeweilige Person.<sup>12</sup> Laut der Definition des DSG 2000 bedeutet Zustimmung: *„die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt“*.<sup>13</sup>

Mit der Frage, wie eine Zustimmung gesetzeskonform aufgesetzt wird und eingeholt werden darf, hat sich der Verfassungsdienst des Bundeskanzleramtes befasst. Dieser ist unter anderem für Beurteilungen von Gesetzesvorlagen und für Vorbereitungen von Datenschutzbestimmungen zuständig. Im Laufe der österreichischen Rechtsprechung haben sich folgende inhaltliche Bedingungen für die Formulierung von Zustimmungsklauseln herauskristallisiert, die in jedem Fall einzuhalten sind<sup>14</sup>:

- Angabe der Datenarten, kein Überbegriff, sondern eine genaue Auflistung darüber, welche personenbezogenen Daten verarbeitet werden
- Angabe der Empfänger der Daten
- Angabe des konkreten Zwecks der Datenanwendung
- Angabe eines jederzeitigen Widerrufsrechts der Zustimmung des Betroffenen zu der Verwendung seiner Daten

Das Anrecht auf Geheimhaltung und die Untersagung der Datenverarbeitung von personenbezogenen Daten gehen ebenfalls verloren, wenn Daten bereits allgemein verfügbar sind oder individuell nicht zugeordnet werden können.<sup>15</sup> Allgemein verfügbar bedeutet, dass die Daten von der betroffenen Person selbst oder von jemand anderen mit ihrer Erlaubnis veröffentlicht wurden und somit für jedermann zugänglich sind.<sup>16</sup> Dazu zählen insbesondere Angaben im Internet, wie es bei Weblogs, Social Networks wie Facebook oder Twitter, privaten Webseiten, Einträgen in Webforen etc. der Fall ist. Daten können nicht individualisiert werden, wenn sie verschlüsselt sind und die Möglichkeit einer Entschlüsselung nicht gegeben ist oder wenn sie anonymisiert sind.<sup>17</sup>

<sup>12</sup> vgl. [Bundeskanzleramt Österreich 2015a], Artikel 1, §1, Absatz (2)

<sup>13</sup> Zitat von [Bundeskanzleramt Österreich 2015a], Artikel 2, §4, Absatz (14)

<sup>14</sup> vgl. [Knyrim Rainer 2003], Seite 168f

<sup>15</sup> vgl. [Mayer-Schönberger and Brandl2006], Seite 23

<sup>16</sup> vgl. [Knyrim Rainer 2003, Bundeskanzleramt Österreich 2015a], Seite 103f, §8, Absatz(2)

<sup>17</sup> vgl. [Knyrim Rainer 2003], Seite 15

Vorgaben für den Einsatz von Cookies, anderer Trackingtechnologien oder personalisierter Werbung werden im Österreichischen Datenschutzgesetz nicht erwähnt.

Am 15. Dezember 2015 wurde eine neue EU-Datenschutz-Grundverordnung beschlossen, welche 2018 in Kraft treten wird. Dabei handelt es sich vorerst um eine rein politische Übereinkunft, detaillierte Gesetzesvorgaben müssen erst vorgelegt werden.<sup>18</sup> Weder auf der Website des Österreichischen Bundeskanzleramts<sup>19</sup>, dessen Verfassungsdienst für die legislative Umsetzung neuer Gesetzesformen zuständig ist, noch auf jener der Österreichischen Datenschutzbehörde<sup>20</sup> gibt es derzeit (Stand Jänner 2016) Informationen darüber, welchen Einfluss die neue Verordnung auf das Österreichische Datenschutzgesetz nehmen wird und welche Änderungen dadurch entstehen werden. Welche Auswirkungen die Reform des EU-Datenschutzrechts hat, wird im Kapitel 3.1.4 *Internationaler Datenschutz* auf Seite 81 erläutert.

### 3.1.2 Telekommunikationsgesetz

Das aktuelle Telekommunikationsgesetz 2003 (TKG 2003) trat am 20. August 2003 in Kraft und ist eine Erweiterung des DSG 2000. Es ergänzt die vorhandenen Datenschutzbestimmungen unter der Berücksichtigung von elektronischer Kommunikation. Die letzte Änderung des TKG 2003 erfolgte durch die Kundmachung des Bundesgesetzblatts BGBl. I Nr. 134/2015 am 26. November 2015. Mit dem TKG 2003 wurde unter anderem die EU-Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 31. Juli 2002, in der Fassung der Richtlinie 2009/136/EG, ABl. Nr. L 337 vom 18. Dezember 2009, in Österreich umgesetzt.<sup>21</sup>

In den Medien wird diese EU-Richtlinie oft auch als Cookie- oder E-Privacy-Richtlinie bezeichnet, da sie restriktive Vorgaben zum Einsatz von Cookies, zur Erhebung bzw. Verarbeitung personenbezogener Daten im Internet und deren Weitergabe an Dritte enthält. User sollen zum Beispiel die Kontrolle über das Setzen von Cookies haben.

<sup>18</sup>vgl. [Europäische Kommission 2015b]

<sup>19</sup>vgl. [Bundeskanzleramt Österreich 2016]

<sup>20</sup>vgl. [Österreichische Datenschutzbehörde]

<sup>21</sup>vgl. [Bundeskanzleramt Österreich 2015c]

Davon ausgenommen sind Session Cookies oder Cookies, die für das Funktionieren einer Website essentiell sind, wie etwa für die Verwendung eines Warenkorbs oder für ein Login, wie zum Beispiel beim Online Banking.<sup>22</sup>

Die beiden relevantesten Erneuerungen bezüglich der EU-Richtlinie im TKG 2003 sind durch die allgemeinen Datenschutzbestimmungen in Abschnitt 12, §96 beschrieben:

*”Die Übermittlung von [...] Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, [...] erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. [...].”<sup>23</sup>*

Dieser Absatz bedeutet, dass keine Datenweitergabe an Dritte stattfinden darf, außer sie ist für die Erbringung der Dienstleistung notwendig. Zum Beispiel ist es in Ordnung und notwendig, dass ein Online Shop die Kontaktdaten seiner Kunden, die eine Bestellung aufgegeben haben, an einen Paketdienst weitergibt, damit die gekaufte Ware zugestellt werden kann.

*”Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft [...], sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat. [...]. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen [...] zu erfolgen. [...].”<sup>24</sup>*

Dieser Absatz besagt unter anderem, dass der Betreiber einer Website gründlich aufzulisten hat, welche Technologien zur Ermittlung von Benutzerdaten in Gebrauch sind.

---

<sup>22</sup>vgl. [Claudia Glechner, ORF.at 2011]

<sup>23</sup>Zitat von [Bundeskanzleramt Österreich 2015c], Abschnitt 12, §96, Absatz (2)

<sup>24</sup>Zitat von [Bundeskanzleramt Österreich 2015c], Abschnitt 12, §96, Absatz (3)

Das ledigliche Einblenden eines Informationsbanners zur Verwendung von Cookies und eine Beschreibung dieser ist zu wenig. Alle Techniken müssen angegeben werden. Weiters müssen alle Kooperationspartner einer Website, mit denen ein Userdatenaustausch stattfindet, genannt werden. Es muss detailliert dargelegt werden, welche Daten, zu welchem Zweck, verarbeitet werden. Es ist unzureichend, wenn ein Dienstleister beschreibt, dass Daten an Kooperationspartner oder Dritte weitergegeben werden, aber diese nicht namentlich anführt. Weiters muss der Websitebesucher aktiv seine Zustimmung zur Datenverarbeitung geben. Das bloße Aufrufen einer Webseite, wie zum Beispiel einer AGB, ist keine aktive Zustimmung.

Die Bedeutung von AGBs und Nutzungsbedingungen von Websites wird im anschließenden Unterkapitel "Organisatorische Maßnahmen" im Abschnitt *3.2.1 Nutzungsbedingungen* auf Seite 86 erklärt.

Die sogenannte Cookie-Richtlinie wird von den meisten Websitebetreibern mittels Einblenden eines Informationsbanners am oberen oder unteren Rand der Webseite umgesetzt. Obwohl die EU-Richtlinie bereits am 12. Juli 2002 veröffentlicht<sup>25</sup> und Ende 2009 in Österreich umgesetzt wurde, wird erst in den letzten Monaten vermehrt auf Internetseiten darauf reagiert. Im Unterschied zur EU-Richtlinie, wo nicht ausschließlich Cookies beschrieben werden, sondern diese als Beispiel "*solcher Instrumente*" genannt werden und laut TKG vor allem auch transparent über Datenermittlung, Datenverarbeitung und deren Zweck informiert werden soll, reduzieren viele Websites ihre Angaben auf ihren Einsatz von Cookies.

Einblendungen der Art "*Durch die Nutzung unserer Angebote erklären Sie sich mit dem Setzen von Cookies einverstanden. OK*" entsprechen nicht den rechtlichen Erfordernissen. Das Klicken des OK-Buttons ist im Sinne der Richtlinie nicht als Zustimmung zu werten. Der User könnte den Banner auch einfach ignorieren.

Dem Websitebesucher müsste auch die Möglichkeit eines nicht Akzeptierens von Cookies geboten werden. In vielen Fällen wird dem User keine Wahl gegeben.

Noch bevor der User darauf reagieren kann, werden häufig beim erstmaligen Besuch einer Webseite Cookies gespeichert oder findet ein Datenaustausch mit einem Drittanbieter statt (zum Beispiel durch Social-Media-Plug-ins mit Facebook oder mit Google durch den Einsatz von Google Analytics). Dies dürfte laut dem TKG nicht passieren.

---

<sup>25</sup>vgl. [Europäisches Parlament, Rat der Europäischen Union 2002]



Zum Beispiel werden beim initialen Laden der Homepage der österreichischen Technologie-Nachrichtenplattform "futurezone.at" Cookies von knapp 30 Drittanbietern gespeichert. Klickt man beim eingeblendeten Banner *"Cookies helfen uns bei der Erbringung unserer Dienste. Durch die Nutzung unserer Angebote erklären Sie sich mit dem Setzen von Cookies einverstanden."* auf die Schaltfläche "Weitere Informationen", wird das Impressum geladen, wo weder zusätzliche Angaben zu Cookies, noch zu Datenschutzbestimmungen, zu finden sind. Unabhängig davon, ob der User auf den "OK"-Button klickt oder nicht, werden Cookies im Browser gespeichert und findet ein Datenaustausch mit Dritten statt. Der Anwender hat weder seine Zustimmung dazu gegeben, noch kann er Einfluss darauf nehmen. Durch Bestätigen des "OK"-Buttons wird der Banner geschlossen und das Cookie "cookieconsent\_dismissed" gespeichert. "Dismissed" bedeutet übersetzt "abgelehnt, verworfen, abgetan", der Internetuser lehnt durch das Anklicken des "OK"-Buttons aber nicht das Setzen von Cookies ab. Beim Öffnen weiterer Unterseiten von futurezone.at werden erneut Erst- und Drittanbietercookies gespeichert. Alleiniger Zweck des hinterlegten "cookieconsent\_dismissed"-Cookies ist es, dass beim anschließenden Surfen auf futurezone.at der Banner nicht mehr angezeigt wird.

**futurezone** TECHNOLOGY NEWS Netzpolitik B2B Produkte Digital Life Science Meinung Games Apps Start-ups Community

Gefällt mir 17.135 @futurezoneat folgen 19,3 Tsd. Follower Follow 43k A1 AUSTRIA'S NEXT TOP START-UP Ansicht wählen:

**PETER GLASER: ZUKUNFTSREICH**  
**Neoisimus - die ewig neue Krankheit**

NEU MEISTGELESEN MEISTKOMMENTIERT

**LINKSYS**  
 Warum ein elf Jahre alter Router für Millionen-Umsätze sorgt

**SERIAL**  
 Nach 16 Jahren Haft: Podcast verhilft Mann zu neuem Prozess

**KI**  
 Aibo-Nachfolger: Sony arbeitet an neuem Roboter-Haustier

**KOOPERATION**  
 Deutsche Mobilfunker sprechen über Allianz bei Netzausfällen

**FITNESS-TRACKER**  
**Test: Samsung Gear Fit 2 nötigt Boxer zu Yoga**  
 Die Gear Fit 2 ist mit GPS, Pulsmesser und Smartwatch-Funktionen ausgestattet und zeichnet Workouts automatisch auf. Die Akkulaufzeit lässt zu wünschen übrig.  
 von Gregor Gruber

**LINKSYS**  
**Warum ein elf Jahre alter Router für Millionen-Umsätze sorgt**  
 Der Linksys WRT54GL ist einer der beliebtesten Router aller Zeiten - und

**ZYLINDER**  
**Internet rätselt über „Illusion des Jahres“**  
 Rund oder rechteckig? Eine Einreichung beim Wettbewerb für die "Illusion des

**AUTOPILOT**  
**Warum wir für selbstfahrende Autos noch nicht bereit sind**  
 Der Hype um selbstfahrende Autos könnte zum Problem werden. Die

Cookies helfen uns bei der Erbringung unserer Dienste. Durch die Nutzung unserer Angebote erklären Sie sich mit dem Setzen von Cookies einverstanden.  
 Weitere Informationen OK

Abbildung 3.1: Die Grafik zeigt einen Ausschnitt der Startseite der Technologie-Nachrichtenplattform "futurezone.at". Am unteren Rand wird ein Informations-Balken zu Cookies dargestellt.

Bildquelle vgl. [Futurezone GmbH ]

Im Zuge der Diplomarbeit konnten kaum Websites gefunden werden, die dem Besucher mittels dem Banner eine Kontrollmöglichkeit über Cookies bietet. Auf "http://eur-lex.europa.eu", dem EU-Recht-Auskunftsportal, wird dezent am oberen Rand der jeweiligen Webseite auf folgendes aufmerksam gemacht: *"Im Interesse der Benutzerfreundlichkeit verwenden wir auf unseren Seiten Cookies. Möchten Sie sie behalten?"*. Der User kann durch Anklicken der entsprechenden Schaltfläche, Cookies zustimmen oder widersprechen. Daraufhin wird das Cookie "validateConsentCookies" entweder auf "true" oder "false" gesetzt.

Es konnte bei der Kontrolle der beiden Werte jedoch kein Unterschied im Verhalten der Website festgestellt werden. Es wurden übereinstimmend die gleiche Anzahl an zusätzlichen Cookies beim Surfen auf eur-lex.europa.eu gespeichert. Weiters suggeriert der Text *"Möchten Sie sie behalten?"*, dass bei einem Widerspruch bisherige oder weitere Cookies gelöscht werden, dies ist nicht der Fall.

Es existiert eine eigene Webseite zum Cookie-Verhalten auf dem Portal, wo der User ergänzend die Möglichkeit hat, Cookies zu akzeptieren oder abzulehnen. Dabei wird ebenfalls der Wert des Cookies "validateConsentCookies" auf "true" oder "false" gesetzt. Die Art wie Cookies auf der Website hinterlegt werden, ändert sich dadurch weiterhin nicht.<sup>26</sup>

---

<sup>26</sup>vgl. [Europäische Union 2016]

Im Interesse der Benutzerfreundlichkeit verwenden wir auf unseren Seiten Cookies. Möchten Sie sie behalten?

EUR-Lex Über EUR-Lex | Wegweiser | Von A bis Z | Fragen und Antworten | Hilfe | Links | Rechtlicher Hinweis | Cookies | Kontakt | Deutsch (de)

Schnellsuche: Geben Sie Freitext, CELEX-Nummern oder Deskriptoren ein. Verwenden Sie „“ für

Erweiterte Suche

EUROPA > EU-Recht und -Veröffentlichungen > EUR-Lex > Cookies

Startseite | Amtsblatt | EU-Recht und damit verbundene Dokumente | Nationales Recht | Rechtsetzungsverfahren | Mehr

### Cookies

Wenn Sie dieses Portal besuchen, legen wir kleine Dateien – so genannte Cookies – auf Ihrem Rechner oder Ihrem mobilen Gerät ab.

#### Was sind Cookies?

Mit Cookies kann sich das Portal bestimmte Eingaben und Vorlieben über einen bestimmten Zeitraum „merken“, und Sie brauchen diese nicht bei jedem weiteren Besuch und beim Navigieren erneut vorzunehmen.

#### Wie setzen wir Cookies ein?

Unsere Seiten verwenden Sitzungscookies, um beispielsweise Ihre gewählte Sprache und Ihre Einstellungen für die Anzeige von Webseiten zu speichern.

Die Cookie-Informationen werden nicht dazu, Sie persönlich zu identifizieren, und die erfassten Daten über Ihr Surfverhalten auf unserem Portal werden nicht weitergegeben. Die Cookies dienen keinen anderen Zwecken als den hier genannten.

#### Kontrolle über Cookies

Sie können Cookies nach Belieben **steuern und/oder löschen**. Sie können alle auf Ihrem Rechner abgelegten Cookies löschen und die meisten Browser so einstellen, dass Cookies gesperrt werden. Im letzteren Fall müssen Sie jedoch möglicherweise einige Einstellungen bei jedem Besuch einer Seite manuell vornehmen und die Beeinträchtigung mancher Funktionen in Kauf nehmen.

Die Cookies dieses Portals können Sie über die folgenden Links **akzeptieren** oder **ablehnen** : [Cookies akzeptieren](#) / [Cookies ablehnen](#) .

Mein EUR-Lex

- Anmelden
- oder [Registrieren](#)
- Meine Suchanfragen (0)
- Meine Artikel (0)
- Meine RSS-Feeds (0)
- RSS-Feeds
- Anmeldung für Webdienste

Abbildung 3.2: Die Grafik zeigt einen Ausschnitt der Cookie-Bestimmungen auf dem EU-Recht-Auskunftsportal eur-lex.europa.eu. Am oberen Rand wird ein Informations-Balken zu Cookies dargestellt. Am Ende der Bestimmungen werden die beiden Auswahlmöglichkeiten ”Cookies akzeptieren / Cookies ablehnen” angezeigt.

Bildquelle vgl. [Europäische Union 2016]

Dieser Umstand, mit der Bitte um Erklärung, wurde am 8. März 2016 per E-Mail an den EUR-Lex Helpdesk herangetragen. Folgende Antwort wurde am 16. März 2016 gesendet:

*”[...] Um Ihnen die gesamte Cookies-Funktionen zu erklären:  
Der Cookie Speicherplatz hängt davon ab ob Sie die Cookies anhand des Banners annehmen oder ablehnen. Wenn diese angenommen werden, werden diese auf dem lokalen Computer-Harddisk gespeichert; meist nur einen Tag lang und nie mehr als 1 Jahr lang.*

*Allerdings, sollten diese abgelehnt werden werden diese wie folgt gehandhabt:*

*1) Die meisten notwendigen Cookies werden als Session Cookies gespeichert die nach der Session sofort entfernt werden.*

*2) Zwei spezifische Cookies werden unabhängig von der Nutzerentscheidung gespeichert:*

*- "validateConsentCookies" der die Entscheidung zur Annahme oder Ablehnung der Cookies speichert,*

*- "ACOOKIE" der für das Funktionieren unserer statistischen Engine notwendig ist und keine persönliche Daten beinhaltet; dieser verfällt automatisch nach einem Tag.*

*Generell gilt daß der Nutzer alle Cookies ablehnen kann die das Funktionieren der EUR-Lex Webseite nicht verhindern bzw. beeinträchtigen. Nur erforderliche Cookies werden, und dies auch nur kurzzeitig, abgespeichert. Diese notwendigen Cookies beinhalten auch keinerlei Identifikationsdaten bzw. persönliche Daten und diese Cookies stehen auch vollständig unter unserer Kontrolle. Die Cookies werden auch nicht für andere Zwecke verwendet als so wie im Cookie-Politik Abschnitt der Webseite exakt beschrieben. [...]"<sup>27</sup>*

Es fällt positiv auf, dass der EUR-Lex Helpdesk sehr um Transparenz bemüht ist. Die rasche und verständliche Auskunft erklärt deutlich das Cookie-Verhalten auf eur-lex.europa.eu. Beim Großteil der gespeicherten Cookies handelt es sich um Session-Cookies bzw. um Cookies, die für das Funktionieren des Webauftritts notwendig sind. Diese Arten von Cookies sind auch dann erlaubt, wenn ein User Cookies nicht akzeptiert.

Wie detailliert österreichische Internetportale ihre Besucher über etwaige Datenerhebungen informieren, welche davon einen Informationsbanner einblenden und was dieser im Detail aussagt, wird anhand von zehn Beispielen in Kapitel 4 *Trackingbeispiele in Österreich* auf Seite 130 gezeigt.

---

<sup>27</sup>Zitat von [Charley Heuertz], E-Mail des EUR-Lex Helpdesk

### 3.1.3 Das E-Commerce-Gesetz

Das E-Commerce-Gesetz (ECG) dient zur Regelung des Geschäfts- und Rechtsverkehrs im Internet, wie zum Beispiel Vertragsabwicklungen, und trat mit 1. Jänner 2002 in Kraft. Neben dem Begriff "kommerzielle Kommunikation" definiert das Gesetz unter anderem die Ausdrücke "Dienst in der Informationsgesellschaft", "Diensteanbieter", "Nutzer" und "Verbraucher" und enthält eine Regelung zu Online-Werbung.<sup>28</sup>

Der Begriff E-Commerce wird im Allgemeinen hauptsächlich mit dem Handel von Waren mittels Online-Shops in Verbindung gebracht. Jedoch werden nach dem ECG Suchmaschinen und Online-Informationsangebote gewöhnlicher Webseiten ebenfalls als Dienste im Internet hinzugezählt, die dem E-Commerce-Gesetz unterliegen.<sup>29</sup> Somit gelten die Werbe-Bestimmungen auch für diese Websites. Das ECG besagt zum Beispiel, dass Werbung offensichtlich als solche erkennbar sein muss.<sup>30</sup> Siehe dazu die nachfolgende Abbildung 3.3, die einen Screenshot der Startseite von [www.heute.at](http://www.heute.at) und darauf gekennzeichnete Werbeanzeigen zeigt. Jedoch gibt es keine Unterscheidung zwischen herkömmlicher und personenbezogener Werbung. Im E-Commerce-Gesetz wird der Begriff personalisierte Werbung, Richtlinien dazu bzw. eine Kennzeichnung als solche nicht erwähnt.

Dabei ist zu beachten, dass das geltende E-Commerce-Gesetz aus 2002 stammt, wo das Abstimmen von Online-Werbung auf ein Individuum, wie es gegenwärtig im Einsatz ist, noch nicht möglich war. Manche der heutigen Internetriesen und Datenmonopole existierten zu der Zeit noch nicht oder befanden sich noch im Anfangsstadium ihrer Unternehmensentwicklung. Facebook wurde etwa erst 2004 gegründet, AddThis und Twitter in 2006, Google existiert seit 1998. Das Gesetz sollte daher ähnlich wie das Datenschutzgesetz aktualisiert werden und zum Beispiel eine Kennzeichnung personalisierter Werbung einführen.

<sup>28</sup> vgl. [Bundeskanzleramt Österreich 2015b]

<sup>29</sup> vgl. [Bundeskanzleramt Österreich 2015b], Artikel 1, §3, Absatz(1)

<sup>30</sup> vgl. [Bundeskanzleramt Österreich 2015b], Artikel 1, §6, Absatz(1)

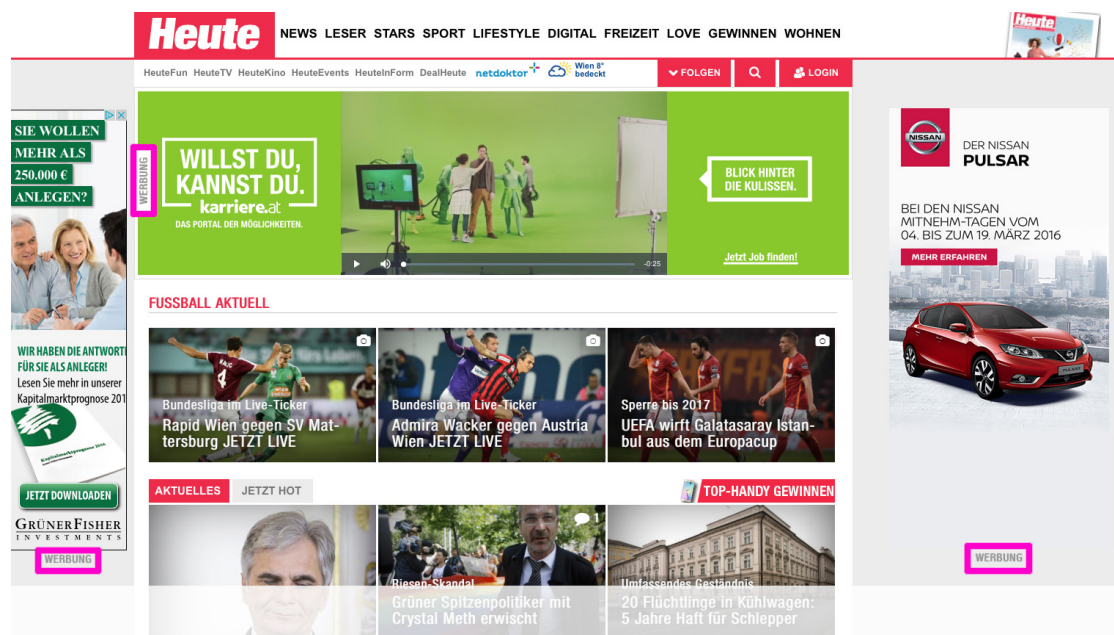


Abbildung 3.3: Die Grafik zeigt einen Ausschnitt der Startseite des Webauftritts der Tageszeitung Heute. Am linken, rechten und oberen Rand wird jeweils eine Werbeanzeige eingeblendet, deren Kennzeichnung ist pink umrandet.

Bildquelle vgl. [Heute 2016]

Abschließend zu den österreichischen Gesetzen soll erwähnt werden, dass in keinem konkret bzw. wörtlich der Einsatz von Trackingtechnologien, wie zum Beispiel Cookies oder die Verwendung von personalisierter Werbung erwähnt wird. Jedoch schreibt das TKG 2003 vor, dass ein Internetnutzer genau darüber informiert werden muss, welche Daten zur Person erhoben und verarbeitet werden. Somit müsste eine Website ihre Besucher explizit darüber informieren, ob Cookies gesetzt werden und zu welchem Zweck bzw. ob andere Trackingtechnologien im Einsatz sind, die personenbezogene Daten generieren können. Weiters sollte der User über die Weitergabe von Daten an Dritte, wie es bei Werbeschaltungen von Drittanbietern oder zum Beispiel durch die Verwendung eines Facebook-Like-Buttons der Fall ist, in Kenntnis gesetzt werden. Wie alle genannten heimischen Gesetze und Vorschriften in der Praxis umgesetzt werden, soll in Kapitel 4 *Trackingbeispiele in Österreich* ab Seite 130 anhand von zehn Beispielen aus der österreichischen Webbranche verdeutlicht werden.

### 3.1.4 Internationaler Datenschutz

Innerhalb der Europäischen Union bietet derzeit die "Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" eine Grundlage für einen einheitlichen Datenschutz. Jeder EU-Mitgliedsstaat hat die Richtlinie anhand eigenständiger Kriterien in nationale Gesetze umgesetzt.<sup>31</sup>

Bereits 2012 wurde eine Neugestaltung des Europäischen Datenschutzrechts durch die Europäische Kommission angeregt, die den technischen Fortschritt und die zunehmende Globalisierung stärker berücksichtigen soll. Es hat drei Jahre gedauert, bis sich am 15. Dezember 2015 das Europäische Parlament, der Europäische Rat und die Europäische Kommission auf eine gemeinsame EU-Datenschutzreform einigen konnten. Der neuen Datenschutz-Grundverordnung wurde Anfang 2016 offiziell zugestimmt.<sup>32</sup>

Am 4. Mai 2016 wurde als Amtsblatt der Europäischen Union der offizielle Text der neuen Datenschutz-Grundverordnung veröffentlicht: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Die neue Verordnung umfasst circa 150 Seiten mit 99 Artikeln. Sie tritt mit 24. Mai 2016 in Kraft und gilt nach einer Übergangsfrist von zwei Jahren ab dem 25. Mai 2018 in allen EU-Mitgliedsstaaten. Die derzeitige Richtlinie 95/46/EG wird mit diesem Stichtag aufgehoben.<sup>33</sup>

Durch die neue Datenschutz-Grundverordnung wird das EU weite Datenschutzrecht modernisiert und innerhalb aller Mitgliedsstaaten der Europäischen Union vereinheitlicht, womit dessen Durchsetzung und Kontrolle vereinfacht wird. Zu den wichtigsten Erneuerungen gehören unter anderem, dass für Unternehmen, deren Firmensitz zwar außerhalb der EU liegt, aber Geschäftsbereiche in der EU haben, ebenfalls das Europäische Datenschutzrecht gilt.

---

<sup>31</sup>vgl. [Europäische Union 1995-2012]

<sup>32</sup>vgl. [Europäische Kommission 2015b]

<sup>33</sup>vgl. [Europäische Kommission 2016]



Die neue Verordnung versucht Datenschutz ebenfalls mittels technischer wie auch organisatorischer Maßnahmen zu regeln. "Privacy by Design" und "Privacy by Default" sollen bei technischen Entwicklungen zum Standard werden und bei der Datenvermeidung bzw. Datensparsamkeit personenbezogener Daten helfen. Der Einsatz von etwa Datenschutzgütesiegel und Selbstregulierungsmaßnahmen wird forciert, wofür geeignete Verhaltensregeln vorgegeben und zusätzlich formuliert werden können.

Zukünftig sollen grundsätzlich so wenig personenbezogene Daten wie möglich verarbeitet werden. Unternehmen müssen gegenüber ihrer Kunden bzw. Anwender eine höchstmögliche Transparenz hinsichtlich ihrer Verwertung von Personendaten darlegen. Den Benutzern werden mehr Rechte eingeräumt, sie sollen eine bessere Kontrolle über ihre Daten erhalten. Zum Beispiel wird das Recht auf Datenberichtigung oder Datenübertragbarkeit eingeführt.

Erstmals kommt in einem Datenschutzgesetz der Begriff "Profiling", das Erstellen von Persönlichkeits- bzw. Interessensprofilen, vor und legt eigene Regelungen dazu fest. Eine Person soll zukünftig darüber informiert werden, wenn Profile anhand ihres Userverhaltens generiert werden, wofür diese Profile anschließend verwendet werden und welche Auswirkungen dies haben kann. Durch Profiling soll der Person gegenüber kein Nachteil entstehen.

Bedeutend ist vor allem, dass einem Unternehmen bei einer Datenschutz-Rechtsverletzung eine Geldstrafe von bis zu 4% des weltweiten Gesamtjahresumsatzes oder 20 Millionen Euro drohen kann, je nachdem welches Bußgeld höher ausfällt. Die im Gegensatz zu den bisherigen deutlich stärkeren Sanktionen sollen dazu führen, dass Unternehmen ihre Datenschutzvorkehrungen ernster nehmen und das Datenschutzgesetz entsprechend umsetzen.<sup>34</sup>

Es ist abzuwarten wie sich in den nächsten Jahren die neue EU Datenschutz-Grundverordnung auswirken wird und welche erhofften Datenschutz-Verbesserungen eintreten werden.

Es gibt Staaten, deren Datenschutzrichtlinien als konform mit denen der Mitgliedsstaaten der Europäischen Union und den zusätzlichen Nationen des Europäischen Wirtschaftsraums, Island, Lichtenstein und Norwegen, erachtet werden. Der EU-Kommission wurde vom Europäischen Rat und dem Europäischen Parlament die Befugnis erteilt, jene Staaten zu bestimmen, die einen äquivalenten Datenschutz besitzen. Dazu gehören momentan Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay und die USA (diesbezüglich ist das "Safe

---

<sup>34</sup>vgl. [Europäisches Parlament und Rat der Europäischen Union 2016], EU DS-GVO

Harbor"-Abkommen bzw. dessen Nachfolger das "EU-US Privacy Shield" relevant, welches im nächsten Abschnitt erklärt wird).<sup>35</sup> In Österreich werden durch den Bundeskanzler die Datenschutzgesetze von Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz und Uruguay ebenfalls als gleichwertig mit den EU-Regelungen erachtet.<sup>36</sup>

Zwischen der EU und den USA bestand seit 2000 das sogenannte "Safe Harbor"-Abkommen, wonach amerikanische Unternehmen bestimmte Auflagen erfüllen mussten, um ein mit der EU übereinstimmendes Datenschutzniveau zu gewährleisten und eine Datenverarbeitung zu ermöglichen. Diese Vereinbarung wurde am 6. Oktober 2015 vom Europäischen Gerichtshof für ungültig erklärt. Am 2. Februar 2016 wurde in Zusammenarbeit von der EU-Kommission und dem amerikanischen Handelsministerium das "EU-US Privacy Shield", als Nachfolger des "Safe Harbor"-Abkommens, präsentiert. Die neue Regelung wird derzeit noch geprüft und ihre Umsetzung ist noch offen (Stand 23. Februar 2016).<sup>37</sup>

Es ist unklar, welche genauen Auswirkungen es für den Datenschutz von Privatpersonen hat, dass das bisherige "Safe Harbor"-Abkommen ungültig und die neue "EU-US Privacy Shield"-Verordnung noch offen ist. Laut einer Statistik von W3Techs speichern 42,7% der laut Alexa zehn Millionen weltweit meistbesuchten Websites ihre Daten auf amerikanischen Servern, weshalb Richtlinien zur sicheren, länderübergreifenden Datenverarbeitung relevant sind.<sup>38</sup>

In der Zwischenzeit ist die Website des ehemaligen "Safe Harbor"-Abkommens weiterhin aktiv und hat sich aufgrund des Urteils nicht wesentlich verändert. Es gibt einen Vermerk zum EuGH-Urteil, aber das US-Handelsministerium betreibt nach wie vor das "Safe Harbor"-Programm mit den ursprünglichen Richtlinien. US-Firmen können sich freiwillig beim Handelsministerium der Vereinigten Staaten für das Abkommen zertifizieren lassen. Um in der "Safe Harbor"-Liste verzeichnet zu werden, muss ein Unternehmen beispielsweise öffentlich in dessen Datenschutzbestimmungen die "Safe Harbor"-Zertifizierung kundtun. Die Zertifizierung muss jährlich neu beantragt werden und richtet sich nach folgenden sieben Grundsätzen<sup>39</sup>:

---

<sup>35</sup> vgl. [Europäische Kommission 2015a]

<sup>36</sup> vgl. [Bundeskanzleramt Österreich 2015d], DSAV §1

<sup>37</sup> vgl. [BfDI 2016]

<sup>38</sup> vgl. [W3Techs 2016a]

<sup>39</sup> vgl. [Export.gov 2016]

- Unternehmen müssen die Betroffenen darüber **informieren**, welche Daten von ihnen gespeichert werden und zu welchem Zweck.
- Unternehmen müssen den Betroffenen die **Wahl** lassen, ob ihre Daten an Dritte weitergegeben oder ebenfalls für andere Zwecke verarbeitet werden dürfen.
- Bei der **Weitergabe** von personenbezogenen Daten an Dritte, muss das Unternehmen darauf achten, dass der Partner ebenfalls zertifiziert ist oder gleichwertige Datenschutzbestimmungen gewährleistet werden.
- Personen muss der **Zugriff** auf die von ihnen gespeicherten Daten ermöglicht werden, auch um eventuelle Falschangaben richtigstellen zu können.
- Unternehmen müssen entsprechende **Sicherheitsvorkehrungen** treffen, um einen Datenmissbrauch, -diebstahl oder -verlust zu verhindern.
- Unternehmen müssen für **Datenintegrität** und somit für eine verlässliche und fehlerfreie Datenverarbeitung sorgen.
- Die **Einhaltung der "Safe Harbor"-Bestimmungen** durch das jeweilige Unternehmen muss jederzeit nachvollziehbar sein.

Viele international bekannte Unternehmen haben die damalige Vereinbarung unterzeichnet und besitzen aktuell eine Zertifizierung, die unter <https://safeharbor.export.gov/list.aspx> abgerufen werden kann. Unter den laut Alexa 100 meistbesuchten Websites Österreichs<sup>40</sup> verfügen folgende amerikanische Unternehmen über ein "Safe Harbor"-Zertifikat: Google Inc. (inkludiert u.a. die Google Tochterunternehmen YouTube und Blogger ), Yahoo! Inc. (inklusive u.a. dem Yahoo Tochterunternehmen Flickr), Microsoft Corporation (gilt u.a. auch für die Suchmaschine bing oder Outlook und das Tochterunternehmen Skype), Facebook Inc., Apple Inc., Adobe Systems Incorporated, Amazon.com Inc. (gilt u.a. ebenfalls für das Tochterunternehmen IMDb), Twitter Inc., Zynga Inc. und LinkedIn Corporation, eBay Inc. und Reddit Inc.

Einige dieser Unternehmen (Google, Microsoft, Facebook, Apple, Amazon, Zynga) ignorieren die derzeitige Ungültigkeit des "Safe Harbor"-Abkommens und gehen in ihren AGBs nicht weiter darauf ein, als hätte es keine Änderung gegeben. Zum Beispiel ist der Datenschutz-Eintrag bezüglich der "Safe Harbor"-Zertifizierung von Google aus 2014 und wurde seitdem nicht aktualisiert.<sup>41</sup>

---

<sup>40</sup>vgl. [Alexa Internet, Inc. 2016a]

<sup>41</sup>vgl. [Google 2014]

Andere, wie etwa Yahoo<sup>42</sup> oder Reddit<sup>43</sup>, vermerken zwar auf das EuGH-Urteil und dass das "Safe Harbor"-Abkommen außer Kraft gesetzt wurde, verweisen aber weiterhin auf die "Safe Harbor"-Zertifizierungsseite des US-Handelsministeriums.

In den Datenschutzerklärungen von Twitter und Ebay wird das Abkommen nicht erwähnt.

Adobe<sup>44</sup> und LinkedIn<sup>45</sup> hingegen gehen detailliert auf das EuGH-Urteil und die Rechtungültigkeit des "Safe Harbor"-Abkommens ein und beschreiben, wie sie durch andere Maßnahmen eine sichere Datenübertragung gewährleisten.

Eine Studie aus Jänner 2015 zeigt, dass es weltweit 109 Länder mit Datenschutzgesetzen gibt und ein weiterer Anstieg prognostiziert wird. Als Vorbild für die meisten Länder gelten die europäischen Datenschutzstandards, deren Datenverarbeitungsrichtlinien und -Restriktionen dadurch global gestärkt werden. Die Studie wurde erstmals 2011 durchgeführt und zeigt die weltweite Entwicklung und Auseinandersetzung mit den Themen Privatsphäre und Datenschutz.<sup>46</sup> Begleitend zur Studie wurde eine Online-"International Privacy Law Library" erstellt, wo alle relevanten Daten abrufbar sind und zum Beispiel auch pro Land entsprechende rechtlichen Grundlagen nachgeschlagen werden können.<sup>47</sup>

Der gesetzliche Rahmen und vor allem die Vielzahl an nationalen und internationalen Datenschutzbestimmungen stellt Privatpersonen, die über kein juristisches Fachwissen verfügen, vor eine große Herausforderung, wie diese Gesetze zu verstehen, einzusetzen oder anzuwenden sind und es lässt die Frage offen, über welche Datenschutzrechte eine Einzelperson im Detail verfügt. Der österreichische Staat, wie auch die Europäische Union und auch Behörden auf internationaler Ebene haben einerseits die Aufgabe, gesetzliche Rahmenbedingungen zum Datenschutz festzulegen und andererseits auch dafür zu sorgen, dass diese eingehalten, kontrolliert und bei etwaiger Verletzung geahndet werden. In Österreich dient die Österreichische Datenschutzbehörde als erster Ansprechpartner und das Österreichische Datenschutzgesetz, das Telekommunikationsgesetz und das E-Commerce-Gesetz bieten die datenschutzrechtlichen Grundlagen. Auf Europaebene wird die Einführung der neuen Datenschutz-Grundverordnung 2018 relevante Änderungen hervorbringen. International wird auch die Regelung des "EU-US Privacy Shield" von Bedeutung sein.

---

<sup>42</sup> vgl. [Yahoo 2015]

<sup>43</sup> vgl. [Reddit, Inc. 2016]

<sup>44</sup> vgl. [Adobe Systems Software Ireland Ltd. 2016]

<sup>45</sup> vgl. [LinkedIn Corp. 2016]

<sup>46</sup> vgl. [Graham Greenleaf 2015]

<sup>47</sup> vgl. [World Legal Information Institute 2016]

## 3.2 Organisatorische Maßnahmen

Das Kundenvertrauen in Online-Unternehmen ist ein wesentlicher Erfolgsfaktor, weshalb mittels organisatorischer Maßnahmen versucht wird, Kunden bestmöglich über Firmenpraktiken zu informieren und dem User freie Entscheidungsmöglichkeiten einzuräumen. Dazu gehören transparente Datenschutzbestimmungen, AGBs und Nutzungsbedingungen, das freiwillige Auferlegen von Datenschutz-Standards via Zertifizierungen und Gütesiegel, sowie die Einhaltung von Selbstregulierungs-Prinzipien, wie etwa das "Self-Regulatory Program for Online Behavioral Advertising" der amerikanischen Marketing- und Werbeindustrie, und etwaigen Opt-Out-Möglichkeiten. Das folgende Kapitel verleiht einen Überblick über gängige Vorgehensweisen und eventuellen Schwächen.

### 3.2.1 Nutzungsbedingungen

Ein Großteil der Website-Betreiber legt für die Verwendung ihrer Seiten bestimmte Regeln, sogenannte Nutzungsbedingungen, fest. Oft werden darin nicht nur die gewünschte Nutzung der Inhalte der jeweiligen Seiten angegeben, sondern auch detaillierte Auskünfte darüber, wie mit den erhobenen Daten der Website-Besucher umgegangen wird. Solche Angaben lassen sich außerdem in den Allgemeinen Geschäftsbedingungen (AGBs) und den Datenschutzrichtlinien (analog zu Datenschutzbestimmungen, Datenschutzhinweis, Datenschutzerklärung oder manchmal nur Datenschutz genannt) finden. Vereinzelt entdeckt man diese Informationen erst nach Aufrufen des Impressums oder der Offenlegung. Auf internationalen, englischsprachigen Seiten wird die Datenverarbeitung persönlicher Informationen unter den "Terms of Use" (dieser Begriff ist gleichbedeutend mit den "Terms of Service") oder schlicht unter "Privacy", "Privacy Policy" bzw. "Privacy Notice" angegeben. Im Englischen wurde ursprünglich zwischen den Begriffen "Datenschutz" und "Privatsphäre" nicht unterschieden, beide wurden mit "Privacy" übersetzt. Inzwischen ist auch die englische Formulierung "Data Protection" etabliert.

Die detaillierte Offenlegung der Datenverarbeitung durch den Internetauftritt eines Unternehmens ist innerhalb der Europäischen Union gesetzlich vorgeschrieben und für Mitglieder des ehemaligen "Safe Harbor"-Abkommens Teil der Zertifizierung. Die Entwicklung der letzten Jahre zeigt, dass Unternehmen vermehrt und fundierter versuchen darüber aufzuklären, welche Datenerhebungen ihrerseits durchgeführt werden. Firmen bemühen sich dadurch einerseits das Vertrauen ihrer Kunden in das Unternehmen zu

stärken, indem sie präzise darüber informieren, wie gespeicherte oder gesammelte Daten verwendet werden. Publik gemachte Datenskandale und Missbräuche von Personendaten können den Ruf einer Firma stark schädigen, und zu Negativ-Werbung und Kundenverlusten führen. Viele Unternehmen setzen sich daher mit bestehenden Datenschutzbestimmungen auseinander, um diese in ihrer Firmenstrategie zu integrieren. Andererseits enthalten Datenschutzrichtlinien oft jene benötigten Zustimmungsklauseln, die Unternehmen rechtlich absichern und deren Anwendungen mit personenbezogenen Daten ermöglichen.<sup>48</sup> Durch das Zustimmung kommt eine Art Vertrag zwischen Anbieter und Nutzer zustande, der den Umgang mit den Personendaten beschreibt.

Meistens kommt ein Internetuser aktiv mit AGBs oder Datenschutzerklärungen beim Registrieren auf einem Webportal in Kontakt und muss diesen zustimmen, um den Dienst nutzen zu können, wie etwa bei Facebook.

Abbildung 3.4: Die Grafik zeigt den Registrierungsschritt auf der Facebook-Homepage, wo man den Nutzungsbedingungen, den Datenschutzrichtlinien und der Bestimmung zur Verwendung von Cookies zustimmt.

Bildquelle vgl. [Facebook 2016]

<sup>48</sup>vgl. [Knyrim Rainer 2003], Seite 159f

Unter der Schaltfläche ist in kleiner Schrift die Information angebracht *”Indem du auf ”Registrieren” klickst, erklärst du dich mit unseren Nutzungsbedingungen einverstanden und bestätigst, dass du unsere Datenrichtlinie einschließlich unserer Bestimmungen zur Verwendung von Cookies gelesen hast.”*<sup>49</sup> Die Wenigsten lesen diese jedoch tatsächlich, da sie oft sehr lang und schwer zu verstehen sind. Will ein User einen Dienst nutzen bleibt ihm ohnedies keine Wahl, als den AGBs zuzustimmen, das vorherige Durchlesen nimmt darauf selten Einfluss

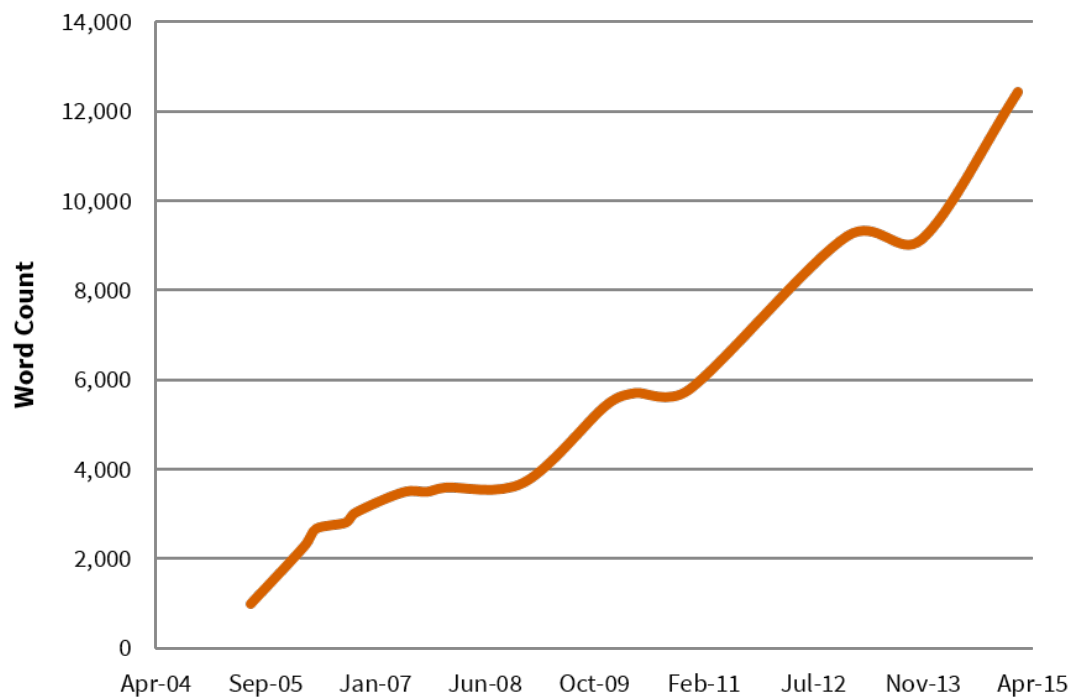


Abbildung 3.5: Die Grafik zeigt die jährliche Erweiterung der Datenschutzbestimmung von Facebook zwischen 2005 und 2015.

Bildquelle vgl. [Shore et al. 2015][Figure 35]

Die Datenschutzerklärung von Facebook begann 2005 mit nur ca. 1.000 Wörter und hat in den darauffolgenden zehn Jahren mehr als 12.000 Wörter erreicht.<sup>50</sup> Selbst wenn ein User vorab die Nutzungsbedingungen, Daten- und Cookierichtlinie gelesen und verstanden hat, ist es damit nicht getan. Eingeloggte Mitglieder sollten sich mit den zusätzlichen Privatsphäre- und Werbeanzeigen-Einstellungen des Facebook-Kontos auseinandersetzen.

<sup>49</sup>vgl. [Facebook 2016]

<sup>50</sup>vgl. [Shore et al. 2015]

Es ist im Allgemeinen empfehlenswert nach einer Registrierung die vorhandenen Kontoeinstellungen durchzugehen und voreingestellte Werte nicht ungeprüft zu übernehmen. Weiters ist es ratsam auf Nutzungsbedingungen zu achten und ebenfalls Aktualisierungen zu kontrollieren, um dementsprechend darauf reagieren zu können.

Anschließend sollen einige relevante Punkte aufgezählt werden, die bei der Entscheidungsfindung, ob man bestimmte Internetdienste aufgrund ihrer Regeln nutzen möchte oder nicht, helfen können:

- Welche Daten müssen tatsächlich bekannt gegeben werden?  
Die Angabe von realen Personendaten ist für die Verwendung eines Internetportals, auch wenn von diesem gefordert, nicht zwingend notwendig. Bei der Erstellung eines kostenlosen E-Mail-Kontos kann es beispielsweise vorkommen, dass nach Name, Adresse und Geburtsdatum verlangt wird. Auch mit falsch ausgefüllten Daten, wird die Dienstleistung korrekt funktionieren. Ein Online-Shop hingegen benötigt reale Personenangaben (wie Name, Adresse, Kreditkartennummer oder Kontodaten), um Verkauf, Versand und Bezahlung erfolgreich abwickeln zu können.
- Welche zusätzlichen Informationen werden von einem User gesammelt, gespeichert, analysiert oder anderweitig verwertet und zu welchem Zweck?  
Zum Beispiel filtert Google bei seinem E-Mail-Dienst Gmail automatisch alle E-Mail-Nachrichten nach Schlagwörtern, um dazu "maßgeschneiderte" Werbung anzuzeigen.<sup>51</sup>
- Werden personenbezogene Daten an Dritte weitergegeben und aus welchem Grund bzw. werden die erhaltenen Daten zu sonstigen Zwecken weiterverwendet?  
Ein Online-Shop wird die Kundenadresse an einen Paketdienst weitergeben, um den Versand abzuwickeln. Aber es ist nicht erforderlich, dass Personendaten an Partnerfirmen für Informationsmaterial zu Werbezwecken übermittelt werden. Google, wie auch Facebook, geben in ihren Datenschutzbestimmungen bekannt, dass sie User-Informationen mit Firmen innerhalb der Unternehmensgruppe bzw. Drittpartnern teilen, um zum Beispiel ihr Service zu verbessern. Weder Google noch Facebook zählen alle Partner detailliert auf. Yahoo macht eine Ausnahme, das als Teil seiner Datenschutzinformationen eine umfangreiche Liste seiner Kooperationspartner, wie etwa Webanalysten oder Werbedienstleister, aufstellt.<sup>52</sup>

---

<sup>51</sup>vgl. [Google 2016c]

<sup>52</sup>vgl. [Yahoo 2016]



- Welche Tracking-Technologien werden eingesetzt? Werden Cookies von Drittanbietern verwendet?

Ein beliebtes Hilfsmittel zur Online-Besucheranalyse ist Google Analytics. Laut einer weiteren Statistik von W3Techs besitzt Google Analytics global einen Marktanteil von rund 83%. Ungefähr 54% aller untersuchten Websites setzen Google Analytics zur Website-Traffic-Analyse ein.<sup>53</sup>

Durch den Gebrauch von Google Analytics wird ein Cookie durch einen Drittanbieter am Rechner des Users gespeichert. Dieser Vorgang sollte in den AGBs enthalten sein.

Dank der sogenannten Cookie-Richtline<sup>54</sup> machen mittlerweile die meisten Unternehmen auf ihren Einsatz von Cookies aufmerksam. Genau genommen sollten alle eingebetteten Trackingtechniken genannt werden. Oft wird jedoch die Formulierung *"Cookies und ähnliche Technologien"* verwendet, ohne auf diese ausführlich einzugehen. Dieser Wortlaut lässt sich bei großen Anbietern wie beispielsweise Google<sup>55</sup>, Facebook<sup>56</sup> oder Microsoft<sup>57</sup> finden.

- Wird personalisierte Werbung angezeigt? Gibt es eine Möglichkeit diese zu deaktivieren?

Der laut Alexa<sup>58</sup> beliebteste Online-Shop Österreichs, Amazon, verwendet etwa getätigte Suchanfragen, Einkäufe und Wunschzetteleinträge um interessensbasierte Werbung zu schalten.<sup>59</sup> Der Kunde hat unter "Mein Konto" → "Mein Amazon.de" → "Personalisierter Inhalt" → "Personalisierte Werbung" die Wahl auf sich zu rechtgeschnittene Werbung zu untersagen.

- Gibt es eine Möglichkeit die gesammelten Benutzerdaten einzusehen und wenn ja diese zu bearbeiten oder zu löschen?

Beispielsweise bietet Facebook unter den Kontoeinstellungen seiner Mitglieder die Möglichkeit an eine Kopie der Facebook-Daten herunterzuladen. Diese enthalten die aktuellen Profilinformationen, alle Pinnwandeinträge, hochgeladene Fotos oder Videos, die aktuelle Freundesliste, alle Notizen, alle Veranstaltungen, alle Nachrichten oder Kommentare des Mitglieds seit seiner Anmeldung bei Facebook. Dies ist jedoch kein vollständiger Einblick in die Datensammlung von Facebook über

---

<sup>53</sup>vgl. [W3Techs 2016b]

<sup>54</sup>Siehe Kapitel 3.1.2 *Telekommunikationsgesetz* auf Seite 71.

<sup>55</sup>vgl. [Google 2015a]

<sup>56</sup>vgl. [Facebook 2015b]

<sup>57</sup>vgl. [Microsoft 2016]

<sup>58</sup>vgl. [Alexa Internet, Inc. 2016a]

<sup>59</sup>vgl. [Amazon.de 2014]

einen User, zum Beispiel werden die gesetzten "Like/Gefällt mir" nicht angegeben. Auf das tatsächliche User-Profil von Facebook wird weder Einblick gegeben, noch hat ein Benutzer die Möglichkeit das Profil zu korrigieren.

Wer ein Google-Konto besitzt erhält über "Mein Konto" → "Persönliche Daten & Privatsphäre" → "Ihre Inhalte gehören Ihnen" unter dem Punkt "Daten herunterladen" und "Archiv erstellen" Zugriff auf jene persönliche Daten, die pro Google-Produkt gespeichert wurden. Auch hier erhält der User keinen vollständigen Blick auf jene Daten, die von ihm gespeichert wurden.

- Welche Sicherheitsvorkehrungen werden von dem Anbieter getroffen, um die Daten zu schützen?

Werden Daten zum Beispiel nicht bis auf Ewigkeit gespeichert, sondern nur für eine notwendige Dauer und anschließend wieder gelöscht? Wird eine sichere Übertragungsart verwendet? Bei zuverlässigen Web-Shops oder auch bei Online-Banking erfolgt die Datenübertragung verschlüsselt. Dies ist unter anderem im Browser in der Adresszeile durch den Einsatz des sicheren Hypertext-Übertragungsprotokoll https erkennbar. Diverse Browser zeigen bei sicheren Verbindungen ein Schlosssymbol an.

- Behält sich ein Unternehmen das Recht vor die gespeicherten Daten zu verkaufen?

Die Initiative "Terms of Service; Didn't Read" hat sich zum Ziel gesetzt, die ihrer Meinung nach größte Lüge im Internet "Ich habe die AGBs gelesen und verstanden" zu eliminieren und versucht eine Hilfestellung beim Verstehen von komplexen Nutzungsbedingungen zu geben. Mittels Browser-Add-ons für Firefox, Chrome, Safari und Opera bietet das Projekt Zusammenfassungen der wichtigsten Punkte einer AGB an, vergibt Bewertungen in einzelnen Kategorien und abschließend eine Gesamtnote von "Class A" (für sehr gute AGBs, Rechte werden respektiert, Daten werden nicht missbraucht) bis "Class E" (die AGBs sind besorgniserregend) und "No Class Yet" (die AGBs wurden noch nicht vollständig überprüft). Das Projekt wurde im Juni 2012 gestartet, folgende bekannte Websites, wie zum Beispiel Google, YouTube, Delicious oder Twitpic, wurden bereits vollständig analysiert. Andere, wie etwa Facebook, Twitter, Yahoo oder Microsoft, haben Einzelbewertungen erhalten und sind noch in Arbeit.<sup>60</sup>

---

<sup>60</sup>vgl. [Projekt Leiter, Hugo Roy]

Um die Komplexität von AGBs zu verdeutlichen wurde in der vorliegenden Diplomarbeit versucht herauszufinden, wie Google bei Gmail Werbeanzeigen schaltet und welche Einstellungsmöglichkeiten ein Anwender dazu hat. Es konnte dazu keine zentrale Website mit allen relevanten Informationen gefunden werden, sondern mindestens sechs Webseiten liefern entsprechende Hinweise. Ausgangspunkt war die Überblicksseite von Googles Datenschutzerklärung und Nutzungsbedingung auf <https://www.google.at/intl/de/policies/>. Daraufhin wurden entsprechende Links und vorgeschlagene Unterseiten von Google geöffnet:

- <https://www.google.com/intl/de/policies/privacy/>  
Die allgemeine Datenschutzerklärung von Google
- <https://www.google.at/intl/de/policies/technologies/ads/>  
Eine zusätzliche Unterseite der Datenschutzerklärung beschreibt die Darstellung von Werbung mittels Google
- <https://support.google.com/ads/answer/1634057>  
Wie Google generell Werbeanzeigen schaltet, u.a. auch bei Gmail
- <https://support.google.com/mail/answer/6603?hl=de>  
Über die Gmail-Hilfeseite, wie Anzeigen in Gmail funktionieren
- <https://privacy.google.com/about-ads.html>  
Website mit Informationen dazu, ob Google persönliche Daten verkauft und daran anschließend wie Werbung auf Google funktioniert
- <https://support.google.com/ads/answer/2662922>  
Mittels der Anzeigen-Hilfezeite, wie interessenbezogene Werbung deaktiviert werden kann

Ein Websitebesucher ist dem Gesetz nach nicht dazu verpflichtet Allgemeine Geschäftsbedingungen/ Nutzungsbedingungen/ Datenschutzerklärungen etc. eines Webportals vollinhaltlich zu lesen. Bei einer Registrierung, wo aktiv eine Bestätigung gegeben werden muss (zum Beispiel durch das Setzen eines Häkchens), dass AGBs etc. gelesen wurden, ist es sinnvoll diese tatsächlich zu lesen. Der User könnte ansonsten Forderungen zustimmen, die später nachteilig für ihn sein könnten.

Folgende Angaben, wie man sie aus gängigen AGBs oder Datenschutzformulierungen kennt, sind dem Recht nach ungültig und nicht datenschutzkonform:

- Mit der Nutzung der Website stimmen Sie den folgenden Bedingungen uneingeschränkt zu.
- Mit der Nutzung dieser Website stimmen Sie der oben beschriebenen Vorgangsweise zur Analyse der Benutzung dieser Website zu.
- Mit dem Aufruf der Website unterwirft sich der User den nachstehenden Bedingungen.
- Nachfolgend bestätigen Sie, dass sie Nutzungs... zur Kenntnis genommen haben und mit diesen einverstanden sind.
- Nutzung der Website ist an AGB gebunden, nicht registrierte User akzeptieren AGB durch Nutzung der Website.

Sätze dieser Art sind nach ao. Univ.-Prof. Dr. Markus Haslinger zu unspezifisch. Der ledigliche Aufruf einer Webseite verpflichtet nicht zum Lesen ihrer AGBs oder Datenschutzbestimmungen, weshalb rechtlich betrachtet keine Zustimmung zustande kommt. Diese hat im Sinne des Datenschutzgesetzes aktiv stattzufinden. Der Benutzer soll vollständig, transparent und völlig unzweideutig über eine Datenverarbeitung informiert werden, um sich der Tragweite einer Einwilligung bewusst sein zu können. Erst danach kann eindeutig entschieden werden, ob einer Datenverarbeitung zugestimmt werden soll. Die Zustimmung muss in jedem Fall eine aktive Handlung sein. Dies ist beim bloßen Laden einer Webseite oder dem Lesen ihrer AGBs keinesfalls gegeben.

Ein Websitebetreiber müsste streng genommen, wenn eine Verarbeitung personenbezogener Daten stattfindet, aktiv die Zustimmung der Anwender einholen, so wie es beim Registrieren verlangt wird. Dies ist jedoch aufgrund mangelnder Sanktionen bzw. fehlender Beschwerden in diese Richtung, keine gelebte Praxis. Der Gesetzgeber könnte zur Verbesserung beitragen, indem zusätzlich zu den Rechtsverordnungen, Textvorschläge angeboten würden, wie sich eine Website korrekt die Zustimmung der Benutzer einholen könnte.

Jede Website verarbeitet auf die eine oder andere Weise Daten von ihren Besuchern. Um eine Vertrauensbasis zu den Nutzern aufzubauen ist es notwendig so transparent und verständlich wie möglich zu sein. In Kapitel 4 *Trackingbeispiele in Österreich* ab Seite 130 wird die Verständlichkeit und der Inhalt der AGBs bzw. der Nutzungsbedingungen von zehn österreichischen Internetseiten analysiert.

### 3.2.2 Datenschutz-Gütesiegel

Die zwei bekanntesten Datenschutz-Gütesiegel sind das amerikanische TRUSTe- und das europäische EuroPriSe-Zertifikat.

Das 1997 gegründete Unternehmen TRUSTe bietet verschiedene Produkte und Dienstleistungen an, die Firmen im Online-Bereich dabei helfen hohe Datenschutzstandards zu setzen und einzuhalten. Die Zertifizierung mit einem TRUSTe-Gütesiegel und die Kontrolle der zugrundeliegenden Anforderungen wird jährlich durchgeführt. Die grundlegenden Kriterien der Zertifikate entsprechen den gesetzlichen Vorgaben der USA. TRUSTe bot auch ein "EU Safe Harbor"-Gütesiegel an und ist seit dessen Ungültigkeit<sup>61</sup> auf eine "EU-US Privacy Shield"-Zertifizierung umgestiegen. Ein Unternehmen mit diesem Kennzeichen zeigt auf, dass es dem "EU-US Privacy Shield"-Abkommen beigetreten ist und die Datenschutzbestimmungen der EU berücksichtigt. Derzeit besitzen mehr als 5000 Webportale ein TRUSTe-Zertifikat, darunter befinden sich bekannte Firmen wie Apple, eBay, Facebook, IBM, LinkedIn oder Zynga. Das Gütesiegel kann in den Datenschutzbestimmungen integriert werden und verweist auf die TRUSTe-Zertifizierungsstelle.<sup>62</sup>

---

<sup>61</sup>Siehe Kapitel 3.1.4 *Internationaler Datenschutz* auf Seite 83.

<sup>62</sup>vgl. [TRUSTe]

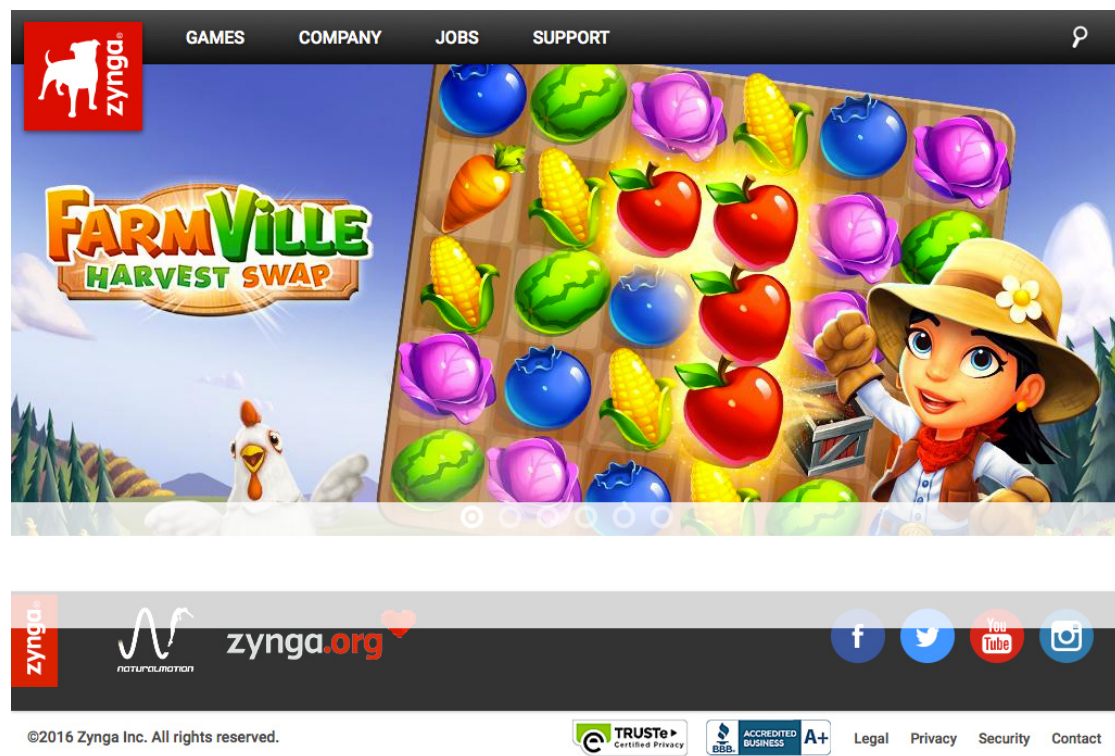


Abbildung 3.6: Die Grafik zeigt das TRUSTe-Gütesiegel klein am unteren Rand auf der Homepage von Zynga.

Bildquelle vgl. [Zynga, Inc. 2016]

**TRUSTe** POWERING TRUST  
in the Data Economy

**Zynga**  
Privacy@zynga.com

**Gültig ab 28.02.16**

Die Datenschutzpraktiken der folgenden Online-Properties wurden von TRUSTe bewertet hinsichtlich Konformität mit:

- + EU Safe Harbor Framework
- + Privacy Certification

**Feedback**

Berichten Sie uns von Ihren Erfahrungen mit Datenschutzpraktiken auf dieser Website:

[Positive Rückmeldung](#) [Eine Beschwerde einreichen](#)

**Need This For Your Business?**  
Demonstrate your commitment to customer privacy - find a TRUSTe solution for your company.

[Get Started >](#)

**Protect Your Privacy Online**  
Consumer tips for internet privacy and safety by TRUSTe.

[Learn More >](#)

**TRUSTe**  
Certified Privacy

Abbildung 3.7: Die Grafik zeigt die TRUSTe-Zertifizierungsbestätigung von Zynga.  
Bildquelle vgl. [TRUSTe 2016]

Das europäische Datenschutz-Gütesiegel EuroPriSe<sup>63</sup> wurde im Rahmen eines von der EU Kommission geförderten Projekts von 2007 bis 2009 entwickelt. Dieses wurde von dem deutschen Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) initiiert. Es kennzeichnet Online-Dienste und IT-Produkte, die sich an die Bestimmungen der europäischen Datenschutzgesetze halten. Unter anderem können Website-Betreiber ein Ansuchen für das Zertifikat stellen und erhalten dieses nach erfolgreicher Erfüllung der geforderten Kriterien, welche innerhalb der Europäischen Union einheitlich sind. Die Kontrolle wird in zwei Stufen von einem autorisierten Gutachter und einer unabhängigen Zertifizierungsstelle regelmäßig durchgeführt. Durchschnittlich erhalten pro Jahr 7 Unternehmen ein EuroPriSe-Gütesiegel. Als eines der ersten Targeting-Unternehmen wurde "nugg.ad" mit dem EuroPriSe-Gütesiegel zertifiziert.

<sup>63</sup>vgl. [EuroPriSe]

Das deutsche Unternehmen hat mit seinem "Predictive Behavioral Targeting" einen Algorithmus entwickelt, der interessensbasierte Werbung in datenschutzkonformer Art anbietet. Personenbezogene Daten werden anonymisiert gespeichert und Werbung wird anhand eines Hochrechnungsverfahrens und Einsatz von Fragebögen zielgruppenorientiert platziert.<sup>64</sup> "Nugg.ad" wurde mehrfach für seine Datenschutzkonformität ausgezeichnet, seit Oktober 2013 trägt es das ePrivacyseal, ein weiteres Datenschutz-Gütesiegel.

The screenshot shows the nugg.ad homepage with the following elements:

- Header:** nugg.ad logo, "predictive behavioral targeting", and language flags (DE, EN, FR, ES).
- Navigation:** "Unternehmen", "Presse", "Partner".
- Sub-navigation:** "VIDEO TOUR", "OPEN TARGETING PLATFORM", "PRODUKTE", "UPDATED!".
- Main Content:**
  - Headline: "We love Branding"
  - Target Audience: "TRAVEL ENTHUSIASTS", "männlich 50+", with interests: Reisen, Kultur, Finanzen, hohes Einkommen, Gesundheit.
  - Text: "Nutzen Sie Europas größte Plattform für Predictive Behavioral Targeting"
  - Image: A smiling man in a Hawaiian shirt.
- Footer/Bottom Section:**
  - Navigation: "ADVERTISERS & AGENCIES", "ADNETWORKS & PUBLISHER", "CONSUMERS", "FACEBOOK", "TWITTER", "BLOGS".
  - "WE'RE HIRING!" with a red arrow.
  - "PREDICTIVE BEHAVIORAL TARGETING" section describing the unique principle of the technology.
  - "DATENSCHUTZ" section with the text: "nugg.ad betreibt datenschutzkonformes Targeting und wurde bereits mehrfach zertifiziert." and a link "mehr...".
  - "European Privacy Seal" logo with text "DE-090007 / Valid till 2011-09".

Abbildung 3.8: Die Grafik zeigt rechts unten das EuroPriSe-Datenschutz-Gütesiegel auf der damaligen Homepage von nugg.ad.

Bildquelle vgl. [nugg.ad 2011]

<sup>64</sup>vgl. [nugg.ad 2015]



### NEUIGKEITEN

22.02.2016

**AKTUELLE NUTZERANALYSE ZEIGT: RUND JEDER FÜNFTE OMS NUTZER IST EIN ENTSCHEIDER AUS KLEINEN UND MITTELSTÄNDISCHEN UNTERNEHMEN**



Gegenüber der bundesweiten Entscheiderdichte in der deutschen Gesamtbevölkerung (vier Prozent lt. LAE 2015 Entscheidungsträger) ist der Anteil an Unternehmensentscheidern unter den Nutzern der mehr als 550 Qualitätsangebote im OMS Digitalportfolio überproportional hoch (19 Prozent). Vier von fünf Entscheidern stammen dabei aus kleinen und mittelständischen Betrieben. Dies belegen die Ergebnisse einer aktuellen Nutzeranalyse, die von „Audience & Research“, der Forschungs-Unit von nugg.ad, im Auftrag des Premiumvermarkters durchgeführt wurde.

### DATENSCHUTZ

nugg.ad betreibt datenschutzkonformes Targeting und wurde bereits mehrfach zertifiziert.



Abbildung 3.9: Die Grafik zeigt rechts unten das ePrivacyseal-Datenschutz-Gütesiegel auf der aktuellen Homepage von nugg.ad.

Bildquelle vgl. [nugg.ad 2011]

Unter den Top 25 Internetseiten Österreichs<sup>65</sup> setzt der Webauftritt der Tageszeitung "Der Standard" nugg.ad für die Platzierung seiner Werbung ein.

The image shows a screenshot of the 'derStandard.at - Impressum' page. At the top, there is a navigation bar with categories like 'International', 'Inland', 'Wirtschaft', 'Web', 'Sport', 'Panorama', 'Etat', 'Kultur', 'Wissenschaft', 'Gesundheit', and 'Bildung'. Below this, there are sub-categories like 'Meinung', 'Blogs', 'dieStandard.at', and 'daStandard.at'. A weather widget in the top right corner shows 'Wien 16°'. The main heading is 'derStandard.at - Impressum' with a timestamp 'REDAKTION, 14. April 2011 12:07'. Below the heading, it says 'Alle Mitarbeiter und Mitarbeiterinnen, alle Kontakte, Copyrightfragen, Blattlinie'. A small photo of a newsroom is visible on the left. Overlaid on the page is a white survey box from nugg.ad. The survey box contains the nugg.ad logo, the derStandard.at logo, and the text: 'Ihre Meinung ist uns wichtig! Machen Sie gemeinsam mit uns Werbung interessanter und persönlicher! Leihen Sie uns fünf Minuten Ihrer Zeit und beantworten Sie bitte einige einfache Fragen. Sie helfen uns ansprechende Inhalte zu entwickeln und gleichzeitig uninteressante oder gar nervige Dinge zu vermeiden. Selbstverständlich behandeln wir Ihre Antworten absolut vertraulich und bringen diese nicht mit persönlichen Daten in Verbindung. Ausführliche Informationen zu den Nutzerrechten und zum Datenschutz finden Sie hier. Herzlichen Dank für Ihre Unterstützung - lassen Sie uns gemeinsam das Internet der Zukunft bauen.' At the bottom of the survey box is a button that says 'Ja, ich mache mit'. Below the survey box, there is a text block: 'Von folgenden Organisationen und Firmen wird ein Cookie gesetzt: Von der ÖWA (www.oewa.at) zur einheitlichen Analyse der österreichischen Mediennutzung im Internet, von NUGG (nugg.ad) zur optimierten Steuerung der Werbung sowie von Google (www.google.at). Die dabei gewonnenen Daten werden anonymisiert gespeichert.'

Abbildung 3.10: Die Grafik zeigt die Impressum-Seite von derstandard.at mit dem eingeblendeten Fragebogen von nugg.ad.

Bildquelle vgl. [derstandard.at GmbH 2011a]

Ein Datenschutz-Gütesiegel soll dazu dienen, das Vertrauen der Internetuser zu besuchten Websites und deren Umgang mit Benutzerdaten zu stärken. Sie symbolisieren qualitative Datenschutzbestimmungen, Transparenz und Einhaltung von gesetzlichen Richtlinien, an denen sich ein Benutzer orientieren kann.

<sup>65</sup>vgl. [Alexa Internet, Inc. 2016a]

Ein weiteres Gütezeichen, das dem Konsumenten speziell beim Einkauf im Internet eine Art Sicherheit versprechen soll, ist das Österreichische E-Commerce-Gütesiegel bzw. das Euro-Label Österreich. Es gehört zum Euro-Label-System, das neben Österreich auch in Deutschland, Polen, Italien, Frankreich und Spanien eingesetzt wird. Zusätzlich zu einem Europäischen Verhaltenskodex, hat jedes Land einen erweiterten Regelkatalog mit nationalen Bestimmungen.<sup>66</sup> Seit 2001 garantiert das Gütesiegel unter anderem dafür, dass laut Österreichs E-Commerce-Gesetz Werbung ersichtlich dargestellt werden muss oder laut Österreichs Datenschutzgesetz personenbezogene Daten nicht zweckentfremdet bzw. die Einhebung und Verarbeitung der Daten deutlich erklärt werden. Das Zertifikat ist jeweils ein Jahr gültig und wird entsprechend jährlich kontrolliert und neu vergeben. Auf der Website des Gütezeichens können alle teilnehmenden österreichischen und europäischen Unternehmen abgefragt werden.<sup>67</sup>

Ebenfalls am heimischen Sektor verbreitet ist das "Trustmark Austria"-Gütesiegel des österreichischen Handelsverbandes, das, ähnlich wie das Österreichische E-Commerce-Gütezeichen, für einen sicheren und gesetzeskonformen Online-Handel wirbt. Die Kriterien für die Zertifizierung richten sich nach EU-Richtlinien und österreichischen Gesetzen. Punkt 4 des "Trustmark Austria"-Verhaltenskodex betrifft etwa Datenschutz und Privatsphäre, welcher Verordnungen zur jeweiligen Datenschutzerklärung eines Unternehmens enthält. Unter anderem werden Grundsätze zum Umgang mit personenbezogenen Daten und Cookies definiert. Auch dieses Internet-Gütesiegel ist für ein Jahr gültig und kann durch eine regelmäßige Kontrolle abermals bescheinigt werden. Zertifizierte Online-Shops können auf der Website von "Trustmark Austria" abgerufen werden.<sup>68</sup>

---

<sup>66</sup> vgl. [EHI Retail Institute GmbH 2016a]


<sup>67</sup> vgl. [Verein zur Förderung der kundenfreundlichen Nutzung des Internet 2016]

<sup>68</sup> vgl. [Handelsverband 2016]

Abbildung 3.11: Die Grafik zeigt die Startseite des Online-Shops der Wiener Linien. Wenn man nach unten scrollt kann man sehen, dass dieser u.a. mit dem Österreichischen E-Commerce- und dem "Trustmark Austria"-Gütezeichen zertifiziert wurde.

Bildquelle vgl. [Wiener Linien 2016]

Die beiden auf der Startseite der Wiener Linien dargestellten Gütesiegel sind anklickbar. Das Österreichische E-Commerce-Gütezeichen verweist auf die Bestätigung der Zertifizierung für den Online-Shop der Wiener Linien, dies kann für den User als eine Art Echtheitsprüfung herangezogen werden. Die daraufhin geladene Webseite enthält Angaben zum Ausstellungsdatum des Zertifikats und Gewährleistungen (siehe folgender Screenshot). Der Link von "Trustmark Austria" führt zu dessen Homepage mit der vollständigen Liste aller zertifizierten Online-Shops.



## ZERTIFIKAT

Euro-Label

---

### Wiener Linien GmbH & Co KG

<b>Internet:</b>	<a href="http://shop.wienerlinien.at">shop.wienerlinien.at</a>
<b>Anbieter:</b>	Wiener Linien GmbH & Co KG Erdbergstraße 202 1030 Wien Österreich
<b>Form des Unternehmens:</b>	GmbH / trust mark ECG-855
<b>(Handels-) Registereintrag:</b>	Österreich, Handelsgericht Wien, 181593z
<b>USt Identifikationsnummer:</b>	ATU 47055001
<b>Zertifiziert seit:</b>	03.01.2012
<b>Warengruppen:</b>	<ul style="list-style-type: none"> <li><input type="radio"/> Reise &amp; Reisebedarf</li> <li><input type="radio"/> Dienstleistung &amp; Service</li> <li><input type="radio"/> Sonstiges</li> </ul>

Tickets online kaufen - einfach und bequem

[Zum Beschwerdeformular](#)

### Online-Shopping mit Fairness & Transparenz

Dieses Zertifikat bestätigt, dass der Shop erfolgreich zertifiziert wurde und autorisiert ist, das Gütesiegel im Shop zu führen. Die Zertifizierung gewährleistet insbesondere

- einen transparenten Bestellvorgang
- vollständige Informationen über Kosten, Kaufvertrag, Lieferung etc.
- Schutz der persönlichen Daten
- neutrales Beschwerdeverfahren durch die Zertifizierungsstelle.

Die Kriterien der Zertifizierung werden laufend weiterentwickelt. Jedes Jahr erfolgt eine vollständige Neuzertifizierung des Shops.

Unser Gütesiegel wird von öffentlichen Einrichtungen empfohlen, darunter das Bundesjustizministerium sowie die Initiative d21, Deutschlands größte Partnerschaft zwischen Wirtschaft und Politik für die Informationsgesellschaft.

**Dieser Shop ist zertifiziert durch:**

**(AT) Öst. E-Commerce Gütezeichen**  
Margaretenstraße 70  
1050 Wien  
Österreich

[www.guetezeichen.at](http://www.guetezeichen.at)

Abbildung 3.12: Die Grafik zeigt die Zertifizierung des Online-Shops der Wiener Linien durch das Österreichische E-Commerce-Gütesiegel.  
Bildquelle vgl. [EHI Retail Institute GmbH 2016b]

Es bleibt zu hinterfragen, wieviel ein Gütezeichen für den Internetnutzer tatsächlich wert ist? Es gibt viele verschiedene E-Commerce-, Privacy- oder Sicherheits-Gütesiegel, die im Internet kursieren. Dabei ist zu beachten, dass sie nicht von der Regierung aufgrund erfüllter Gesetzesvorgaben oder einer unabhängigen Zertifizierungsstelle vergeben werden. Hinter einem Internet-Gütesiegel steht meistens ein Unternehmen, das von dem jeweiligen Website-Betreiber dafür bezahlt wird, die Sicherheitskriterien zu überprüfen und ein Zertifikat auszustellen. Die Vergabe von Gütezeichen ist dessen Geschäftszweig.

Der User sollte einem Gütezeichen daher nicht blind vertrauen, sondern sich darüber informieren, wer bzw. was dahinter steht.

Zum Beispiel kam es 2014 zu einem außergerichtlichen Vergleich zwischen der Federal Trade Commission (FTC) und TRUSTe. Die FTC ist eine unabhängige amerikanische Wettbewerbs- und Verbraucherschutzbehörde. Sie warf TRUSTe vor in einem Zeitraum von sieben Jahren, zwischen 2006 und 2013, bei mehr als 1000 Unternehmen keine jährliche Kontrolle durchgeführt aber dennoch ein TRUSTe-Gütesiegel ausgestellt zu haben. Das Zertifizierungsunternehmen bezahlte eine Strafe von 200.000 US-Dollar.<sup>69</sup>

### 3.2.3 Selbstregulierungs-Systeme

Mit dem verstärkten Einsatz von personalisierter Werbung im Internet, stiegen auch die Bedenken der User, ihre Privatsphäre würde dadurch verletzt werden. Die Federal Trade Commission veröffentlichte 2007 eine Liste von Selbstregulierungs-Prinzipien, um auf die Entwicklung in der Werbebranche aufmerksam zu machen und den Dialog darüber zu fördern<sup>70</sup>. Auf diesen Prinzipien aufbauend wurde das "Self-Regulatory Program for Online Behavioral Advertising" der amerikanischen Marketing- und Werbeindustrie ins Leben gerufen. Konsumenten sollen dadurch besser über personenbezogene Werbung informiert werden und mehr Kontrolle über verhaltensbasierte Werbeanzeigen erhalten. Weiters soll das Sammeln von Personendaten transparenter dargestellt werden und bei sensiblen Informationen, wie etwa dem Gesundheitszustand oder der Finanzlage eines Konsumenten, muss für besonders hohe Datensicherheit gesorgt werden. Durch die genaue Aufklärung über nutzungsbasierte Reklame soll das Vertrauen der Konsumenten in Online-Werbung gestärkt werden.<sup>71</sup>

In Europa pflegt die "European Advertising Standards Alliance (EASA)" einen Selbstregulierungs-Standard, der im April 2011 veröffentlicht wurde. Der Standard soll europaweit gelten, ist aber nicht verbindlich, sondern gilt als Richtlinie, die von den teilnehmenden Werbeverbänden und Unternehmen dem Umfeld entsprechend bestmöglich umgesetzt werden soll. Ihr liegen ebenfalls Prinzipien zugrunde, die mit jenen des amerikanischen "Self-Regulatory Program for Online Behavioral Advertising" vergleichbar sind.<sup>72</sup>

<sup>69</sup> vgl. [heise online, Stefan Krempel 2014]

<sup>70</sup> vgl. [Federal Trade Commission 2007]

<sup>71</sup> vgl. [Digital Advertising Alliance 2010]

<sup>72</sup> vgl. [European Advertising Standards Alliance 2011]

Das "Interactive Advertising Bureau (IAB)" ist einer der am amerikanischen Selbstregulierungs-System beteiligten Werbeverbände. Ihm gehören eine Vielzahl der führenden Medien und IT-Unternehmen an, darunter befinden sich Amazon, ebay, Facebook, Google, LinkedIn, Microsoft Advertising, Pinterest, Twitter oder Yahoo. Gemeinsam sind sie für den Großteil der Online-Werbung in den USA verantwortlich. Alle Mitglieder des IAB sind dazu verpflichtet sich an den IAB-Verhaltenskodex zu halten. Dieser beinhaltet neben den grundlegenden Prinzipien des "Self-Regulatory Program for Online Behavioral Advertising" auch das Platzieren des "Advertising Option Icon (AdChoice Icon)".<sup>73</sup>

Das "Advertising Option Icon" ist ein eindeutiges Symbol, das einerseits personalisierte Werbung kennzeichnen und andererseits auf zusätzliche Informationen verlinken soll. Der Link dient dazu, Konsumenten über interessensbasierte Werbeanzeigen Auskunft zu geben und "Opt-Out"-Möglichkeiten anzubieten.<sup>74</sup>

Durch die "Opt-Out"-Möglichkeit wird versucht, eines der Selbstregulierungs-Prinzipien, "Consumer Control", umzusetzen. Der User kann entscheiden, ob er zu seinen Interessen bzw. zu seiner Person maßgeschneiderte Werbeanzeigen geschaltet bekommen möchte oder nicht. Das "Opt-Out" funktioniert meistens so, dass von dem entsprechenden Anbieter ein "Opt-Out"-Cookie<sup>75</sup> im Browser des Benutzers gespeichert wird. Dieses Cookie wird beim Surfen im Internet immer mitgesendet und signalisiert, keine personenbezogene Werbung dieses Dienstleisters erhalten zu wollen. Der Benutzer kann entweder bei den einzelnen Websites das "Opt-Out" aktivieren (die Funktion ist oft Teil der "Privacy Policy") oder sich in Unternehmens-Listen eintragen, wie sie zum Beispiel vom "Self-Regulatory Program for Online Behavioral Advertising" angeboten wird.<sup>76</sup> Auch das europäische Programm verfügt über eine "Opt-Out"-Liste. Auf [www.youronlinechoices.com](http://www.youronlinechoices.com), das für 33 Länder zur Verfügung steht, werden neben einem Präferenzmanagement allgemeine Informationen zu Datenschutz und personenbezogener Werbung angeboten.<sup>77</sup>

---

<sup>73</sup>vgl. [Interactive Advertising Bureau 2011]

<sup>74</sup>vgl. [Interactive Advertising Bureau]

<sup>75</sup>Eine detailliertere Beschreibung zu Cookies im Allgemeinen ist im Kapitel 2.2.1 *HTTP-Cookie* auf Seite 20 zu finden.

<sup>76</sup>vgl. [Digital Advertising Alliance]

<sup>77</sup>vgl. [Your Online Choices 2016]

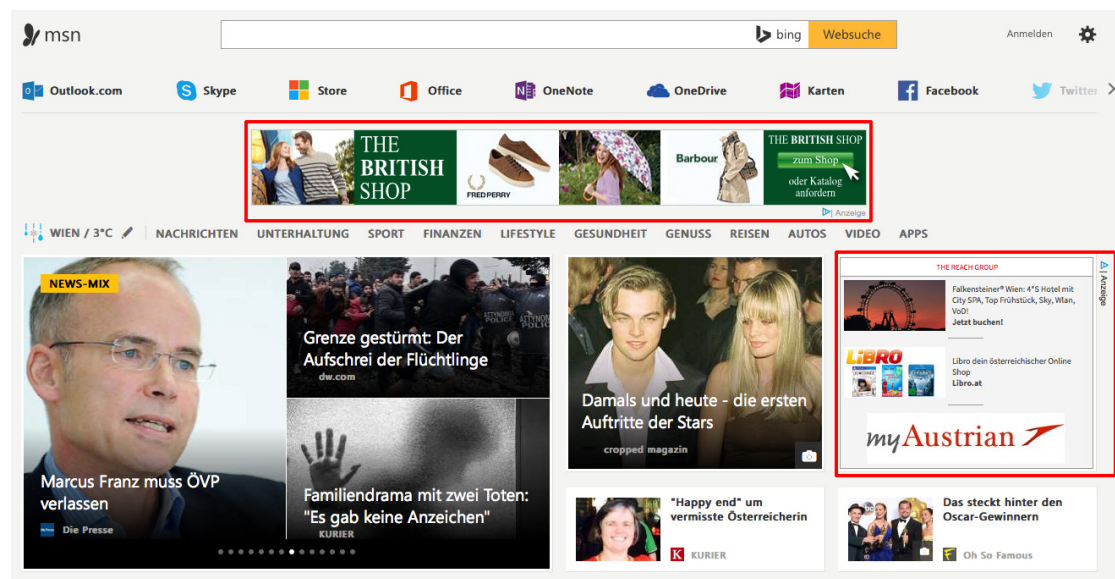


Abbildung 3.13: Die Grafik zeigt einen Ausschnitt der österreichischen Homepage von msn. Die mit dem "Advertising Option Icon" gekennzeichnete Werbung ist rot umrandet.

Bildquelle vgl. [Microsoft ]



Ich stimme zu, dass diese Seite Cookies für Analysen, personalisierten Inhalt und Werbung verwendet [Erfahren Sie mehr darüber](#) ✕

Wenn Sie keine personalisierten Anzeigen in diesem Browser sehen möchten, muss Ihr Browserverlauf Cookies von Erstanbietern und von Drittanbietern zulassen, und der Browser muss so eingestellt sein, dass der Browserverlauf beim Beenden NICHT gelöscht wird. Anleitungen zum Aktivieren von Cookies und zum Konfigurieren des Browserverlaufs finden Sie möglicherweise in den Einstellungen des Browsers, in den Datenschutzrichtlinien oder in der Hilfedokumentation. ✕

**Microsoft** [Anmelden](#)

### Infos zu unseren Anzeigen

Für eine persönlichere Onlineerfahrung werden einige Anzeigen, die Ihnen möglicherweise über Microsoft-Websites und -Apps angezeigt werden, auf Ihre vorherigen Aktivitäten, Suchvorgänge und Websitebesuche angepasst. Sie behalten die Kontrolle, und hier können Sie die für Sie passende Werbung auswählen.

#### Wo kann ich weitere Informationen zu Werbung auf Microsoft-Websites und -Apps erhalten?

Microsoft arbeitet mit Partnern wie AOL, AppNexus und anderen dritten Diensteanbietern zusammen, um angepasste Inhalte bereitzustellen und Werbung auf MSN, Outlook.com und anderen Websites und Apps anzuzeigen. Microsoft übermittelt auch Suchanzeigen an Bing und unsere Konsortialsuchpartner. Weitere Informationen zu den Datenschutzpraktiken von Microsoft erhalten Sie hier: [hier](#). Mehr Informationen zu interessenbezogener Werbung von AOL und AppNexus finden Sie in deren Datenschutzbestimmungen: [AOL](#) und [AppNexus](#).

#### Welche Optionen stehen bei interessenbezogener Werbung zur Verfügung?

Auf dieser Seite können Sie angeben, dass Sie keine interessenbezogene Werbung mehr von Microsoft empfangen möchten. Zudem können Sie auf den folgenden Websites angeben, dass Sie keine interessenbezogene Werbung mehr von allen selbstregulierten Mitgliedern, einschließlich Microsoft, AOL, AppNexus und Anzeigennetzwerken von Drittanbietern, erhalten möchten:

- In den USA: [Digital Advertising Alliance \(DAA\)](#)
- In Europa: [European Interactive Digital Advertising Alliance \(EDAA\)](#)
- In Kanada: [Ad Choices: Digital Advertising Alliance of Canada \(DAAC\)](#)

Sie können die interessenbezogene Werbung in Windows-Apps steuern, indem Sie die Option [Werbe-ID](#) in den Windows-Einstellungen deaktivieren.

**Personalisierte Werbung in diesem Browser**

EIN

Überprüfen Sie die Einstellung „Personalisierte Werbung“ für diesen Webbrowser.

[Erfahren Sie mehr](#) ▾

**Beim Verwenden meines Microsoft-Kontos immer personalisierte Werbung anzeigen**

AUS [Zum Ändern anmelden...](#)

Überprüfen Sie die Einstellung „Personalisierte Werbung“. Sie gilt, wenn Sie sich auf einem Computer oder Gerät mit Ihrem Microsoft-Konto anmelden. Dies gilt auch für Windows, Windows Phone, Xbox und andere Geräte.

Abbildung 3.14: Die Grafik zeigt die Microsoft-Auskunftseite zu personalisierter Werbung und bietet Einstellungsoptionen diesbezüglich an.

Bildquelle vgl. [Microsoft]

Abbildung 3.14 zeigt das Ergebnis, wenn der Anwender bei msn auf das "Advertising Option Icon" klickt: die Auskunftseite von Microsoft zu personalisierter Werbung wird geladen. Dort erfährt der Benutzer, wie Microsoft personalisierte Werbung platziert, mit welchen Selbstregulierungsbehörden das Unternehmen zusammenarbeitet und welche Kontrollmöglichkeiten der User hat. Diese setzen sich aus Einstellungen für den Browser, das registrierte Microsoft-Konto und für Windows-Applikationen zusammen. Um über den Browser Microsoft zu kommunizieren, dass keine personenbezogene Werbung geladen werden soll, muss der Browser Erst- und Drittanbietercookies akzeptieren und die Chronik darf nicht gelöscht werden.<sup>78</sup>

<sup>78</sup> vgl. [Microsoft]

Jedoch sind gerade das Blockieren von insbesondere Drittanbietercookies und das Löschen des Browserverlaufs, zwei der einfachsten Sofortmaßnahmen gegen User-Tracking. Weiters verhindert das Setzen eines "Opt-Out"-Cookies weder das Sammeln, Speichern oder Auswerten von Benutzerdaten, noch das Tracking bzw. Profiling, sondern lediglich das Laden verhaltensbasierter Werbeanzeigen. Datenschützer kritisieren regelmäßig Selbstregulierungs-Systeme, da sie keinen wirkungsvollen Schutz vor Tracking bieten und Unternehmer rechtlich nicht dazu verpflichtet sind daran teilzunehmen und ohne Kontrolle von unabhängigen Stellen die Prinzipien umsetzen. Daten werden weiterhin erfasst und analysiert und Internetuser haben nach wie vor keine tatsächliche Kontrolle über die von ihnen gesammelten Informationen.

Ein zusätzlicher Kritikpunkt an "Opt-Out"-Cookies ist, dass sie vorwiegend nicht persistent sind. Internetanwender, die als Standardeinstellung ihres Browsers zum Beispiel Cookies beim Beenden automatisch löschen, entfernen dadurch auch gesetzte "Opt-Out"-Cookies und müssten sich jedes Mal aufs neue in Abmelde-Listen eintragen. Außerdem besteht die Möglichkeit, dass ein User seinem Browser generell das Setzen von Cookies untersagt, in diesem Fall können auch "Opt-Out"-Cookies nicht gesetzt werden oder müssen gesondert bzw. manuell gewartet werden. Bisher gibt es keine universell gültige "Opt-Out"-Variante. Benutzer müssen sich entweder auf diverse "Opt-Out"-Listen eintragen oder gar auf jeder besuchten Website einzelne Einstellungen vornehmen. Dabei darf nicht vergessen werden, dass durch das "Opt-Out" kein Tracking verhindert wird, sondern ausschließlich das Platzieren interessensbasierter Werbung.

Wie bereits im Kapitel 2.2.1 *HTTP-Cookie* auf Seite 20 erwähnt, haben Forscher Ende 2015 die Verbreitung von u.a. Drittanbietercookies untersucht. Dabei kamen sie zu dem Ergebnis, dass auf den laut Quantcast<sup>79</sup> 100 meistbesuchten, us-amerikanischen Interneteiten, allein durch das Laden der Startseite, 6.000 HTTP-Cookies gesetzt werden. 83% davon werden von 275 unterschiedlichen Drittanbietern platziert.<sup>80</sup> Gesetzt den Fall, dass alle diese Anbieter ein "Opt-Out" ermöglichen, müsste ein Internetuser nicht nur 275 "Opt-Out"-Cookies speichern, sondern genau genommen 275 Drittanbieterwebsites aufrufen, deren Datenschutzbestimmungen nicht nur lesen und verstehen, sondern auch dementsprechend darauf reagieren. Zuvor müsste der Besucher darüber informiert werden, welche Drittanbieter mit einem Webauftritt kooperieren und welche möglichen fremden Inhalte oder Dienstleistungen auf einer Website geladen werden.

---

<sup>79</sup>Quantcast ist ein internationales Technik-Unternehmen mit Sitz in San Francisco, USA, das sich auf die Analyse von Internet-Datenverkehr auf konkreten Websites und darauf aufbauend auf zielgerichtete Werbeplatzierung spezialisiert hat.

<sup>80</sup>vgl. [Altaweel et al. 2015]

Im Kapitel 4 *Trackingbeispiele in Österreich* auf Seite 130 wird anhand einzelner Beispiele aufgezeigt, wie österreichische Websites Drittanbieter handhaben.

Auch am "Advertising Option Icon" wird Kritik geübt. Ein Bericht vom 18. August 2011 von Jonathan Mayer macht darauf aufmerksam, dass nur 9,9% der geladenen Werbung von Drittanbietern mit einem "Advertising Option Icon" angezeigt wurde, und nur 5,1% waren auch mit einem Informations-Link ausgestattet. Dabei wurden die Startseiten der laut Alexa 500 weltweit beliebtesten Websites untersucht. Neben der geringen Verbreitung, wird bei vorkommenden Symbolen deren Unscheinbarkeit bemängelt.<sup>81</sup> Die kleine Darstellung des "AdChoice Icon" wird auf der Abbildung 3.13 "Advertising Option Icon" auf der Homepage von msn auf Seite 105 wiedergegeben. Leider wurde der Bericht von Jonathan Mayer nicht wiederholt und es konnten keine aktuellen Statistiken zur Verbreitung des "Advertising Option Icon" gefunden werden.

Eine Studie der Parks Associates aus 2014 hat ergeben, dass 2011 nur 5% der befragten, amerikanischen Internetuser das "AdChoice Icon" bei Online-Werbeanzeigen wahrgenommen haben. Im Vergleich dazu stieg die Prozentzahl bei einer Wiederholung der Befragung in 2013 lediglich um 1% an.<sup>82</sup> Es ist unklar, wie sich die Distribution des "AdChoice Icon" weiterentwickelt hat, allerdings wird es mittlerweile auch auf österreichischen Websites angezeigt.



Abbildung 3.15: Die Grafik zeigt einen Ausschnitt der kurier.at-Startseite. Die mit dem "Advertising Option Icon" gekennzeichnete Werbung ist rot umrandet.  
Bildquelle vgl. [Kurier 2016]

<sup>81</sup>vgl. [Mayer Jonathan 2011a]

<sup>82</sup>vgl. [Parks Associates 2014]

---

Als organisatorische Maßnahmen wurden die Allgemeinen Geschäftsbedingungen und Privacy Policies thematisiert, und einige Online-Gütesiegel, wie das amerikanische TRUSTe, das europäische EuroPrise und die beiden österreichischen Zertifizierungen, das E-Commerce-Gütesiegel und das Trustmark Austria, vorgestellt. Zuletzt wurde die Problematik von Selbstregulierungs-Systemen, vor allem der Praktik des "Opt-Out", deutlich gemacht. Datenschützer verlangen klare Gesetzesvorgaben für den Einsatz von Tracking-Techniken und der Wahrung des Datenschutzes im Internet, ausgereifte Softwarelösungen innerhalb des Browsers, die für den Anwender sowohl leicht verständlich, wie auch einfach zu bedienen sind, und ein Umdenken zu "Opt-In"-Methoden, anstatt simpler und freiwilliger "Opt-Out"-Mechanismen, die dem Internetbenutzer wenig Kontrolle geben. Eine Reihe von technischen Maßnahmen, darunter das vielversprechende "Do Not Track"-Signal, werden im folgenden Kapitel aufgezeigt.

### 3.3 Technische Maßnahmen

Das anschließende Kapitel soll darstellen, welche technischen Möglichkeiten es gibt, Daten beim Surfen im Internet zu schützen, Tracking zu verhindern bzw. zu erschweren, keine personalisierte Werbung zu erhalten bzw. die Privatsphäre im Internet zu erhöhen. Das grundlegende Werkzeug dabei ist der Browser. Die laut "StatCounter"<sup>83</sup> am verbreitetsten Browser in Österreich sind Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari, Opera und Microsoft Edge.

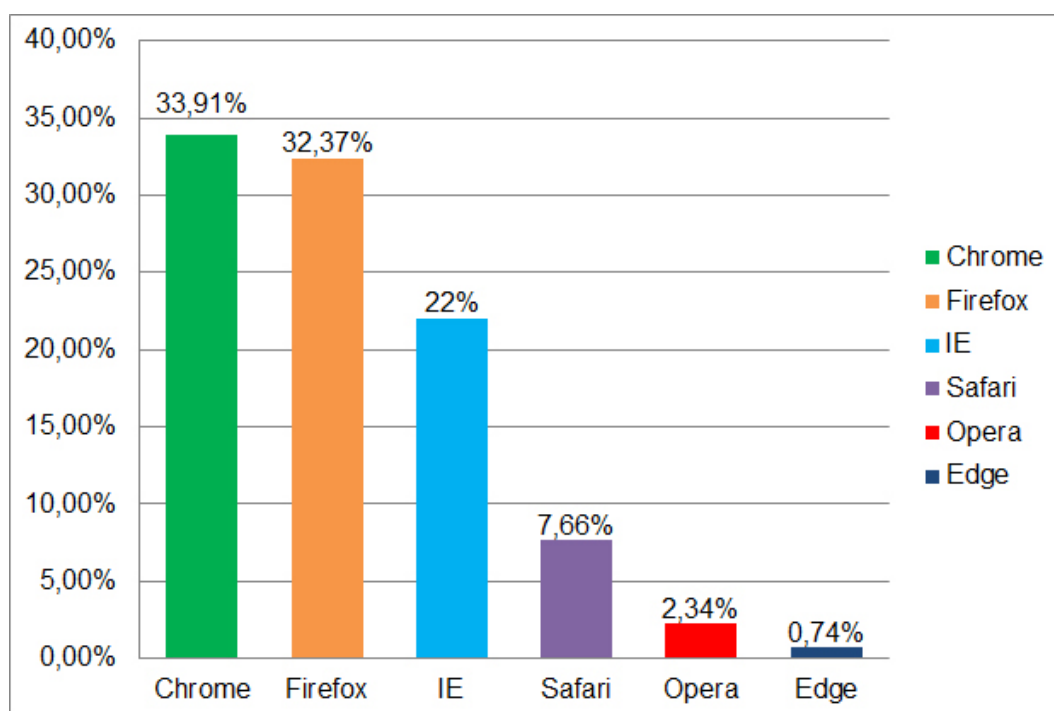


Abbildung 3.16: Die Grafik zeigt den Marktanteil der führenden Browser in Österreich in einem Zeitraum von Jänner 2015 bis Dezember 2015: Chrome 33,91%, Firefox 32,37%, Internet Explorer 22%, Safari 7,66%, Opera 2,34% und Edge mit 0,74%.

Bildquelle vgl. [StatCounter 2015a]

<sup>83</sup>StatCounter ist ein Web-Analyse-Service, das weltweit auf über drei Millionen Websites integriert ist und Statistiken zur Verbreitung von Browser, Browserversionen, Betriebssystemen, Suchmaschinen oder etwa sozialen Netzwerken liefert.

### 3.3.1 Einstellungen im Browser

In den Datenschutz- und Privatsphäreinstellungen des Browsers können benutzerdefinierte Angaben zur Chronik und der Akzeptanz von Cookies oder dem Speichern von Dateien im Cache, zu "Do Not Track" oder zur Verwendung der defaultmäßigen Suchmaschine gemacht werden.

**Cookies**, im spezifischen Drittanbietercookies, stellen eines der grundlegendsten, ältesten und am weitest verbreiteten Tracking-Elemente dar.<sup>84</sup> Daher ist es für Anwender von Vorteil und essentiell, dass der Browser so konfiguriert werden kann, dass das Setzen von bestimmten Cookies nicht erlaubt wird, oder dass sie beim Beenden des Browsers gelöscht werden. Außer Safari, der als einziger voreingestellt keine Cookies von Drittanbietern akzeptiert, erlauben Browser in ihrer Standardkonfiguration immer das Setzen von Drittanbietercookies, die weiters beim Beenden des Browsers auch nicht gelöscht werden.

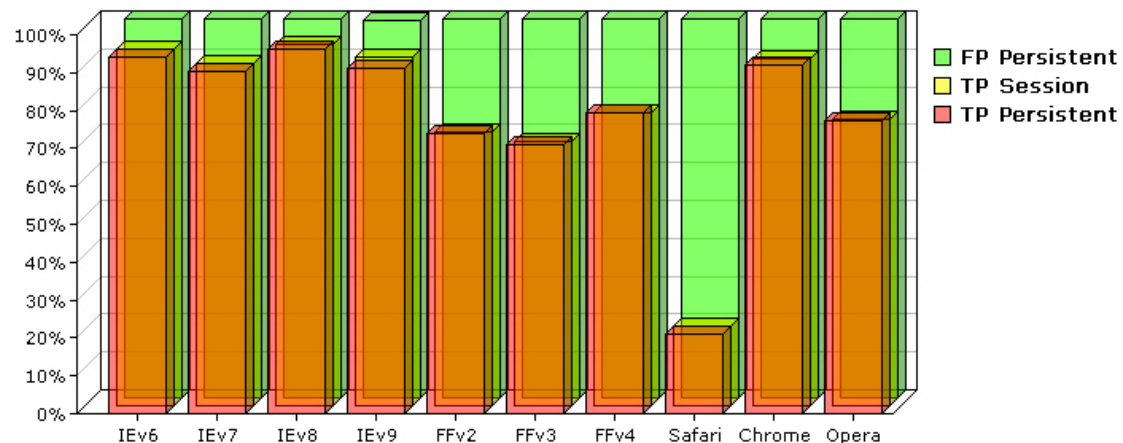


Abbildung 3.17: Die Grafik zeigt die jeweiligen First- und Third-Party-Cookie-Einstellungen der verschiedenen Browser an.

Bildquelle vgl. [Gibson Research Corporation 2016]

<sup>84</sup> Auf die genaue Bedeutung von Cookies und Drittanbietercookies wird im Kapitel 2.2.1 *HTTP-Cookie* auf Seite 20 eingegangen.

Die Gibson Research Corporation<sup>85</sup> misst die Browsereinstellungen ihrer Seitenbesucher und veröffentlicht dazu wöchentlich Statistiken, wie in der oben gezeigten *Abbildung 3.17* dargestellt wird. Diese stellt die First- und Third-Party-Cookie-Einstellungen der verwendeten Browser der ca. 67.250 User dar, die in der Woche vom 20. bis 26. Juni 2016 die Seiten der Gibson Research Corporation aufgerufen haben. Zu den geprüften Browsern gehören der Internet Explorer, Firefox, Safari, Chrome und Opera. Es wird zwischen persistenten First-Party-Cookies (FP Persistent), Third-Party-Session-Cookies (TP Session) und persistenten Third-Party-Cookies (TP Persistent) unterschieden. Die Gibson Research Corporation hat die Grafik ihrer Auswertung in den letzten Jahren nicht auf die aktuellsten Browserversionen erweitert, dennoch sind die Daten aussagekräftig. Die Besucherstatistik zeigt unmissverständlich, dass im Durchschnitt ca. 84% aller User Third-Party-Cookies akzeptieren. Dabei sticht Safari als einziger Browser durch einen sehr niedrigen Wert besonders hervor. Nur ca. 21% aller Safari-Anwender erlauben das Setzen von Third-Party-Cookies. Dieser Prozentsatz ist auf die Voreinstellen bei Safari zurückzuführen, die alle Third-Party-Cookies zunächst blockiert. Das Ergebnis verdeutlicht die Relevanz von "Privacy by Default" bei Browser-Standard-Einstellungen in Zusammenhang mit Cookies und dem Schutz vor Online-Tracking.<sup>86</sup>

Weiters können im Browser Einstellungen zur **Chronik**, dem Verlauf der bisher besuchten Webseiten, vorgenommen werden. Sie kann ebenfalls zu Tracking-Zwecken ausgelesen werden<sup>87</sup> und wird per Default in allen Browsern langfristig gespeichert. Eine Konfigurationsmöglichkeit wäre keine Chronik anzulegen oder diese jedes Mal beim Beenden des Browsers automatisch zu löschen.

Aufgrund der, wie im vorigen Kapitel<sup>88</sup> beschriebenen Problematik von Opt-Out-Cookies, den verschiedenen Tracking-Varianten<sup>89</sup> und der andauernden Diskussion über Tracking-Richtlinien zwischen den Gesetzgebern, Datenschützern und der Werbeindustrie wurde von Jonathan Mayer (Informatiker und Jurist an der Stanford Universität) und Arvind Narayanan (Universitätsassistent der Informatik an der Princeton Universität) bereits 2011 versucht eine universelle "**Do Not Track**"-Möglichkeit zu entwickeln. Der Mechanismus von "Do Not Track" basiert auf einem HTTP-Header-Feld,

---

<sup>85</sup>Die Gibson Research Corporation gehört dem amerikanischen Softwareentwickler und Journalisten Steve Gibson, dessen Hauptfokus ist das Thema IT-Sicherheit. Auf der dazugehörigen Website [www.grc.com](http://www.grc.com) werden einige hilfreiche Informationen und Werkzeuge zu diesem Thema angeboten. Unter anderem betreut Gibson gemeinsam mit Leo Laporte den wöchentlichen Podcast "Security Now", worin aktuelle IT-Sicherheits-Angelegenheiten diskutiert werden.

<sup>86</sup>vgl. [Gibson Research Corporation 2016]

<sup>87</sup>Siehe Kapitel 2.2.8 *History Sniffing* auf Seite 30.

<sup>88</sup>Siehe Kapitel 3.2.3 *Selbstregulierungs-Systeme* auf Seite 103.

<sup>89</sup>Siehe Kapitel 2.2 *Tracking-Technologien* ab Seite 20.

das beim Aufrufen einer Internetseite durch den Browser die Information mitsendet, dass man nicht getrackt werden möchte. Websites können dementsprechend darauf reagieren, die Wünsche des Users berücksichtigen und Tracking deaktivieren. Der Vorteil des "Do Not Track"-Headers ist, dass seine Abfrage leicht im Code der Webapplikation oder des Webservers eingebunden werden kann. Die entsprechenden Vorlagen werden sogar auf der Projekt-Website von donottrack.us bereitgestellt. Der Nachteil ist, dass das Berücksichtigen des "Do Not Track"-Headers von Websitebetreibern nur freiwillig, nicht gesetzlich verankert, daher nicht verpflichtend ist und auch keinem Kontrollorgan unterliegt.<sup>90</sup> Der User weiß nicht bzw. kann nicht nachvollziehen, welche Auswirkungen der aktive "Do Not Track"-Mechanismus hat.

Das World Wide Web Consortium hat die Entwicklung eines gültigen "Do Not Track"-Standards noch nicht vollständig abgeschlossen (Stand Juni 2016). Es existieren zwei Dokumente, Tracking Preference Expression (DNT) und Tracking Compliance and Scope (TCS), mit Handlungsvorschlägen und technischen Spezifikationen, wie Unternehmen auf einen gesetzten DNT-Header reagieren können. Eine offizielle Freigabe des Standards ist noch ausständig.<sup>91</sup> Einige Websites weisen in ihren AGBs oder Datenschutzbestimmungen auf ihren Umgang mit einem empfangenen "Do Not Track"-Signal hin. Sie stoppen etwa die Anzeige personalisierter Werbung, andere schränken das Tracking und Datensammeln ein, manche wiederum ignorieren das Signal. Es ist offen, welche Erwartungen ein Anwender von einem gesetzten "Do Not Track"-Status hat und wie sich die Handhabung durch die Empfänger in Zukunft weiterentwickeln wird.

Im Internet Explorer 8, der im März 2009 veröffentlicht wurde, gab es bereits so etwas ähnliches wie "Do Not Track", das "InPrivate Filtering". Dieses erkannte auf vom User besuchten Internetseiten wiederkehrende Drittanbieter, ermöglichte es deren Inhalte zu blockieren und somit ein Tracking zu unterbinden. Dabei war das Erkennen und Sammeln der Drittanbieter automatisch aktiv, und das Blockieren musste manuell gesetzt werden.<sup>92</sup> Mit dem Internet Explorer 9 wurde im März 2011 ein Tracking-Schutz eingeführt, der auf Tracking-Listen basiert, die zusätzlich importiert werden müssen. Die Schutzlisten werden von verschiedenen Organisationen angeboten und beinhalten bekannte Tracking-Unternehmen, deren Datenabfragen mittels der Liste blockiert werden können. Das "InPrivate Filtering" war bei IE9 weiterhin als "Personalisierte Liste für den Tracking-Schutz" vorhanden und konnte als zusätzliche Schutzliste aktiviert werden. Weiters wurde mit dem IE9 Release bei aktivem Tracking-Schutz ein "Do Not

---

<sup>90</sup>vgl. [Mayer Jonathan und Narayanan Arvind 2010]

<sup>91</sup>vgl. [W3C 2016]

<sup>92</sup>vgl. [Microsoft Corporation]



Track"-Signal im Sinne von Jonathan Mayer und Irving Narayanan ausgesendet.<sup>93</sup> Mit der Veröffentlichung des Internet Explorers 10 für Windows 8 im September 2012 wurde der "Do Not Track"-Header defaultmäßig auf aktiv gesetzt. Internet Explorer war zu dieser Zeit der einzige Browser, wo diese Einstellung bei der Softwareinstallation gesetzt wurde.<sup>94</sup> Seit April 2015 hat Microsoft sein Vorgehen revidiert und aktiviert das "Do Not Track"-Signal standardmäßig nicht mehr.<sup>95</sup> Durch die Einführung des neuen Windows Betriebssystems Windows 10 am 29. Juli 2015 wurde der Internet Explorer von einem neuen Microsoft Browser abgelöst, Microsoft Edge. In Österreich verwenden seitdem ca. 2% Microsoft Edge als Standardbrowser.<sup>96</sup> Dieser bietet eine "Do Not Track"-Funktion an, welche automatisch nicht aktiv ist.<sup>97</sup>

Firefox bietet seit der Version 4.0, die ebenfalls, wie der IE9 im März 2011 veröffentlicht wurde, eine "Do Not Track"-Option nach den Vorstellungen von Jonathan Mayer und Irving Narayanan an.<sup>98</sup> Auch bei der derzeitigen Firefox Version 43.0.4 (Stand Jänner 2016) kann über das Einstellungsmenü des Browsers unter "Datenschutz" bei "Websites auffordern, meine Aktivitäten nicht zu verfolgen" ein Häkchen gesetzt werden, um "Do Not Track" zu aktivieren.

2011 wurde der "Do Not Track"-Header bei Internet Explorer und Firefox eingeführt, weder Google Chrome, noch Safari oder Opera hatten zu dieser Zeit eine "Do Not Track"-Möglichkeit in ihren Browsereinstellungen integriert. Mittlerweile bieten alle Browser diese Funktion an, welche vom User manuell gesetzt werden muss.

Alle gängigen Browser stellen mit unterschiedlicher Namensgebung einen **Privatmodus** für das Surfen im Internet zur Verfügung: Privater Modus bzw. Privates Fenster bei Firefox<sup>99</sup>, InPrivate Browsen bei Internet Explorer<sup>100</sup>, InPrivate Modus bzw. InPrivate Fenster bei Microsoft Edge<sup>101</sup>, Inkognitomodus bei Chrome<sup>102</sup>, Privates Surfen bei Safari<sup>103</sup> und Privates Surfen bzw. Privates Fenster bei Opera<sup>104</sup>. Dadurch wird jedoch lediglich verhindert, dass am Computer keine Daten im Browsercache, Chronik,

---

<sup>93</sup>vgl. [Microsoft Corporation 2014]

<sup>94</sup>vgl. [Microsoft Corporate Blogs 2012]

<sup>95</sup>vgl. [Microsoft Corporate Blogs 2015]

<sup>96</sup>vgl. [StatCounter 2016]

<sup>97</sup>vgl. [Microsoft Corporation 2016b]

<sup>98</sup>vgl. [Mozilla Firefox 2011]

<sup>99</sup>vgl. [Mozilla Firefox 2016b]

<sup>100</sup>vgl. [Microsoft Corporation 2016a]

<sup>101</sup>vgl. [Microsoft Corporation 2016b]

<sup>102</sup>vgl. [Google 2016b]

<sup>103</sup>vgl. [Apple Inc. 2016]

<sup>104</sup>vgl. [Opera Software ASA 2016]

Passwörter, Formulareinträge oder Suchanfragen gespeichert werden. Je nach Browser gibt es verschiedene Einstellungsmöglichkeiten für diesen Modus. Sie alle haben gemein, dass andere Benutzer desselben Browsers am jeweiligen Rechner nicht nachvollziehen können, welche Webseiten zuvor geöffnet und welche Inhalte angesehen oder heruntergeladen wurden. Es bedeutet nicht, dass man sich anonym im Internet bewegt oder keine Datenspuren hinterlässt, sondern nur direkt am Computer werden keine Daten gespeichert. Im Privatmodus des Browsers können Tracking-Daten des Benutzers generiert werden. Firefox bietet seit November 2015 mit dem Versionrelease 42.0 eine "Do Not Track"-Funktion für den "Privat Modus" des Browsers an.<sup>105</sup> Diese ist bei den Datenschutz-Einstellungen unter dem Punkt "Schutz vor Aktivitätenverfolgung in privaten Fenstern verwenden" per Default aktiv. Aber wie bereits erwähnt, gibt es noch keine Standards dafür, wie Websitebetreiber auf "Do Not Track" reagieren müssen.

Eine weitere Einstellungsmöglichkeit bei Browsern ist welche **Suchmaschine** standardmäßig eingesetzt werden soll. Bei Firefox, Safari, Opera und Chrome ist die Marktführerin Google, bei Internet Explorer und Microsoft Edge ist bing als Suchmaschine voreingestellt. Außer Chrome, Internet Explorer und Microsoft Edge bieten alle Browser als Option DuckDuckGo an, wovon Safari der erste Browser war, der DuckDuckGo bei der Auswahl inkludiert hat. Der Vorteil dieser alternativen Suchmaschine ist, dass abgesetzte Suchabfragen und der vollständige Suchverlauf eines Users anonym bleiben und somit über Suchen nicht getrackt und kein Profiling betrieben werden kann.<sup>106</sup>

---

<sup>105</sup> vgl. [Mozilla Firefox 2016a]

<sup>106</sup> vgl. [Gabriel Weinberg 2012]

In Österreich verwendeten im Jahr 2015 laut "StatCounter" 93,96% Google für Online-Suchen. Microsofts Bing wird, obwohl als Suchmaschine beim Internet Explorer voreingestellt, nur von 3,27%, Yahoo! von 1,88%, Ask Jeeves von 0,31% und die anonyme Suchmaschine DuckDuckGo von 0,24% eingesetzt.

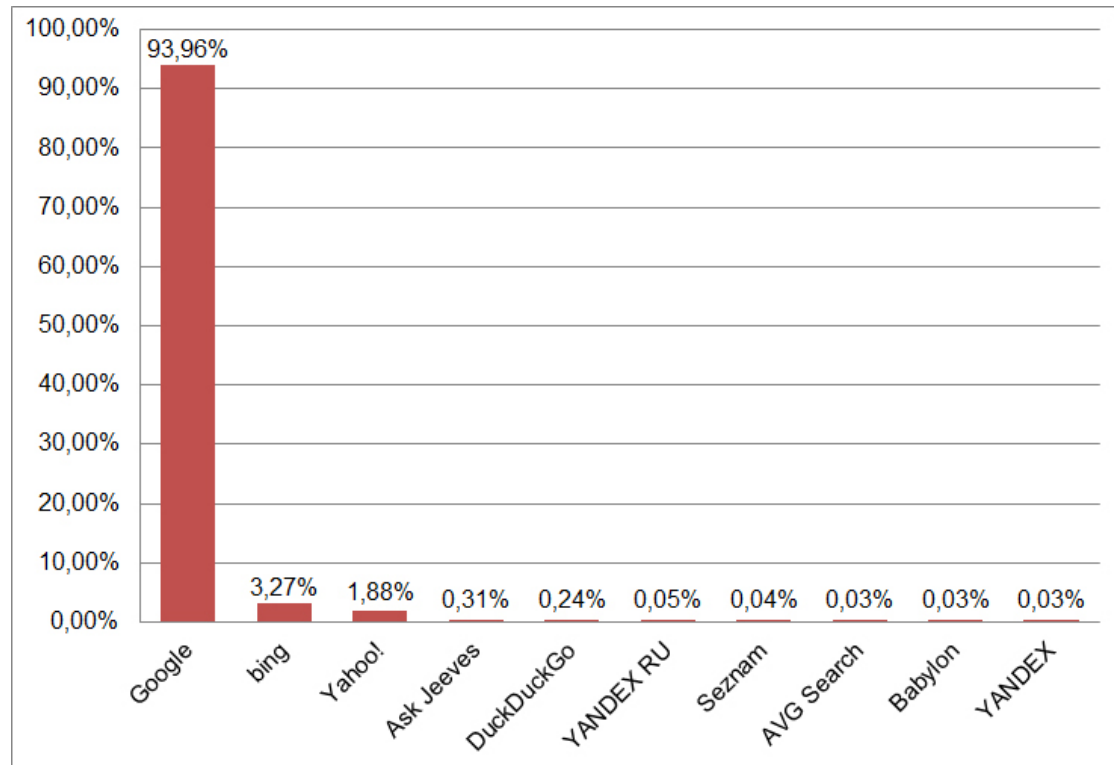


Abbildung 3.18: Die Grafik zeigt die Marktanteile der verschiedenen in Österreich eingesetzten Suchmaschinen im Jahr 2015.

Bildquelle vgl. [StatCounter 2015b]

Weltweit hält Googles Suchmaschine ebenfalls die Vorherrschaft mit 88,66%, Bing hat international einen Marktanteil von 4,13%, Yahoo! von 3,55% und DuckDuckGo von 0,13%.

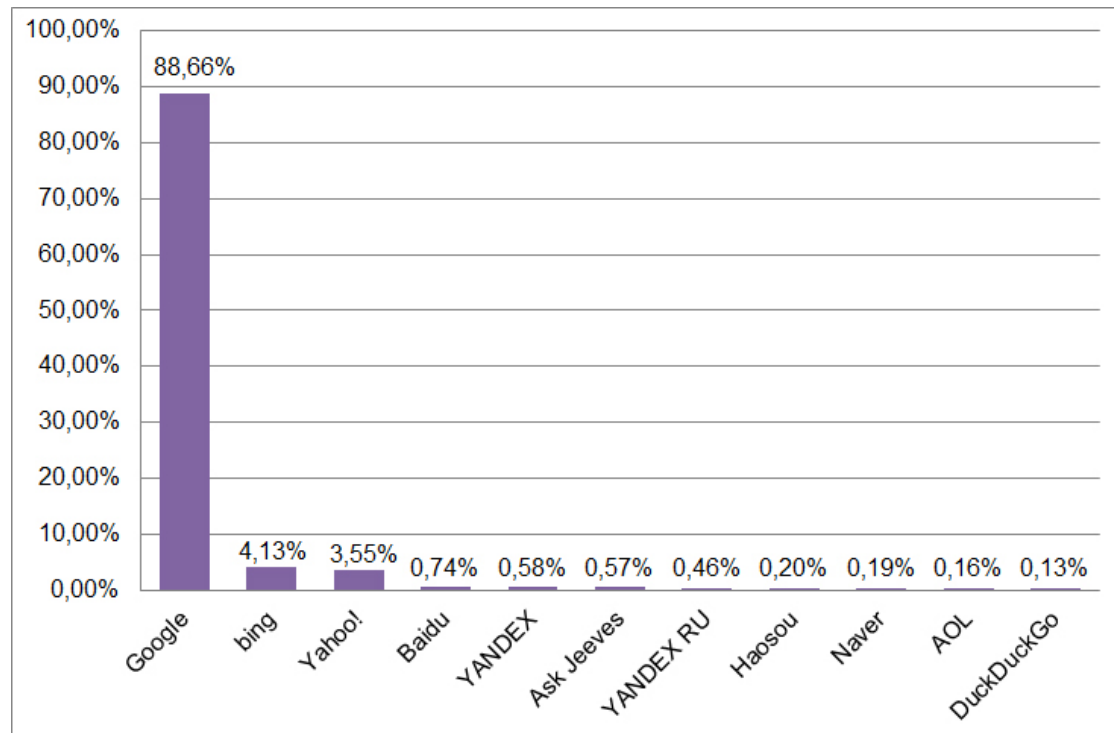


Abbildung 3.19: Die Grafik zeigt die Marktanteile der verschiedenen weltweit eingesetzten Suchmaschinen im Jahr 2015.

Bildquelle vgl. [StatCounter 2015c]

Zwei weitere Alternativen zu Google sind die beiden Suchmaschinen StartPage und Ixquick des niederländischen Privatunternehmens Surfboard Holding B.V.. Ixquick wurde 1998 gegründet, StartPage 2009, beide speichern keinerlei persönliche Daten der Anwender, weder IP-Adresse, noch Suchbegriffe oder Suchchronik. Der Unterschied zwischen den zwei Suchmaschinen ist, StartPage liefert anonym die Suchergebnisse von Google, wogegen Ixquick beim Generieren der Trefferseite eine Kombination mehrerer Suchmaschinen exklusive Google verwendet. Am 14. Juli 2008 wurde Ixquick mit dem ersten europäischen Datenschutz-Gütesiegel EuroPriSe ausgezeichnet.<sup>107/108</sup> Keiner der gängigen Browser bietet sie als Option bei den Sucheinstellungen an, der User kann sie aber manuell hinzufügen.

<sup>107</sup> vgl. [Surfboard Holding B.V.a]

<sup>108</sup> vgl. [Surfboard Holding B.V.b]

Der folgende Screenshot zeigt eine denkbare Konfiguration des Datenschutzes in der Firefox Browserversion 47.0. Cookies werden akzeptiert, aber nach Beenden des Browsers gelöscht. Cookies von Drittanbietern werden allgemein nicht erlaubt. Die Chronik wird ebenfalls gelöscht, wenn Firefox geschlossen wird. Do Not Track ist aktiviert, die Funktion ist via dem Link "Websites mitteilen, ihre Aktivitäten nicht zu verfolgen" abrufbar.

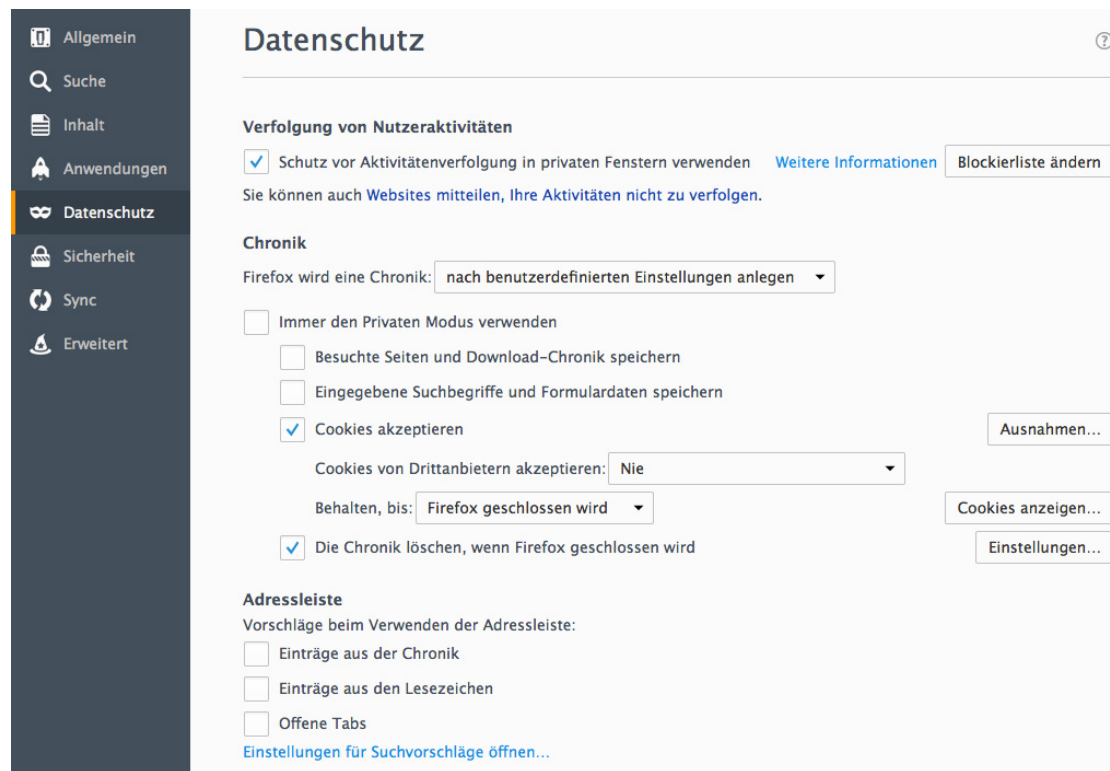


Abbildung 3.20: Die Grafik zeigt eine benutzerdefinierte Datenschutz-Einstellung des Firefox Browsers Version 47.0.

Es liegt in der Eigenverantwortung des Anwenders sich mit den Standardeinstellungen des bevorzugten Browsers auseinanderzusetzen und diese entsprechend zu adaptieren, wenn man sich vor Internet-Tracking schützen bzw. dieses erschweren oder verhindern möchte. Egal welchen Browser man wählt, es ist entscheidend, sich mit dessen Privatsphäre- und Datenschutzeinstellungsmöglichkeiten vertraut zu machen und einzusetzen.

### 3.3.2 Browsererweiterungen

Für die gängigen Browser, vor allem für Firefox und Google Chrome, existieren eine Vielzahl an Add-ons, die die vorhandenen Funktionen optimieren können. Im folgenden Abschnitt sollen einige nützliche Erweiterungen aus den Kategorien Sicherheit, Datenschutz und Privatsphäre vorgestellt werden, die dabei helfen Trackingmechanismen zu blockieren:

Der Werbeblocker **Adblock Plus**<sup>109</sup> ist die beliebteste und am häufigsten heruntergeladene Firefox-Ergänzung. Im Jänner 2016 zählte sie im Durchschnitt täglich ca. 21,7 Millionen Anwender.<sup>110</sup> Sie ist auch für Google Chrome, Internet Explorer, Safari, Opera und Microsoft Edge verfügbar und bietet eine eigene Browser-Version für das mobile Betriebssystem Android an. Das Add-on wurde 2006 ursprünglich dafür entwickelt, um Werbeanzeigen aller Art (Pop-Ups, Animationen, Bilder) auf Internetseiten zu blockieren. Deren Erkennung basiert auf installierten Filterlisten. Im Laufe der Add-on-Entwicklung wurde sie um zusätzliche Funktionen erweitert. Inzwischen können Trackingelemente, Social-Media-Buttons oder bekannte Malware ebenfalls blockiert werden. Möchte der User auf bestimmten Websites Werbung erlauben, kann Adblock Plus auf diesen Seiten entweder manuell deaktiviert werden oder die entsprechende Website zu einer Whitelist hinzufügen, wo Adblock Plus automatisch deaktiviert ist.

Seit 2011 wird per Default tolerierbare Werbung angezeigt. User, die absolut keine Werbung sehen und jede Werbeanzeige blockieren möchten, müssen die Funktion manuell deaktivieren. Welche Werbung als "akzeptabel" gilt, wird anhand definierter Kriterien der Betreiberfirma des Add-ons, Eyeo, entschieden. Dies soll einerseits dazu dienen Websites zu unterstützen, die sich mittels Werbung finanzieren und bemüht sind unaufdringliche Werbeanzeigen zu schalten, andererseits sichert sich Adblock Plus dadurch sein Bestehen.<sup>111</sup>

Eyeo wird von Datenschützern für das Anzeigen unaufdringlicher Werbung und dem zugrundeliegenden Geschäftsmodell stark kritisiert. Denn große Werbeanbieter wie zum Beispiel Google, Yahoo, Amazon oder Ebay bezahlen das Unternehmen dafür, um als "akzeptabel" gewertet und auf die entsprechende Whiteliste gesetzt zu werden. Google soll 2013 25 Millionen US-Dollar (rund 22 Millionen Euro) für die Aufnahme auf die Whitelist investiert haben.<sup>112</sup>

---

<sup>109</sup>vgl. [Wladimir Palant 2016a]

<sup>110</sup>vgl. [Mozilla Foundation 2016]

<sup>111</sup>vgl. [Wladimir Palant 2016b]

<sup>112</sup>vgl. [Sascha Pallenberg 2014]

Laut einer Studie von PageFair<sup>113</sup> hat Google im 2. Quartal 2013 durch das Blockieren von Werbeanzeigen einen Verlust von ca. 887 Millionen US-Dollar (rund 796 Millionen Euro) erlitten.<sup>114</sup> Es ist daher nicht verwunderlich, dass ein kleiner Teilbetrag davon für den Eintrag auf die Whitelist von Adblock Plus ausgegeben wird, wenn dadurch Einbußen in dreistelligen Millionensummen vermieden werden können.

Nennenswerte Alternativen von Adblock Plus sind **uBlock Origin** und **AdBlock**. uBlock Origin gibt es als Add-on für Firefox, Google Chrome und Opera. Es kann auch über den Firefox Browser für das mobile Betriebssystem Android als Erweiterung hinzugefügt werden.<sup>115</sup> AdBlock steht für Google Chrome, Safari, Opera und für das mobile Betriebssystem iOS zur Verfügung.<sup>116</sup> Seit Oktober 2015 kooperiert AdBlock mit seinem Konkurrenten Adblock Plus und bietet ebenfalls das Einblenden von "akzeptabler" Werbung mittels derselben Whitelist an.<sup>117</sup>

Auch Websitebetreiber kritisieren die durch Werbeblocker verursachten Einbußen und versuchen unter anderem gerichtlich gegen sie vorzugehen. Mehrere Medienunternehmen haben in den letzten Jahren gegen Browsererweiterungen wie Adblock Plus geklagt, um diese rechtlich verbieten zu lassen, bisher ohne Erfolg. Zuletzt entschied das Landgericht München im März 2016 in der Klage der Süddeutschen Zeitung gegen die Eyeo GmbH gegen den Kläger. Es wäre nicht die Pflicht der Konsumenten Werbung im Browser anzeigen zu lassen und der Einsatz von Adblock Plus gesetzlich erlaubt.<sup>118</sup>

Manche Websites sperren aufgrund dessen ihre Inhalte für User, die einen Werbeblocker im Browser aktiviert haben. Anwender können erst darauf zugreifen, wenn sie entweder das Add-on deaktivieren oder bereit sind für das Laden der Inhalte zu zahlen. Zum Beispiel sperrt das Online-Portal der Bild-Zeitung seine Artikel für Kunden, die einen Werbeblocker einsetzen. Beim Aufruf der Webseite [www.bild.de](http://www.bild.de) mit dem Browser Firefox und aktiven Adblock Plus, werden keine Medienberichte geladen, stattdessen erhält der Websitebesucher Informationen darüber, warum die Inhalte von [bild.de](http://bild.de) gesperrt wurden. Es gibt zwei Optionen die Sperre aufzuheben: Entweder der Werbeblocker wird deaktiviert, um [bild.de](http://bild.de) die Finanzierung durch Werbeeinnahmen zu ermöglichen oder der User ist dazu bereit ein Online-Abo abzuschließen.<sup>119</sup>

<sup>113</sup>PageFair ist ein irisches Unternehmen, das sich vor allem durch Trend-Prognosen bezüglich dem Einsatz von Werbeblocker einen Namen gemacht hat.

<sup>114</sup>vgl. [PageFair Team 2013]

<sup>115</sup>vgl. [Raymond Hill 2016]

<sup>116</sup>vgl. [Michael Gundlach 2016]

<sup>117</sup>vgl. [Torsten Kleinz 2015]

<sup>118</sup>vgl. [Torsten Kleinz 2016]

<sup>119</sup>vgl. [BILD.de 2016]



## Warum sehe ich BILD.de nicht?

Abbildung 3.21: Der Screenshot zeigt die Startseite von bild.de mit einem Infotext, warum der Inhalt für Kunden mit aktiviertem Werbeblocker nicht angezeigt wird.

Bildquelle vgl. [BILD.de 2016]

Das Firefox-Add-on **Flashblock**<sup>120</sup> verhindert das Laden von Flash-Elementen und zeigt stattdessen einen Button an. Erst nach dessen Anklicken wird der Inhalt geladen. Für Seiten, wie das Video-Portal YouTube, das u.a. Flash-Filme abspielt, können Einträge in eine Whitelist gemacht werden, die danach Flash automatisch erlaubt. Das Add-on blockiert ebenfalls das Laden von Flash basierten Werbeanzeigen oder versteckten Flash-Elementen und somit auch das Setzen von etwaigen Flash-Cookies<sup>121</sup>. Im Jänner 2016 setzten ca. 700.000 Nutzer täglich Flashblock ein. Personen, die Google Chrome verwenden, können die funktionsähnliche Erweiterung **Flashcontrol**<sup>122</sup> installieren. Anwendern von Safari steht **ClickToFlash**<sup>123</sup>, von Opera **NoFlash**<sup>124</sup> zur Verfügung. Für den Internet Explorer konnte kein äquivalentes Add-on gefunden werden.

<sup>120</sup> vgl. [Philip Chee 2016]

<sup>121</sup> Siehe Kapitel 2.2.2 *Flash-Cookie* auf Seite 22.

<sup>122</sup> vgl. [davec 2016]

<sup>123</sup> vgl. [Marc Hoyois 2016]

<sup>124</sup> vgl. [dr34polw 2016]



The screenshot shows the top navigation bar of derStandard.at with categories like International, Inland, Wirtschaft, Web, Sport, Panorama, Etat, Kultur, Wissenschaft, Gesundheit, Bildung, Reisen, and Lifestyle. A search bar and weather widget for Wien (23°C) are also visible.

The main content area features a sidebar on the left with the headline "Das Wichtigste in aller Kürze." and a link to "express.derStandard.at". The main content is dated "Dienstag, 27. September 2011, 14:55" and offers a "chronologisch sortieren" option.

The main content is divided into three columns:

- Left Column:** Contains three article teasers:
  - NEUE FEATURES:** "Google+: Teile deine Kreise" (9 Postings) - "Neues Feature erlaubt Circle-Sharing - Zynga bringt Cityville für Googles soziales Netzwerk".
  - TRACKING:** "Facebook schnüffelt selbst ausgeloggten NutzerInnen nach" (259 Postings) - "Soziales Netzwerk liest weiter Account-Details aus - Experte warnt vor Sicherheits- und Privacy-Implikationen".
  - ADVERTORIAL:** "Apple Computer, iPads & Co." - "seit kurzem beim Computerspezialisten DiTech. Apple Einsteiger profitieren von Profi-Beratung, Apple Fans freuen sich über Vorteile wie online Lagerstand & hohe Verfügbarkeit".
- Middle Column:** Features a large Flash block replacement area, indicated by a grey background and a small "werbung" label at the top. A small "f" logo is visible in the center of the block.
- Right Column:** Contains a poll titled "UMFRAGE" with a photo of a hand pointing up. The text reads: "Plussen" statt "Liken": Wie nennen Sie die Google+-Funktionen? [142] Weiche Wortneuschöpfungen beschert uns Google+?".

Abbildung 3.22: Die Grafik zeigt auf derstandard.at die Darstellung der Flashblock-Schaltfläche, wenn das Anzeigen von Flash-Inhalten verhindert wird.  
Bildquelle vgl. [derstandard.at GmbH 2011b]

The screenshot shows the derStandard.at website interface. At the top, there is a navigation bar with categories like 'International', 'Innovationen', 'IT-Business', 'Telekom', 'Netzpolitik', 'Games', 'Webmix', and 'Preisvergleich'. A search bar on the right shows 'Wien 23°'. Below the navigation bar, there are several featured articles and advertisements:

- Das Wichtigste in aller Kürze.** A link to [express.derStandard.at](#).
- RENAULT** advertisement: 'JETZT TESTFAHRT IN EINEM UNSERER RENAULT Z.E ELEKTROFAHRZEUGE SICHERN! Wir freuen uns, Sie am Wiener Heldenplatz am 08.10. begrüßen zu dürfen!' with images of Renault electric cars.
- NEUE FEATURES** section:
  - Google+: Teile deine Kreise** (9 Postings): 'Neues Feature erlaubt Circle-Sharing - Zynga bringt Cityville für Googles soziales Netzwerk'.
  - TRACKING** section:
    - Facebook schnüffelt selbst ausgeloggten NutzerInnen nach** (259 Postings): 'Soziales Netzwerk liest weiter Account-Details aus - Experte warnt vor Sicherheits- und Privacy-Implikationen'.
    - ADVERTORIAL** section:
      - Apple Computer, iPads & Co.**: 'seit kurzem beim Computerspezialisten DiTech. Apple Einsteiger profitieren von Profi-Beratung, Apple Fans freuen sich über Vorteile wie online Lagerstand & hohe Verfügbarkeit.'
  - UMFRAGE** section: 'Plussen" statt "Liken": Wie nennen Sie die Google+-Funktionen? [142] Welche Wortneuschöpfungen beschert uns Google+?' with an image of a hand pointing up.
  - werbung** section: 'Aufbruchstimmung. IBM. Get ready to break free.' with the IBM logo and a globe icon.

Abbildung 3.23: Die Grafik zeigt die beiden Werbeanzeigen auf derstandard.at, nachdem der Flashblock-Button gedrückt wurde.

Bildquelle vgl. [derstandard.at GmbH 2011b]

Mehr als zwei Millionen User (Stand Jänner 2016) verwenden das Firefox-Addon **NoScript**<sup>125</sup>. Es hindert Webseiten daran benötigte Browser-Plug-ins wie u.a. JavaScript, Java, Flash oder Silverlight auszuführen, die Tracking-Elemente steuern können. Die genannten Plug-ins sind oft ein üblicher Bestandteil vieler Web-Anwendungen, weshalb ein generelles Deaktivieren keine praktikable Lösung ist. NoScript ermöglicht deshalb das Eintragen von vertrauenswürdigen Internetseiten in eine Whitelist. Vergleichbare Erweiterungen existieren auch für Google Chrome, **ScriptSafe**<sup>126</sup>, welche jedoch seit Mai 2014 nicht mehr aktualisiert wurde, und **ScriptBlock**<sup>127</sup>. Eine weitere Alternative ist **NoScript Suite Lite**, die es für Opera, Google Chrome und Firefox gibt.<sup>128</sup>

<sup>125</sup> vgl. [Giorgio Maone 2016]

<sup>126</sup> vgl. [Andrew Y. 2016]

<sup>127</sup> vgl. [compvid30 2016]

<sup>128</sup> vgl. [MyBrowserAddon 2016]

**Ghostery**<sup>129</sup> ist ein umfangreiches Add-on, das es für Firefox, Internet Explorer, Safari, Google Chrome, Opera und für die mobilen Betriebssysteme Android und iOS bzw. als Erweiterung für den mobilen Firefox Android Browser zum Download gibt. Es listet einerseits die Ursprünge der beteiligten Third-Party-Tracker<sup>130</sup> einer besuchten Internetseite auf und ermöglicht andererseits das Laden diverser Tracking-Elemente und somit das Tracking selbst zu blockieren. Weiters löscht Ghostery Flash- und Silverlightcookies. Man kann einstellen, ob einzelne Anbieter bzw. Elemente nicht gesperrt werden sollen bzw. ob man bestimmten Websites einheitlich vertraut und einen vollständigen Zugriff mittels einem Eintrag in eine Whitelist von Ghostery erlaubt.

The screenshot shows the homepage of willhaben.at. At the top, there is a navigation bar with the logo 'WILLHABEN.AT' and links for 'Mein willhaben', 'Anzeigen', 'Merkliste', 'Suchagent', 'Login | Registrieren', and 'ANZEIGE AUFGEBEN'. Below this, there are statistics for different categories: IMMOBILIEN (87.002), AUTO & MOTOR (126.852), JOBS & KARRIERE (8.640), and MARKTPLATZ (3.337.846). The main content area features four large icons representing these categories: Immobilien (87.002 Häuser und Wohnungen), Auto & Motor (126.852 Gebrauchtwagen und Motorräder), Jobs & Karriere (8.640 Jobs und Stellenangebote), and Marktplatz (3.337.846 Anzeigen). A central counter shows '171702 Neue Anzeigen in den letzten 48 Stunden'. Below this, there is a section for 'Aktuelle Trends auf dem Marktplatz' with three featured items: 'Hippie Chic' (Boho Kleider, Fransentaschen, Hüte, Sonnenbrillen), 'EURO 2016' (Trikots, Neue Fußballschuhe, Panini Sticker, Flat-TVs), and 'Griller' (Gasgriller, Kugelgriller, Elektrogriller, Grillbesteck). On the right side, there is a 'Benutzer-Login' section with a text input field containing 'enola@gmx.net', a password field with asterisks, and a 'LOGIN' button. Below the login section, there is a 'willhaben-Code-Suche' section with a text input field and a 'willhaben' logo. A purple alarm box is overlaid on the right side, titled '9 Tracker', listing the following blocked trackers: Adition, Amazon-Associates, AT-Internet, Audience-Science, eXense, Facebook-Connect, Google-AdWords-Co..., Optimizely, and QWA.

Abbildung 3.24: Die Grafik zeigt einen Screenshot der Homepage von willhaben.at mit aktiviertem Ghostery. Die violette Alarmierung wird rechts unten angezeigt, neun Tracking-Elemente wurden erkannt und blockiert.

Bildquelle vgl. [willhaben 2016]

<sup>129</sup>vgl. [Ghostery, Inc. 2016a]

<sup>130</sup>Siehe Kapitel 2.1 *Was ist Internet-Tracking und wofür wird es eingesetzt?* ab Seite 6.

Ghostery kann derzeit 2073 verschiedene Tracker erkennen (Stand Jänner 2016).<sup>131</sup> Über ihre Support-Webseite gelangt man zu einem Firmenverzeichnis, wo alle Unternehmen gelistet sind, die in unterschiedlichen Formen (zum Beispiel Webanalyse, Werbedienstleister oder Datenaggregation) mit Tracking zu tun haben und von Ghostery blockiert werden können.<sup>132</sup> Klickt man auf einen Namen wird das entsprechende Ghostery-Profil der Firma geladen, das unter anderem eine Beschreibung des Unternehmens, welche Daten von ihnen gesammelt werden, einen Link zu ihren Datenschutzbestimmungen oder Kontaktdaten liefert. Über die Blockieroptionen des Add-ons kann auch nach der Trackingart, wie zum Beispiel "History Sniffing" oder "Fingerprinting", gefiltert und die zugehörige Firmenliste und deren Profile geladen werden.

Durch Ghostery wird mittels der Funktion "Click-to-Play" die Kommunikation zu Facebook, Twitter, Google-Plus und anderen sozialen Netzwerken, deren Schaltflächen auf Webseiten integriert sind<sup>133</sup>, unterbunden. Je nachdem, wie diese implementiert sind, kann es vorkommen, dass sie durch die Aktivierung entweder durch eine Ghostery-Darstellung ersetzt oder überhaupt nicht mehr angezeigt werden. Bei ersterem kann der Social-Media-Button durch einfaches Anklicken aktiviert und verwendet werden. Bei zweiterem muss der User zuerst das blockierte Tracking-Element wieder freigeben und danach die Webseite neu laden, um die Schaltfläche richtig anzuzeigen. In diesem Fall wird jedoch auch der Tracking-Schutz aufgehoben.



Abbildung 3.25: Die Grafik zeigt drei von Ghostery blockierte Social-Media-Buttons: Facebook, Twitter und Google-Plus.

Bildquelle vgl. [Ghostery, Inc. 2016a]

<sup>131</sup>vgl. [Ghostery, Inc. 2016c]

<sup>132</sup>vgl. [Ghostery, Inc. 2016b]

<sup>133</sup>Siehe Kapitel 2.2.12 *Tracking durch Facebook-, Twitter-, Google-Plus-Button und Co.* auf Seite 41.

Ähnlich wie Adblock Plus geriet auch Ghostery unter Kritik von Datenschützern. Grund dafür ist eine zusätzliche Funktion von Ghostery (vormals GhostRank genannt), die es erlaubt Daten über jene Trackingelemente zu sammeln, die beim jeweiligen User mittels Ghostery erkannt und blockiert werden. Die Funktion ist per Default deaktiviert und anonym, der User entscheidet, ob er daran teilnehmen möchte oder nicht. Ghostery finanziert sich durch die Vermarktung der gewonnenen Informationen. Dabei wird bemängelt, dass Werbe- und Trackingunternehmen Abnehmer der durch Ghostery gewonnen Daten sind, um damit ihre Trackingprodukte zu verbessern.<sup>134</sup>

Ein anderes Add-on, das 2011 herausgebracht wurde und ähnlich wie Ghostery funktioniert, ist **Disconnect**. Die Erweiterung kann für Firefox, Google Chrome, Safari und Opera heruntergeladen und als App auch für die mobilen Betriebssysteme Android und iOS installiert werden. Die Browservariante teilt Trackingelemente von Drittanbietern einer besuchten Webseite in unterschiedliche Kategorien ein: Facebook, Google, Twitter, Werbung, Analyse, Sozial und Inhalt, wobei alle Kategorien außer jene, die mit Inhalt gekennzeichnet sind, per Default geblockt werden. Der User kann sich genau anzeigen lassen, welche Tracker verhindert werden und kann sie manuell freischalten bzw. sperren oder die ganze Website auf eine Whitelist setzen. Für Chrome und Safari ist es derzeit (Stand Jänner 2016) möglich zusätzlich zur Liste der Trackingelemente einer Webseite, eine visuelle Darstellung davon anzeigen zu lassen, welche das Ausmaß aktiver Tracker auf einer Internetseite verdeutlicht.<sup>135</sup>

---

<sup>134</sup>vgl. [Tom Simonite 2013]

<sup>135</sup>vgl. [Disconnect 2016a]

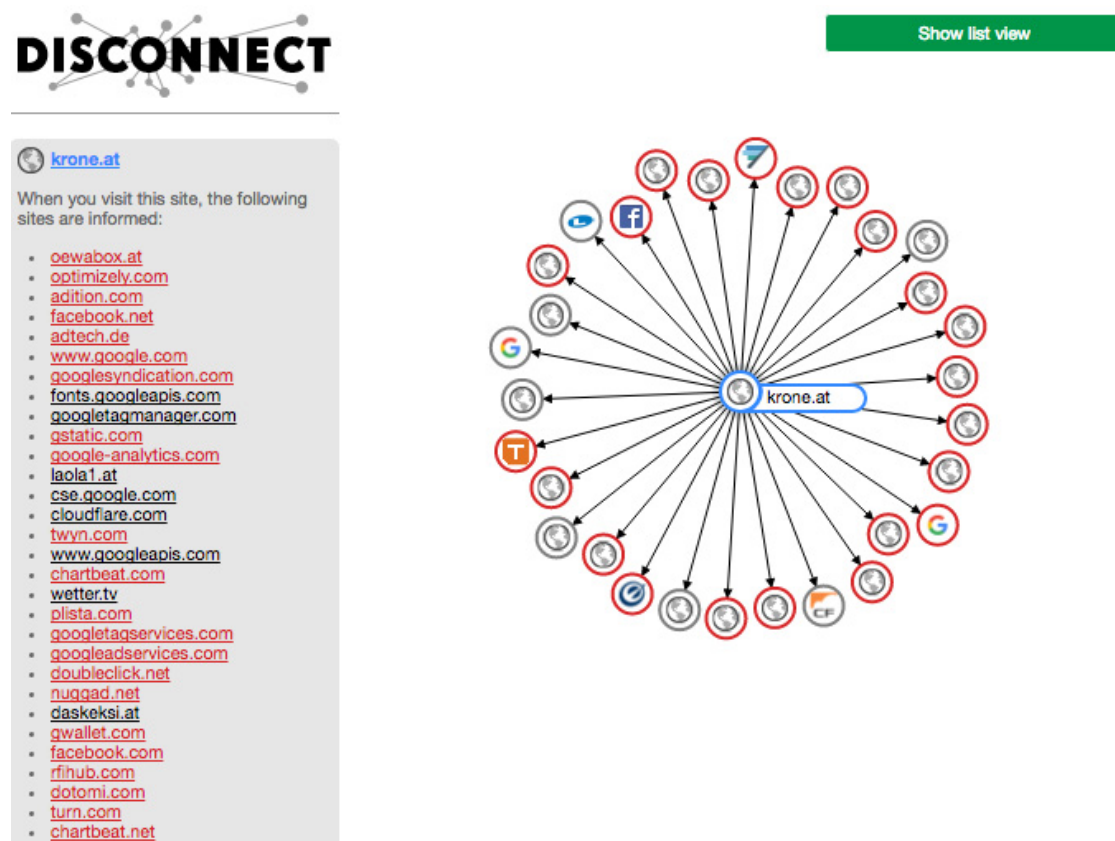


Abbildung 3.26: Die Grafik zeigt die visuelle Darstellung aller erkannten Trackingelemente des Add-ons Disconnect auf einer Artikelseite von krone.at.

Bildquelle vgl. [Disconnect 2016b]

Zum Abschluss wird eine weitere Alternative zu Ghostery vorgestellt, das Mitte 2015 veröffentlichte Projekt der amerikanischen Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) **Privacy Badger**. Die Browser-Erweiterung gibt es derzeit für Firefox und Google Chrome (Stand Jänner 2016) und möchte in Kürze auch für Opera, Safari und den mobilen Firefox Browser für Android zur Verfügung stehen. Privacy Badger analysiert laufend die Seitenaufrufe des Anwenders und erkennt Drittanbieter, die versuchen den User ohne dessen Zustimmung über mehrere Seiten hinweg zu tracken und blockiert daraufhin deren Inhalte. Dabei lernt es bei jeder neuen geladenen Webseite dazu. Das Add-on überprüft die Zustimmung indem es kontrolliert, ob Drittanbieter ein "Do Not Track"-Signal berücksichtigen oder ignorieren. Jene Inhalte von Drittanbietern, die für eine fehlerfreie Darstellung des Webangebots notwendig bzw. für den

User nützlich sind, werden identifiziert und zugelassen. Privacy Badger versucht darin eingebaute Trackingelemente weiterhin zu sperren. Aufbauend auf das ShareMeNot-Projekt<sup>136</sup> werden anstelle der Social-Media-Buttons von Facebook, Twitter, Google Plus, LinkedIn, Pinterest, Stumbleupon und AddThis alternative, von Privacy Badger generierte Schaltflächen angezeigt, um deren Tracking zu unterbinden.<sup>137</sup>

Zu Beginn der technischen Maßnahmen wurde ein Überblick über die Verbreitung der gängigsten Browser in Österreich gegeben. Danach wurden die für Datenschutz und Privatsphäre relevantesten Browsereinstellungen zu Cookies, zur Chronik und zur hinterlegten Suchmaschine beschrieben. Der "Do Not Track"-Mechanismus wurde vorgestellt, ebenso welche Vorteile das Internetsurfen im Privatmodus des Browsers hat. Anschließend wurden hilfreiche Anti-Tracking-Browsererweiterungen präsentiert, wie der Werbeblocker Adblock Plus, Flashblock, NoScript, Ghostery, Disconnect oder Privacy Badger.

Alle drei Bereiche der vorgestellten Schutzmaßnahmen gegen Internet-Tracking und Profiling, gesetzliche, organisatorische, sowie technische, spielen eine wichtige Rolle für ein Gleichgewicht zwischen invasiven Industriepraktiken zum Sammeln, Auswerten und Vermarkten von personenbezogenen Daten und der Einhaltung von Datenschutzbestimmungen und der Wahrung der Privatsphäre von Privatpersonen.

Fast zehn Jahre nach Erscheinen seines Buches "Das Ende der Privatsphäre: der Weg in die Überwachungsgesellschaft" hat die Aussage von Peter Schaar<sup>138</sup>: *"Für die Zukunft des Datenschutzes werden weltweit anerkannte Datenschutzstandards von entscheidender Bedeutung sein."*<sup>139</sup> nicht an Signifikanz verloren.

Es bleibt abzuwarten, ob die vielversprechende neue Datenschutz Grundverordnung der EU nach ihrer Umsetzungsphase in den nächsten zwei Jahren für eine Verbesserung der Datenschutzstandards in der Europäischen Union sorgen wird und welchen Einfluss sie auf den internationalen Datenaustausch und den Schutz personenbezogener Daten haben wird. Weiters ist die Entwicklung des "EU-US Privacy Shield" offen. Der Einsatz entsprechender Kontrollorgane und angemessener Konsequenzen werden von Relevanz sein.

---

<sup>136</sup>vgl. [Rösner et al. 2014]

<sup>137</sup>vgl. [Electronic Frontier Foundation 2016]

<sup>138</sup>Peter Schaar war von 2003 bis 2013 der Bundesbeauftragte für Datenschutz und Informationsfreiheit in Deutschland.

<sup>139</sup>Zitat von [Peter Schaar 2007]

Allgemeine Geschäfts- und Nutzungsbedingungen, anerkannte Gütesiegel und die Einhaltung von sinnvollen Selbstregulierungssystemen sorgen für eine Unterstützung des rechtlichen Rahmens. In diesen Aufgabengebieten sorgt das Festlegen zusätzlicher Verhaltensregeln vor allem für mehr Datensparsamkeit und Transparenz im Umgang mit Personendaten.

Die Weiterentwicklung der technischen Systeme wird zeigen, ob "Privacy by Design" und "Privacy by Default" sich zu einem IT-Standard etablieren und Enduser dabei unterstützt werden, die Kontrolle über ihre Daten zu behalten bzw. die Weitergabe beeinflussen und steuern zu können.

Im nachfolgenden Kapitel wird anhand von zehn österreichischen Beispielen die Handhabung von Datenschutzrichtlinien und die Verarbeitung personenbezogener Daten analysiert.



---

## 4 Trackingbeispiele in Österreich

Im März 2016 wurde für die vorliegende Arbeit aus Alexas 100 meistbesuchten Websites in Österreich<sup>1</sup> eine Auswahl von zehn österreichischen Internet-Auftritten getroffen, um einen groben Überblick des Datenschutzstandards der jeweiligen Seite zu geben:

- [www.orf.at](http://www.orf.at) - Österreichischer Rundfunk ORF
- [www.derstandard.at](http://www.derstandard.at) - Webportal der Tageszeitung Der Standard
- [www.kurier.at](http://www.kurier.at) - Online-Auftritt der Tageszeitung KURIER
- [www.krone.at](http://www.krone.at) - Online-Portal der Kronen Zeitung
- [www.willhaben.at](http://www.willhaben.at) - Kleinanzeigenportal Willhaben
- [www.herold.at](http://www.herold.at) - Gelbe Seiten HEROLD
- [www.karriere.at](http://www.karriere.at) - Online-Stellemarkt Karriere
- [www.bmf.gv.at](http://www.bmf.gv.at) - Bundesministerium für Finanzen
- [www.raiffeisen.at](http://www.raiffeisen.at) - Webauftritt der Raiffeisen Bank
- [www.sparkasse.at](http://www.sparkasse.at) - Online-Portal der Erste Bank und Sparkasse

Um die eingesetzten Tracking- und Profiling-Techniken zu erkennen wurden die jeweiligen AGBs bzw. Datenschutzrichtlinien gelesen und kontrolliert, wieviele Cookies im Browser gesetzt wurden und die beiden Browser-Add-ons Ghostery und Disconnect eingesetzt, um zu erkennen, welche Tracking-Elemente von Drittanbietern im Hintergrund geladen wurden.<sup>2</sup> Die Websites wurden einerseits mit Firefox in der Version 45.0 und Ghostery in der Version 6.0.3 und zur Kontrolle mit Chrome in der Version 49.0.2623.75 und Disconnect in der Version 5.18.23 aufgerufen. Beide Browser wurden dabei jeweils mit ihrer Standardkonfiguration und einer leeren Startseite geöffnet.

---

<sup>1</sup>vgl. [Alexa Internet, Inc. 2016a]

<sup>2</sup>Die Funktionen der beiden Add-ons Ghostery und Disconnect werden im Kapitel *3.3.2 Browser-Erweiterungen* auf Seite 123 beschrieben.

Im Rahmen der Begutachtung sollen zuerst die einzelnen Internetseiten vorgestellt werden. Dabei wird jeweils untersucht, welche First- und Third-Party-Cookies auf der Startseite gesetzt werden und welche Tracker von Drittanbietern aktiv sind. Weiters wird eine beliebige Unterseite geladen und der Unterschied zur Homepage bezüglich der gespeicherten Cookies und den aktiven Trackern analysiert.

Es wird beschrieben, wo die Datenschutzbestimmungen der jeweiligen Website hinterlegt sind, wie aktuell, umfangreich, verständlich und transparent diese sind. Mit Hilfe von ao. Univ.-Prof. Dr. Markus Haslinger werden die einzelnen AGBs bzw. Datenschutzerklärungen der untersuchten Websites auf ihre Datenschutzkonformität und Userfreundlichkeit hin kritisch hinterfragt und die Erkenntnisse im Einzelnen und in der Zusammenfassung präsentiert. Der dazugehörige Fragenkatalog ist im Anhang der Diplomarbeit ab Seite 161 zu finden.

Es wird ebenso angegeben, welches Webportal Social-Media-Plug-ins verwendet und welches eine Gütesiegel-Zertifizierung besitzt oder andere Selbstregulierungen getroffen hat und zum Beispiel "Opt-Out"-Möglichkeiten anbietet. Ferner soll beurteilt werden wie präsent bzw. aufdringlich Werbeanzeigen platziert, als solche gekennzeichnet und wo AdChoice Icons angezeigt werden.

Es soll klargestellt werden, dass diese Auswertung nur einen flüchtigen Überblick bietet, da als User nicht festgestellt werden kann, mit wie vielen Dienstleistern eine Website genau kooperiert. Bei jedem neuen Aufruf einer Webseite besteht die Möglichkeit, dass unterschiedliche Anzeigen von neuen Anbietern geladen werden bzw. kann sich das Angebot, wie auch die Kooperationspartner, täglich verändern bzw. variieren.

Im Anschluss wird die Website mit den meisten und jene mit den wenigsten Trackingelementen prämiert.

In einem weiteren Schritt sollen alle ausgewählten Websites in einem unmittelbaren Durchlauf geladen werden, so als würde ein User normal im Internet surfen und die einzelnen Webseiten hintereinander aufrufen. Auf diese Weise wird dargelegt, wie viele Cookies dabei insgesamt gespeichert werden und welche Drittanbieter auf unterschiedlichen Webportalen wiederholt vorkommen.

Einleitend wird noch einmal darauf hingewiesen, dass ein Websitebesucher dem Gesetz nach nicht dazu verpflichtet ist Allgemeine Geschäftsbedingungen/ Nutzungsbedingungen/ Datenschutzerklärungen etc. eines Webangebots vollinhaltlich zu lesen. Bei einer Registrierung, wo aktiv eine Bestätigung gegeben werden muss (zum Beispiel durch das Setzen eines Häkchens), dass AGBs etc. gelesen wurden, ist es sinnvoll diese tatsächlich zu lesen. Der User könnte ansonsten Forderungen zustimmen, die später nachteilig für ihn sein könnten.

Der ledigliche Aufruf einer Webseite verpflichtet nicht zum Lesen dieser Unterlagen, weshalb rechtlich betrachtet keine Zustimmung zustande kommt. Diese hat im Sinne des Datenschutzgesetzes aktiv stattzufinden. Der Benutzer soll vollständig, transparent und völlig unzweideutig über eine Datenverarbeitung informiert werden, um sich der Tragweite einer Einwilligung bewusst sein zu können. Erst danach kann eindeutig entschieden werden, ob einer Datenverarbeitung zugestimmt werden soll. Die Zustimmung muss in jedem Fall eine aktive Handlung sein. Dies ist beim bloßen Laden einer Webseite oder dem Lesen ihrer AGBs keinesfalls gegeben.

Inhalte der Art *”Mit der Nutzung der Website stimmen Sie den folgenden Bedingungen uneingeschränkt zu.”* oder *”Mit dem Aufruf der Website unterwirft sich der User den nachstehenden Bedingungen.”*, wie man sie aus den gängigen AGBs oder Datenschutzerklärungen kennt und wie sie auch bei den untersuchten österreichischen Websites vorkommen, sind dem Recht nach ungültig und nicht datenschutzkonform.

Weiters wird die Kernaussage des TKG 2003, Abschnitt 12, §96 zusammengefasst und wiederholt: Eine Website muss alle Kooperationspartner und involvierte Dritte, wo ein Austausch mit Benutzerdaten stattfindet, nennen. Der Betreiber muss detailliert bekannt geben, welche Userdaten gespeichert werden und zu welchem genauen Zweck eine Datenverarbeitung erfolgt. Es müssen abgesehen vom Hinterlegen von Cookies auch alle anderen eingesetzten Trackingtechniken angeführt werden. Das Gesetz dient dazu, um dem Internetbenutzer eine vollständige Transparenz im Bezug zur Verarbeitung seiner Daten zu bieten.<sup>3</sup>

---

<sup>3</sup>Siehe dazu Kapitel 3.1.2 *Telekommunikationsgesetz* ab Seite 71.

## 4.1 Österreichischer Rundfunk ORF - [www.orf.at](http://www.orf.at)

Auf der Startseite des Österreichischen Rundfunks werden insgesamt vier Cookies hinterlegt, ein First-Party-Cookie und drei Third-Party-Cookies: von [adworx.at](http://adworx.at) und [oewabox.at](http://oewabox.at). Durch das Aufklappen eines Nachrichtenartikels auf der Homepage werden drei weitere Third-Party-Cookies gespeichert: [syreta.at](http://syreta.at), [s373.meetrics.net](http://s373.meetrics.net). Beim Aufklappen eines anderen Artikels kommen weitere zwei Third-Party-Cookies hinzu: [doubleclick.net](http://doubleclick.net). Beim Besuch von Subseiten kommen neue First-Party-Cookies hinzu, wenn Unterseiten des ORF wie zum Beispiel [debatte.orf.at](http://debatte.orf.at) oder [sport.orf.at](http://sport.orf.at) geöffnet werden. Auch Third-Party-Cookies vermehren sich, je nachdem ob Inhalte von Drittanbietern wie zum Beispiel Instagram oder YouTube eingebettet werden. Ghostery und Disconnect erkennen vier Tracker: Xaxis, ÖWA, DoubleClick, Meetrics.

Auf [orf.at](http://orf.at) gibt es keinen Informationsbanner zum Einsatz von Cookies. Über das Impressum im Footer gelangt der User zu einer Liste an unterschiedlichen Offenlegungen der einzelnen Bereiche im ORF, wie auch zur Privacy Policy und einer detaillierten Cookie-Richtlinie. Beide Dokumente sind nicht datiert, weshalb der Benutzer nicht weiß, wie aktuell die Angaben sind. In der Cookie-Richtlinie wird unter anderem erklärt, welche Browsereinstellungen man zum Blockieren oder Löschen von Cookies vornehmen kann und welche Arten von Cookies von [orf.at](http://orf.at) eingesetzt werden: zur Darstellung, zur Authentifizierung, zur Webanalyse mittels ÖWA, zur Schaltung von Werbeanzeigen (der Dienstleister Adworx wird genannt), beim Anklicken von Social-Media-Buttons in Form der Zwei-Klick-Lösung und zur Einbettung externer Inhalte (Fotos von Instagram, Videos von YouTube, Twitter-Meldungen, etc.).

Bei den Werbecookies weist [orf.at](http://orf.at) darauf hin, dass sich die externen Unternehmen beim Verarbeiten der Userdaten an österreichische bzw. europäische Datenschutzbestimmungen halten. Angaben dieser Form täuschen dem User eine Art Sicherheit vor, die so nicht gewährleistet werden kann, da [orf.at](http://orf.at) auch mit internationalen Drittanbietern kooperiert, wo weder österreichische noch europäische Datenschutzrichtlinien gelten.

Weiters wird auf [www.youronlinechoices.com](http://www.youronlinechoices.com) verwiesen. Nachdem es aber keine Liste aller Kooperationspartner des ORF gibt, sondern der ORF diese allgemein als "Werbeanbieter" bezeichnet, kann der User nicht kontrollieren, ob alle Anbieter auch Mitglieder des Präferenzmanagements auf Your Online Choices sind. So sind zum Beispiel die durch Ghostery und Disconnect erfassten Tracker DoubleClick und Meetrics keine Mitglieder und können mittels Your Online Choices nicht blockiert werden. Orf.at hat kein Datenschutz-Gütesiegel.

Social-Media-Buttons werden auf der Startseite nur bei aufgeklappten Artikeln angezeigt. Auf Subseiten gibt es zwei Arten von Social-Media-Buttons: entweder im oberen Drittel als normale Schaltflächen oder am Ende eines Artikels durch ein Zwei-Klick-Lösung gemeinsam für alle Social-Media-Buttons. Datenschutzkonformer wäre eine Zwei-Klick-Lösung für jeden einzelnen Button. Ein Mouse-Over informiert über die Datenweitergabe an Dritte bei deren Aktivierung. Bei den herkömmlichen Buttons im oberen Drittel handelt es sich um keine Social-Media-Plug-ins, da sie weder von Ghostery noch von Disconnect blockiert werden.

Auf der Homepage und den Subseiten wird jeweils ein großer Werbebanner am rechten Rand geladen, der mit Klick geschlossen werden kann. Das AdChoice Icon wird nicht angezeigt.

## 4.2 Tageszeitung Der Standard - [www.derstandard.at](http://www.derstandard.at)

Beim Erstbesuch von [derstandard.at](http://derstandard.at) werden 14 Cookies hinterlegt: sechs First-Party-Cookies, davon kein Session-Cookie und acht Third-Party-Cookies von fünf Drittanbietern ([adition.com](http://adition.com), [adverserve.net](http://adverserve.net), [doubleclick.net](http://doubleclick.net), [oewabox.at](http://oewabox.at), [nuggad.net](http://nuggad.net)). Beim Öffnen eines Nachrichtenartikels kommt ein First-Party-Cookie und elf Third-Party-Cookies von fünf weiteren Drittanbietern hinzu. Ghostery und Disconnect erkennen auf der Homepage sechs Tracker: Adition, DoubleClick, Meetrics, Nugg.Ad, Google Analytics, ÖWA, auf einer Artikelseite kommen keine Tracker hinzu.

Auf [derstandard.at](http://derstandard.at) wird kein Banner zur Setzung von Cookies eingeblendet. Datenschutzinformationen sind im Impressum & Offenlegung, in der Datenschutzrichtlinie und in den AGBs im Footer zu finden. Es ist kein Datenschutz-Gütesiegel vorhanden.

Im Impressum wird auf das Speichern von Cookies durch ÖWA, Nugg.Ad und Google aufmerksam gemacht. Derstandard.at verlangt von seinen Lesern, falls installiert, das Deaktivieren von Werbeblockern. Deren Einsatz wird jedoch von der Website nicht kontrolliert. Nach österreichischer Gesetzeslage darf eine Website das Deaktivieren von Browser-Plug-ins, wie etwa Werbeblocker, vom User nicht verlangen. Derstandard.at könnte jedoch überprüfen ob der Websitebesucher ein entsprechendes Plug-in installiert hat und darauf reagieren, indem es jenen Besuchern zum Beispiel keine Inhalte mehr anzeigt, solange ein Werbeblocker aktiviert ist oder eine Bezahloption und damit verbunden einen Webauftritt ohne Werbeanzeigen anbietet. In Kapitel 3.3.2 *Browsererweiterungen* auf Seite 120 wird anhand des Beispiels des Webangebots der deutschen Boulevardzeitung Bild näher darauf eingegangen.

Die Datenschutzrichtlinie, die zuletzt im Juni 2015 aktualisiert wurde, informiert den Benutzer, dass konkret Cookies von ÖWA, Nugg.Ad und Google oder von beliebigen anderen Dienstleistern eingesetzt werden, wobei Userdaten nur anonymisiert gespeichert werden.

Die Allgemeinen Geschäftsbedingungen stammen ebenfalls vom Juni 2015 und enthalten in Absatz 3 die gleichen Formulierungen, wie in der Datenschutzrichtlinie.

Im Header der Start- und Ressortseiten wird auf die jeweilige Facebook-, Google-Plus- und Twitter-Unternehmensseite verlinkt. Bei einer Artikelseite werden Social-Media-Buttons von Facebook, Google-Plus und Twitter geladen, wobei es sich um keine Plug-ins handeln dürfte, da sie weder von Ghostery, noch von Disconnect blockiert werden und somit keine Verbindung zum jeweiligen sozialen Netzwerk beim Laden der Schaltfläche herstellen. Die Social-Media-Buttons werden in den Datenschutzbestimmungen nicht erwähnt.

Auf der Homepage wird oben und auf der rechten Seite ein Werbebanner und im Hauptteil im oberen Ansichtsdrittel eine weitere Werbung zwischen den Standardartikeln geladen, welche mit "BEZAHLTE ANZEIGE" gekennzeichnet ist. Auf den Artikelseiten werden ebenfalls oben und auf der rechten Seite Werbebanner eingeblendet. Im Hauptteil werden weitere zwei Werbeanzeigen platziert, die mit "bezahlte Anzeige" betitelt sind. Auf derstandard.at kommt kein AdChoice Icon zum Einsatz.

### 4.3 Tageszeitung KURIER - www.kurier.at

Auf der Startseite der Tageszeitung KURIER werden 18 Cookies gespeichert: neun First-Party-Cookies, davon keine Session-Cookies und neun Third-Party-Cookies von fünf Drittanbietern (adition.com, doubleclick.net, mookie1.com, oewabox.at, bs.serving-sys.com). Beim Laden einer Unterseite werden zwei weitere First-Party-Cookies und insgesamt 36 Third-Party-Cookies von neun zusätzlichen Drittanbietern gesetzt. Ghostery und Disconnect erkennen auf der Homepage sieben Tracker: Adition, ChartBeat, DoubleClick, Meetrics, Google Analytics, ÖWA, TrackJS, bei einem Nachrichtenartikel sind zwei weitere Tracker, Outbrain und Twitter Badge, aktiv.

Der KURIER zeigt keinen Informationsbanner bezüglich Cookies an. Es ist keine Zertifizierung durch ein Gütesiegel vorhanden. In den Allgemeinen Nutzungsbedingungen wird in Abschnitt 4 auf die Datenschutzbestimmungen von kurier.at eingegangen. Diese wurden zuletzt im Juni 2013 aktualisiert. Laut ANB darf ein User, falls installiert, keine Werbeblocker aktivieren. Deren Einsatz wird jedoch von der Website nicht kontrolliert. Diesbezüglich gilt das Gleiche wie bei derstandard.at und die Website darf ein Deaktivieren eines Browser-Plug-ins nicht einfordern.

Es wird darüber informiert, dass Webanalyse-Software, wie zum Beispiel jene der ÖWA, im Einsatz ist, Elemente von Drittanbietern wie zum Beispiel Facebook und Twitter auf kurier.at integriert sind und Werbung angezeigt wird. Es gibt keine genaue Auflistung aller Kooperationspartner.

Im Footer wird auf die jeweilige Facebook-, Twitter- und Google-Plus-Unternehmensseite verlinkt. Nachrichtenartikel zeigen Social-Media-Buttons von Facebook, Twitter, Pinterest, LinkedIn und Google-Plus an. Laut der ANB werden erst beim Anklicken Daten an das jeweilige soziale Netzwerk übertragen. Ghostery und Disconnect blockieren die Schaltflächen nicht.

Auf der Homepage wird auf der rechten Seite ein großer Werbebanner geladen. Im Hauptteil werden im Bereich "Special" bezahlte Artikel neben tatsächlichen redaktionellen Kurier-Beiträgen angezeigt. Diese sind mit "POWERED BY CONTENT GARDEN" gekennzeichnet. Content Garden ist ein Dienstleister, der sich auf die Verbreitung digitaler Inhalte und Content Marketing spezialisiert hat<sup>4</sup>. Bei aktivem Ghostery oder Disconnect werden diese Artikel nicht angezeigt. Klickt man einen Content-Garden-Artikel an, wird eine Unterseite geladen, die sich kaum vom Aussehen echter Kurier-Nachrichtenartikel unterscheidet. Lediglich das "powered by Content Garden" zu Beginn des Beitrags deutet auf einen externen Inhalt hin. Weiters kann der bezahlte Artikel nicht via soziale Netzwerke geteilt werden, die Buttons fehlen, und der Beitrag ist keiner Rubrik zugeordnet. Ein weiterer nicht redaktioneller Artikel mit dem Untertitel "LESESTOFF" ist eine Kooperation mit Morawa und präsentiert neue Bucherscheinungen der österreichischen Buchhandlung. Ein User muss sehr aufmerksam sein, um die Werbebeiträge als solche zu erkennen.



Abbildung 4.1: Die Grafik zeigt rot umrandet zwei gesponserte Beiträge auf der Homepage von "kurier.at" mit den Hinweisen "POWERED BY CONTENT GARDEN" und "LESESTOFF".

Bildquelle vgl. [KURIER 2016]

<sup>4</sup>vgl. [Content Garden 2016]



## Mehr Flair im Bad mit Dusch-WCs



SHUTTERSTOCK.COM

Sie wünschen sich ein neues Badezimmer? Schon kleine Veränderungen verbessern das Flair.

powered by Content Garden

15.03.2016

Rund sechs Euro gibt jeder österreichische Haushalt laut Statistik Austria monatlich für Badezimmermöbel aus. Im Schnitt ist das Bad jener Raum, der am wenigsten oft renoviert wird. Dusch-WCs haben nicht nur Vorteile in ihrer Anwendung, sondern beeinflussen auch die Atmosphäre im Raum positiv.

Abbildung 4.2: Die Grafik zeigt die Darstellung eines bezahlten Inhalts von Content Garden. Die Unterschiede sind rot markiert.  
Bildquelle vgl. [Content Garden 2016]

futurezone film.at events.at *Telepolis* SHOPWELT freizeit NEWSLETTER WETTER TV ABO/CLUB LOGIN

**KURIER** Lifestyle Suche

ÜBERBLICK **POLITIK** WIRTSCHAFT CHRONIK SPORT KULTUR MEINUNG JOB IMMOBILIEN KARRIERE

## Werner Faymann: "Alle Routen sind zu schließen"



Foto: APA/ROLAND SCHLAGER

Bundeskanzler Werner Faymann

Kanzler vor EU-Asylgipfel: "Durchwinken" sei zu Ende. Kritik von Lopatka und Strache.

16.03.2016, 13:19



"Das Durchwinken ist zu Ende. Alle Routen sind zu schließen."  
 Bundeskanzler Werner Faymann hat bei einer Erklärung im Nationalrat die Entschlossenheit der Regierung bei der Umsetzung der neuen Flüchtlingspolitik betont. Der Zeitpunkt ist brisant: Am Donnerstag beginnt der nächste EU-Gipfel zur Asylkrise (*mehr dazu siehe unten*)

Abbildung 4.3: Die Grafik zeigt einen tatsächlichen Nachrichtenbeitrag von KURIER in der Rubrik "Politik". Die Unterschiede sind rot markiert.

Bildquelle vgl. [KURIER ]

Auf Artikelseiten werden im Header und auf der rechten Seite große Werbebanner, links vom Text eine kleinere Werbeanzeige geladen. Innerhalb des Hauptteils wird ein kleingedrucktes Inserat angezeigt, welches mit dem AdChoice Icon gekennzeichnet ist. In den ANBs wird das AdChoice Icon nicht beschrieben.

Am Ende eines Nachrichtenartikels wird der Leser auf weitere Beiträge aufmerksam gemacht, welche mit den Überschriften "Nicht verpassen" oder "Das könnte Sie auch interessieren" angekündigt werden. Im Gegensatz zur Startseite und dem Dienstleister Content Garden, nutzt der KURIER auf Unterseiten Outbrain, um bezahlte Artikel zu positionieren. Outbrain ist ebenfalls ein Dienstleister, der digitale Inhalte verbreitet und sich auf Content Marketing spezialisiert hat<sup>5</sup>. Es werden jeweils zwei bezahlte Artikel angezeigt, die oberhalb ihres Titels mit "SPONSORED" markiert sind und auf eine externe Website verlinken, die unabhängig von dem Webangebot des KURIERS ist. Darunter sind zwei tatsächliche Kurier-Artikel platziert. Dass es sich um bezahlte Artikel handelt, ist zusätzlich am Rand mit einem kleingedruckten "empfohlen von" und einem Icon von "outbrain.com" erkennbar. Beim Anklicken des Icons öffnet sich ein Informationstext zu Outbrain, der dem User erklärt:

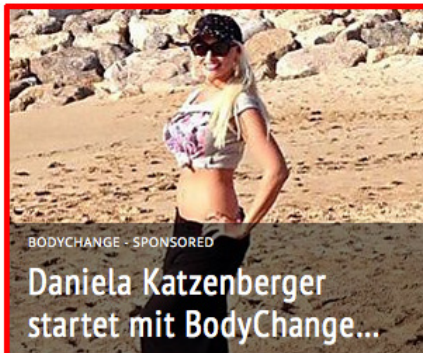
*"Wenn Sie eine Content-Empfehlung von Outbrain sehen, können Sie darauf vertrauen, dass Sie zu hochwertigen Inhalten weitergeleitet werden. Outbrain wird Sie niemals zu belangloser Werbung leiten. Daher können Sie beruhigt auf unsere Links („Wir empfehlen“ oder „Aus dem Netz“) klicken, denn Sie werden ausschließlich zu hochwertigen Inhalten weitergeleitet. Sie können bedenkenlos auf von Outbrain empfohlene Inhalte klicken."*<sup>6</sup> [Abbildung 4.5 zeigt einen Screenshot des Informationstexts]

---

<sup>5</sup>vgl. [outbrain 2016]

<sup>6</sup>Zitat von [KURIER 2016]

## Nicht verpassen



CHRONIK

### **Adelstitel: "Strafmandate" für den Hochadel**

Seit 1919 sind Adelstitel tabu. Verwenden Adelige ihre Titel trotzdem, sollen sie mehr Strafe zahlen.



POLITIK

### **Panzer statt Blumen? "Schande für Österreich"**

Die Militärpräsenz und die neue Stimmung macht Flüchtlingshelfern Sorgen – und sogar Angst.



Abbildung 4.4: Die Grafik zeigt rot umrandet zwei gesponserte Beiträge auf "kurier.at" und am rechten, unteren Rand den kleingedruckten Hinweis "empfohlen von" und das Logo von "outbrain.com".

Bildquelle vgl. [KURIER 2016]

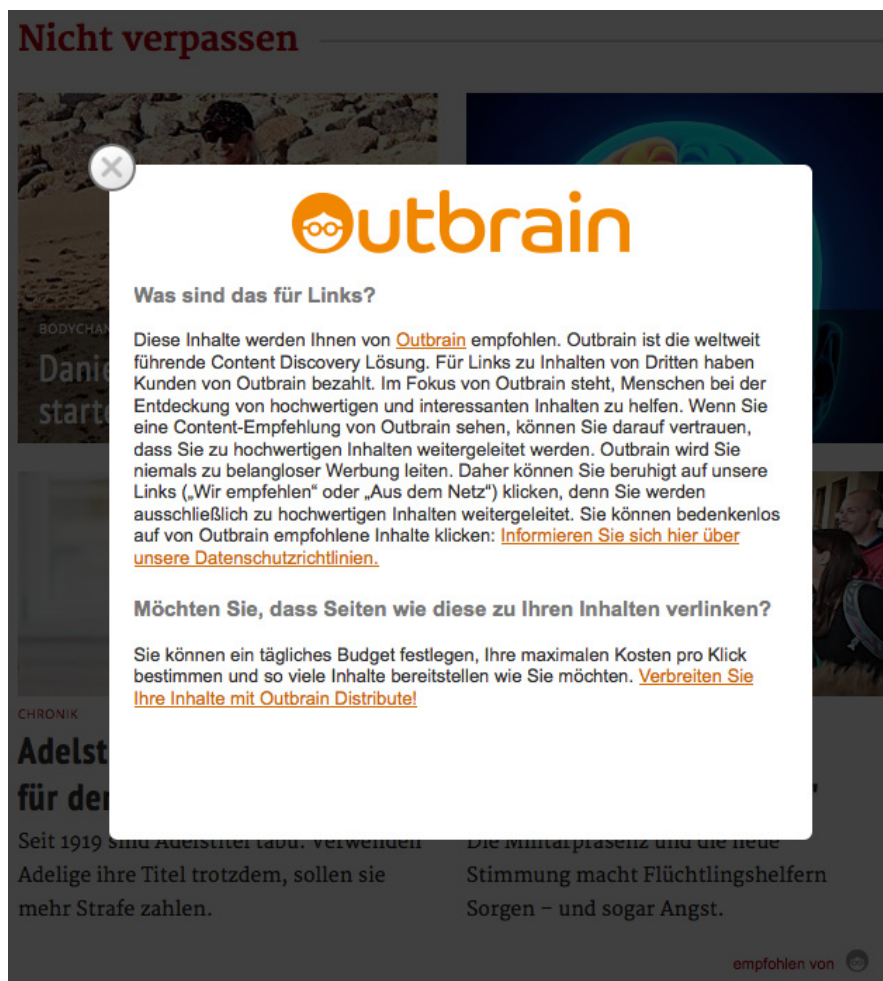


Abbildung 4.5: Die Grafik zeigt den Informationstext, wenn man auf das Logo von "outbrain.com" klickt.

Bildquelle vgl. [KURIER 2016]

Die Kooperation mit Content Garden und Outbrain wird in den ANBs nicht erwähnt.

## 4.4 Kronen Zeitung - www.krone.at

Auf der Startseite des Online-Auftritts der Kronen Tageszeitung werden 21 Cookies gespeichert: 6 First-Party-Cookies, davon kein Session-Cookie und 15 Third-Party-Cookies von 5 Drittanbietern (adtech.de, doubleclick.net, nuggad.net, oewabox.at, twyn.com). Beim Aufruf eines Nachrichtenartikels kommen 2 First-Party-Cookies und 38 Third-Party-Cookies und 17 Drittanbieter hinzu.

Ghostery und Disconnect erkennen 10 Tracker auf der Homepage: ChartBeat, Double-Click, Google Adsense, Meetrics, Nugg.ad, Twyn, Adtech, Google Analytics, ÖWA, Facebook Connect. Beim Aufruf einer Unterseite kommen drei Tracker hinzu: Adition, Plista und Twitter.

Im Footer wird ein Informationsbalken zum Einsatz von Cookies eingeblendet, "Weitere Informationen!" verlinkt zu den Allgemeinen Nutzungsbedingungen. Diese beschreibt in Abschnitt 12 ausführlich die Datenschutzbestimmungen von krone.at. Es wird darauf hingewiesen, dass sowohl Facebook-Social-Plug-ins, wie auch das Facebook-Login verwendet werden. Meldet sich ein Nutzer über sein Facebook-Konto am Portal der Kronen Zeitung an, übermittelt Facebook etwa folgende Daten an krone.at: Name, Geburtsdatum, Geschlecht, E-Mail-Adresse und Profilfoto. Krone.at macht darauf aufmerksam, dass Google Analytics, Google Adsense, Google-Plus und Google Maps integriert sind und der User der Datenverarbeitung durch Google zustimmt.

Als einzige analysierte Website erwähnt krone.at das "Safe Harbor"-Abkommen und dass Google daran teilnimmt. Im Abschnitt zu Google Analytics wird auf das von Google zur Verfügung gestellte Browser-Add-on für ein persistentes Opt-Out verlinkt. Weiters wird die Einbindung der Social-Media-Buttons von Twitter und Pinterest mitgeteilt. Zusätzlich zu Google Analytics kommen ÖWA und das Echtzeit-Webanalyse-Werkzeug Chartbeat zum Einsatz. Krone.at klärt darüber auf, welche Userdaten gespeichert, wie diese verarbeitet und dass sie an Dritte weitergegeben werden.

Jedoch wird der Zweck nicht ausführlich beschrieben ("*sonstige Marketingmaßnahmen*") und obwohl einige Drittanbieter genannt werden, werden nicht alle Kooperationspartner vollständig aufgelistet.

Die Nutzungsbedingungen wurden zuletzt im November 2014 aktualisiert. Krone.at ist mit keinem Gütesiegel zertifiziert.

Auf der Homepage kommen keine Social-Media-Buttons vor, im Header wird lediglich auf die Unternehmensseiten bei Facebook, Twitter und Google-Plus verlinkt. Ein Nachrichtenartikel kann via Facebook, Twitter und Google-Plus geteilt werden, alle drei Social-Media-Buttons werden in den AGBs erwähnt.

Ein großer Werbebanner auf der rechten Seite wird auf der Startseite eingeblendet, bei einem Artikel kommen ein Werbebanner im Header und ca. zehn weitere Artikel im Hauptteil der Webseite hinzu. Diese sind teilweise mit dem AdChoice Icon gekennzeichnet, welches in den AGBs nicht erklärt wird. Ähnlich wie beim KURIER werden zwischen echten Krone-Artikel, bezahlte Artikel angezeigt. Der Bereich wird mit "Das könnte Sie auch interessieren" angekündigt und am Ende mit einem kleingedruckten "hier werben" und "powered by plista" gekennzeichnet. Die gesponserten Beiträge sind mit dem AdChoice Icon markiert. Über die Kooperation mit Plista wird in den AGBs nicht informiert.

**Das könnte Sie auch interessieren**



**"Freunde" als Täter**  
**Asylwerber (15) von vier Jugendlichen missbraucht**  
 Zuerst rauchten fünf junge Asylwerber am Samstagabend im steirischen Söding Marihuana, dann...



**Anzeige**  
**Reich mit nur 1.000€**  
 Ohne Geldsorgen mit nur 1.000 € an der Börse. Wir zeigen nur heute kostenlos wie! Klicken Sie HIER!



**Heißer Titelkampf**  
**Hickersberger: "Beric? Mit ihm wäre Rapid..."**  
 Zehn Runden sind noch zu spielen - die österreichische Bundesliga ist spannend wie selten...



**Anzeige**  
**Dieser Trick wird Sie überraschen!**  
 Millionärs Paar zeigt Ihnen ,wie Sie monatlich 12.500€ verdienen können!



**"Bestellfernsehen"**  
**Wirbel um Wutaufrtritt des Vizekanzlers in...**  
 Bundeskanzler Werner Faymann (SPÖ) wird am Sonntag in der ORF-Reihe "Im Zentrum" zur...



**Anzeige**  
**Hochwertige Sitzauflagen für Ihre Gartenmöbel.**  
 Direkt vom Hersteller. Versandkostenfrei ab 99.- €

hier werben 

Abbildung 4.6: Die Grafik zeigt rot umrandet drei gesponserte Beiträge auf "krone.at" und am rechten, unteren Rand den kleingedruckten Hinweis "powered by plista" und dessen Logo.

Bildquelle vgl. [KronenZeitung 2016]



## 4.5 Kleinanzeigenportal Willhaben - www.willhaben.at

Auf der Startseite des Kleinanzeigenportals Willhaben werden 40 Cookies gespeichert: 15 First-Party-Cookies, davon drei Session Cookies und 25 Third-Party-Cookies von 9 Drittanbietern: adfarm1.adition.com, adnxs.com, cxense.com, oewabox.at, revsci.net, styria-digital.com, doubleclick.net, w55c.net, xiti.com. Auf einer Inseratsseite werden 17 weitere Third-Party-Cookies gespeichert, vier weitere Drittanbieter kommen hinzu. Ghostery und Disconnect erkennen neun Tracker auf der Homepage: Adition, Amazon Associates, cXense, DoubleClick, Google Adwords, AT Internet, Optimizely, ÖWA, Facebook Connect. Die Tracker bleiben unverändert, wenn man ein Inserat öffnet.

Im Footer wird ein Informationsbalken eingeblendet, der erklärt, dass Cookies eingesetzt werden, um willhaben.at zu personalisieren, soziale Medien zu integrieren und Website-Statistiken zu erstellen und dass der User sich durch die Nutzung der Website damit einverstanden erklärt.

”Details ansehen” verlinkt zu ”Nutzungsbedingungen und Datenschutz”.

Eine zusätzliche AGB behandelt in Absatz 3 ”Daten und Datenschutz”, sie wurde zuletzt im Juli 2011 aktualisiert.

Bei den Nutzungsbedingungen ist kein Datum angegeben und der User weiß nicht, wie aktuell diese Daten sind. Willhaben gibt darin unter anderem an, Website-Analyse-Software zu verwenden, dass Third-Party-Cookies von Kooperationspartnern gespeichert und Daten ausgewertet werden und wie das Verhalten von Cookies anhand des Browsers gesteuert werden kann.

In den AGBs wird in Absatz 3.1 erklärt, dass der Benutzer zustimmt, dass alle User-Daten einerseits von Willhaben gespeichert und verarbeitet und andererseits an Dritte weitergegeben werden. Hinweise dieser Art sind nach dem TKG 2003 unzureichend. Willhaben müsste ausführlich bekannt geben, zu welchem Zweck Daten erhoben und an Dritte weitergegeben werden, weiters müssten involvierte Dritte auch genannt werden.

Willhaben.at hat keine Zertifizierung durch ein Gütesiegel.

Auf der Homepage wird ein Facebook-Like-Button angezeigt, auf den Artikelseiten kann die jeweilige Anzeige mittels Facebook, Google-Plus und Twitter geteilt werden. Social-Media-Buttons werden in der Datenschutzerklärung nicht erwähnt.

Willhaben.at blendet im Header, am rechten Rand und im Hauptteil Werbeanzeigen ein, die teilweise mit dem AdChoice Icon gekennzeichnet sind. Das AdChoice Icon wird in den AGBs nicht beschrieben. Bei den Inseraten werden jeweils am rechten Rand ein großer Werbebanner und am Ende der Webseite drei Anzeigen eingeblendet, wobei zwei davon als Google-Anzeigen markiert sind.

## 4.6 Gelbe Seiten HEROLD - [www.herold.at](http://www.herold.at)

Der Internetauftritt von HEROLD setzt auf seiner Homepage 33 Cookies: zehn First-Party-Cookies, davon zwei Session-Cookies und 23 Third-Party-Cookies von 19 Drittanbietern, zum Beispiel [adform.net](http://adform.net), [adfarm1.adition.com](http://adfarm1.adition.com), [doubleclick.com](http://doubleclick.com), [xiti.com](http://xiti.com), [oe-wabox.at](http://oe-wabox.at). Beim Aufruf eines Inserats kommen sechs First-Party- und fünf Third-Party-Cookies hinzu. Ghostery und Disconnect erkennen fünf aktive Tracker: Facebook-Social-Plug-ins, ÖWA, Google Analytics, Adition und Audience Science. Auf der Inseratsseite kommt ein Tracker von AddThis hinzu.

Im Footer wird auf den Einsatz von Cookies zu unter anderem Marketingzwecken hingewiesen und auf die Cookie-Richtlinie der Website verlinkt. Diese ist ein Teil der zusätzlichen Allgemeinen Nutzungsbedingungen, wo unter Punkt 6 detailliert auf die Datenschutzbestimmungen von [herold.at](http://herold.at) eingegangen wird. Es wird aufgezählt, welche Arten von Cookies (Einstellungen, Statistik, Third-Party-Cookies) eingesetzt werden. Der Werbepartner "twyn group IT solutions & marketing services AG", DoubleClick und Google Analytics werden konkret vorgestellt. Es wird erklärt, dass Browsereinstellungen gegen das Setzen von Cookies vorgenommen werden können, im Absatz von DoubleClick wird auf die Datenschutzerklärung von Google und dessen Einsatz von Cookies für Werbung verlinkt und im Absatz von Google Analytics wird auf das von Google zur Verfügung gestellte Browser-Add-on für ein persistentes Opt-Out verlinkt.

In den AGBs wird mehrmals wiederholt, dass man sich durch die Nutzung der Website zur beschriebenen Datenverarbeitung einverstanden erklärt. Herold.at unterscheidet in seinen Nutzungsbedingungen zwischen registrierten und nicht registrierten Benutzern. Diese haben die Option, anstatt sich neu zu registrieren, sich über ihr vorhandenes Facebook-Konto bei [herold.at](http://herold.at) anzumelden.

Beim Nutzen dieser Möglichkeit, wird von Facebook eine Vielzahl an Userdaten herold.at zur Verfügung gestellt: darunter Name, Geburtsdatum, Freundesliste, Wohnort, Ausbildung, Interessen oder "Gefällt mir"-Angaben. Laut den AGB von herold.at erklärt sich der User damit einverstanden, dass seine Facebook-Daten von "HEROLD zu eigenen Werbe- und Marketingzwecken sowie zu Werbe- und Marketingzwecke von Werbekunden und Kooperationspartner von HEROLD verwendet werden"<sup>7</sup>[AGB, Abschnitt 6.4, e)]. Die positiven Aspekte dieses AGB-Abschnitts sind die genaue Auflistung der Facebook-Userdaten, die an herold.at übermittelt werden, wenn sich der Benutzer mit seinem Facebook-Konto anmeldet. Unzureichend sind die mangelhaften Informationen zu den Werbe- und Marketingzwecken und die fehlende Nennung der Werbekunden und Kooperationspartner.

Ein registrierter User kann der Verarbeitung seiner Daten widersprechen, worauf laut AGB das Kundenkonto gelöscht wird. Das österreichische Datenschutzgesetz gewährleistet, dass eine Person die Zustimmung zur Verarbeitung ihrer Daten jederzeit widerrufen darf. Das Gegenüber, in diesem Fall HEROLD, ist wiederum dazu berechtigt im Rahmen seiner Vertragsfreiheit festzulegen, dass wenn keine Zustimmung erfolgt, kein Vertrag zustande kommt und daraufhin ein Kundenkonto gelöscht wird.

Die AGB wurde zuletzt Ende Februar 2016 aktualisiert. Es gibt kein Datenschutz-Gütesiegel.

Auf der Homepage kommt das Social-Media-Plug-in von Facebook zum Einsatz, auf einer Inseratsseite werden Social-Media-Buttons von Facebook und Google-Plus geladen. Deren Einsatz wird in den AGBs nicht beschrieben.

Herold.at ladet auf seiner Startseite bis zu ca. 10 unterschiedliche Werbeanzeigen, welche vereinzelt mit einem AdChoice Icon gekennzeichnet sind. Dieses wird in den AGBs nicht erwähnt.

---

<sup>7</sup>Zitat von [HEROLD 2016]

## 4.7 Online-Stellmarkt - www.karriere.at

Auf der Startseite von karriere.at werden elf Cookies hinterlegt: acht First-Party-Cookies, davon ein Session-Cookie und drei Third-Party-Cookies von adspirit.net und oewabox.at. Beim Öffnen eines Stelleninserats kommen 54 Cookies hinzu: fünf First-Party-Cookies und 49 Third-Party-Cookies von 15 weiteren Drittanbietern. Darunter speicherte alleine der Dienstleister rubikonproject.com 14 Cookies.

Ghostery und Disconnect erkennen auf der Homepage drei Tracker: Google Analytics, ÖWA, Ad Spirit. Die Webanalyse-Programme Google Analytics und ÖWA sind auf allen Webseiten vertreten, Werbeanbieter wechseln je nach Angebot und Subseite, zum Beispiel: DoubleClick, Criteo, AdRoll, Ad Spirit.

Im Footer wird erklärt, dass der Benutzer mit dem Speichern von Cookies einverstanden ist. "Mehr erfahren" verlinkt zu "Datenschutz und Cookies". Separat können AGBs für Bewerber und Unternehmen gelesen werden, die nur für Registrierungen auf karriere.at relevant sind. Karriere.at unterscheidet in der Datenverarbeitung zwischen registrierten und nicht registrierten Benutzern. In der Datenschutzerklärung wird detailliert beschrieben, welche Daten erhoben werden, welche Arten von Cookies (Einstellungen, Sicherheit, Statistik, Werbung) gesetzt, wofür sie verwendet und wie sie gelöscht werden können.

Google Analytics und ÖWA werden als integrierte Webanalyse-Programme vorgestellt. Ein eigener Absatz beschreibt "Interessensbasierte Werbeschaltung durch Retargeting". Dabei werden auf karriere.at hinterlegte Third-Party-Cookies dazu verwendet, um auf dazugehörigen externen Websites, aufbauend auf dem Besuch von karriere.at, passende Werbeanzeigen zu schalten. Um Retargeting zu unterbinden werden zwei Opt-Out-Möglichkeiten angeboten: deaktivieren der Google Anzeigeeinstellungen und blockieren der Mitglieder der Network Advertising Initiative (NAI)<sup>8</sup>. Jedoch sind nicht alle Dienstleister, die mit karriere.at zusammenarbeiten, Mitglieder der NAI. Karriere.at müsste alle Retargeting-Kooperationspartner auflisten, nennt in seinen Datenschutzbestimmungen aber nur zwei Beispiele, Google und AdRoll.

Es ist kein Datum angegeben, wie aktuell die Datenschutzbestimmungen sind. Karriere.at hat kein Datenschutz-Gütesiegel.

Auf karriere.at werden keine externen Werbebanner angezeigt, am Ende der Homepage werden jeweils drei Unternehmen mit offenen Job-Angeboten präsentiert.

---

<sup>8</sup>Die Network Advertising Initiative ist einer der teilnehmenden Verbände des amerikanischen Selbstregulierungs-Systems, siehe dazu Kapitel 3.2.3 *Selbstregulierungs-Systeme* ab Seite 103.

Im Footer wird zu den Unternehmensseiten von [karriere.at](http://karriere.at) auf YouTube, Instagram, Twitter und Facebook verlinkt. Social-Media-Buttons kommen nur auf Inseratsseiten vor, die Art und Weise ist von der jeweiligen Firma, von der das Inserat stammt, abhängig. Darauf wird in den Datenschutzbestimmungen nicht hingewiesen. Es wäre seriöser, wenn [karriere.at](http://karriere.at) auf die unterschiedliche Integration externer Inhalte durch die inserierenden Unternehmen aufmerksam machen würde.

## 4.8 Bundesministerium für Finanzen - [www.bmf.gv.at](http://www.bmf.gv.at)

Auf der Startseite des Bundesministeriums für Finanzen werden drei First-Party-Cookies, davon ein Session-Cookie und keine Third-Party-Cookies gespeichert. Beim Laden von weiteren Webseiten kommen keine Cookies hinzu. Ghostery und Disconnect erkennen einen Tracker: das Open-Source Webanalyse-Werkzeug Piwik Analytics.

Es wird kein Informationsbalken bezüglich dem Einsatz von Cookies eingeblendet. Im Impressum gibt es einen zweizeiligen Datenschutzvermerk, dass Daten des Webseitenbesuchs anonymisiert für Statistiken ausgewertet werden. Dafür wird keine Opt-Out-Möglichkeit angeboten, obwohl Piwik dies zur Verfügung stellt.<sup>9</sup> [Bmf.gv.at](http://bmf.gv.at) hat kein Datenschutz-Gütesiegel und blendet keine Werbung von Drittanbietern ein. Das BMF könnte, um vollständig transparent zu sein, einerseits das eingesetzte Webanalyse-Werkzeug namentlich nennen und andererseits ein Opt-Out dazu anbieten. Da die Analyse anonymisiert stattfindet ist dieser Schritt nicht zwingend notwendig.

Am Ende jeder Webseite wird die Zwei-Klick-Lösung für die Social-Media-Buttons von Facebook, Twitter und Google-Plus angeboten. Aber weder ein Mouse-Over, noch sonstige Informationen erklären das Verhalten oder begründen die Zwei-Klick-Lösung.

---

<sup>9</sup>vgl. [Piwik 2016]

## 4.9 Raiffeisen Bank - www.raiffeisen.at

Auf der Homepage der Raiffeisen Bank werden insgesamt 28 Cookies hinterlegt: 13 First-Party-Cookies, davon 6 Session-Cookies, und 15 Third-Party-Cookies, von doubleclick.com, info.elba.at, iasds01.com, t.mindtake.com und zehn von styria-digital.com. Ghostery und Disconnect erkennen drei Tracker: Google Analytics, DoubleClick und SMART AdServer. Beim Laden einer Unterseite bleibt die Anzahl der Cookies und Tracker unverändert.

Im Header wird darüber informiert, dass der User zustimmt, dass auf raiffeisen.at *”Cookies für Analysen, personalisierten Inhalt und Werbung verwendet”* werden. Über *”Weitere Informationen”* wird auf einen kurzen *”Hinweis zum Datenschutz und zum Einsatz von Cookies”* verlinkt. Dort wird erklärt, dass auf der Website Analyse-Software eingesetzt wird und Cookies folgender Drittanbieter für Werbeeinblendungen gespeichert werden: twyn.com, yoondo.com, xaxis.at, smartadserver.com. Es wird wiederholt, dass man durch die Nutzung der Website, dem Setzen von Cookies für Websiteanalysen und Werbung zustimmt. Es werden keine Opt-Out-Möglichkeiten angeboten, aber auf etwaige Browsereinstellungen für Cookies hingewiesen.

In drei Bereichen wird auf Datenschutz eingegangen: Impressum, Disclaimer, Hinweis zu Datenschutz, wobei dieser Absatz eine Kopie aus dem Disclaimer und keine zusätzliche Information darstellt. Die AGBs beinhalten rein Bedingungen für tatsächliche Bankkunden und sind unabhängig von der Website. Das Impressum ist ohne Datum, der Disclaimer wurde zuletzt im März 2012 aktualisiert. Im Impressum wird detailliert auf den Einsatz von Google-Analytics hingewiesen und auf das von Google zur Verfügung gestellte Browser-Add-on für ein persistentes Opt-Out verlinkt. Es ist keine Zertifizierung durch ein Datenschutz-Gütesiegel vorhanden.

Auf den Subseiten von raiffeisen.at wird die Zwei-Klick-Variante von heise für die Social-Media-Buttons von Facebook, Twitter und Google-Plus eingesetzt. Ein Mouse-Over informiert bei jedem Button über die mögliche Datenweitergabe an Dritte. Weder im Impressum, noch im Disclaimer wird darauf eingegangen. Im Footer wird auf die jeweilige Unternehmensseite auf Facebook, Twitter, YouTube und Google-Plus verlinkt.

Raiffeisen.at lädt jeweils auf der Homepage und den Subseiten auf der rechten Seite einen großen Werbebanner. Dabei handelt es sich meistens um Eigenwerbung, es werden aber auch externe Inserate wie etwa von einem Mobilfunkanbieter oder Lebensmittelkonzern angezeigt. Die Werbungen haben kein AdChoice Icon integriert.

## 4.10 Erste Bank und Sparkasse - [www.sparkasse.at](http://www.sparkasse.at)

Auf der Startseite der Sparkasse werden insgesamt 7 Cookies gespeichert: sechs First-Party-Cookies, davon drei Session-Cookies, und ein Third-Party-Cookie des Webanalyse-Anbieters Webtrekk. Beim Laden einer Unterseite kommt ein Drittanbietercookie von Doubleclick hinzu. Ghostery und Disconnect erkennen folgende Tracker: Webtrekk auf allen Webseiten und Doubleclick auf Subseiten.

Im Header wird ein Informationsbanner eingeblendet, der auf den Einsatz von Cookies und Analysesoftware aufmerksam macht und zu den Datenschutzbestimmungen verlinkt. Darin wird auf den Einsatz von Webtrekk hingewiesen und eine Opt-Out-Möglichkeit angeboten, beim Anklicken eines Links wird das persistente Cookie "webtrekkOptOut" gespeichert. Zusätzlich wird die Verwendung von Retargeting und Tracking beschrieben, um personalisierte Werbung zu schalten. Auch hiervon kann man sich über einen Link, der beim Anklicken das persistente Cookie "SPARKASSE\_GLOBAL\_OPT\_OUT" hinterlegt, abmelden.

In den Datenschutzbestimmungen wird die Zusammenarbeit mit sozialen Netzwerken und das Umgehen einer Datenweitergabe erklärt. Unterseiten können über Facebook, Twitter und LinkedIn geteilt werden, aber erst beim Anklicken des jeweiligen Buttons werden Daten weitergegeben. Ghostery und Disconnect blockieren die Schaltflächen nicht. Im Footer wird auf die jeweilige Unternehmensseite auf Facebook und YouTube verlinkt.

Insgesamt gibt es drei Bereiche, die Informationen zu Datenschutz auf [sparkasse.at](http://sparkasse.at) liefern: Impressum, Datenschutz/ Sicherheit und Geschäftsbedingungen, wobei nur die speziellen Geschäftsbedingungen für das Portal relevant sind. Bei Impressum und Datenschutzerklärung wird kein Datum angegeben, der User weiß nicht, wann die Informationen zuletzt aktualisiert wurden. Die AGB des Portals stammt aus März 2006. Sofern die gesetzlichen Rechtsgrundlagen unverändert bleiben und konsumentenschutz-

rechtliche Neuerungen eine Website nicht dazu verpflichten, müssen AGBs, Nutzungsbedingungen, Datenschutzerklärungen etc. nicht laufend überarbeitet werden. Es existieren keine rechtlichen Vorgaben, dass ein Websitebetreiber regelmäßige Aktualisierungen durchzuführen hat. Der Datenschutzabschnitt in den Geschäftsbedingungen des Sparkasse-Portals ist einfach und allgemein formuliert. Dies lässt darauf schließen, dass die Version aus 2006 weiterhin gültig ist.

Sparkasse.at hat kein Datenschutz-Gütesiegel und blendet keine Werbung von Drittanbietern ein.

## 4.11 Tracking-Ergebnisse

Generell muss darauf hingewiesen werden, dass die Anzahl der Cookies und Tracker aufgrund unterschiedlicher Kooperationspartner beim wiederholten Aufrufen von Webseiten selten ident ist und leicht variiert. Das Ergebnis wurde anhand eines Websitebesuchs bestimmt.

Die Untersuchung der zehn Websites hat ergeben, dass beim Aufruf der Startseite von willhaben.at insgesamt die meisten Cookies gespeichert werden: 40, davon sind 15 First-Party-Cookies und 25 Third-Party-Cookies von 9 Drittanbietern.

Wird eine zusätzliche Unterseite geladen, werden am häufigsten Cookies bei karriere.at hinterlegt: 65, davon 52 Third-Party-Cookies. Aber auch auf willhaben.at mit 63, davon 42 Third-Party-Cookies, und krone.at mit 61, davon 53 Third-Party-Cookies, ist die Anzahl der Cookies beim Öffnen einer weiteren Webseite hoch.

Herold.at kooperiert mit den meisten Drittanbietern. Es konnten 24 unterschiedliche Unternehmen festgestellt werden.

Das Bundesministerium für Finanzen hat das geringste Cookie-Aufkommen. Beim Laden der Homepage werden drei First-Party-Cookies und keine Third-Party-Cookies gesetzt. Ein Tracker, "PiWiK Analytics", ist aktiv. Dieser wird für Website-Analysen eingesetzt. Dem Besucher wird dafür keine Opt-Out-Option geboten, jedoch werden laut den Datenschutzbestimmungen des BMFs nur anonymisierte Daten gespeichert.



Der am häufigsten vorkommende Drittanbieter ist DoubleClick. Neun der zehn Websites setzen das Tochterunternehmen von Google, das sich auf Online-Werbung spezialisiert hat, ein. Nur herold.at informiert den User in seinen Datenschutzbestimmungen über die Zusammenarbeit mit DoubleClick und verlinkt zu Googles "Datenschutzerklärung & Nutzungsbedingungen" bezüglich Werbung, in denen auch über Einstellungs- und Opt-Out-Möglichkeiten informiert wird.

In einem Durchgang werden beim Öffnen aller zehn Startseiten und einer jeweiligen Unterseite 270 Cookies gespeichert: 91 First-Party-Cookies und 179 Third-Party-Cookies von 74 Drittanbietern. Möchte sich ein User mit allen Datenschutzbestimmungen auseinandersetzen, müsste er einerseits jene zehn AGBs/ Datenschutzerklärungen/ Impresen der ursprünglich aufgerufenen Websites lesen und andererseits 74 weitere der zusätzlich involvierten Drittanbieter. 74 sind nur jene Drittanbieter, die mittels Third-Party-Cookies identifiziert werden konnten. Es können auch noch weitere Dienstleister beteiligt sein, die abgesehen von Cookies, andere Tracking-Elemente anwenden, womit sich die Zahl der zu beachtenden Datenschutzrichtlinien noch erhöht.

Sieben der zehn Websites kooperieren mit der Österreichischen Webanalyse ÖWA. Sie ist ein Verein, deren Mitglieder sich aus einer Vielzahl von österreichischen Online-Anbietern zusammensetzt. Die durchgeführte Datenerhebung soll einen objektiven Überblick über die Online-Angebote ihrer Mitglieder und vergleichbare Datensätze liefern, die auch online abrufbar sind. Sie bietet ihren Kunden eine Auswertung der Nutzung der jeweiligen Internetpräsenz an. Dabei werden folgende Kriterien analysiert: eindeutige Besucher der Website, Zugriffe auf die Website, Aufrufe von verschiedenen Einzelseiten der Website, Anteile der Seitenaufrufe aus Österreich in Prozent und die durchschnittliche Verweilzeit auf der Website.<sup>10</sup> Fünf der sieben Websites erwähnen den Einsatz der Webanalyse-Software der ÖWA in ihren AGBs.

---

<sup>10</sup>vgl. [OEWA]

Drei Websites, krone.at, willhaben.at und herold.at, verwenden Social-Media-Plug-ins und geben somit direkt Userdaten an das jeweilige soziale Netzwerk weiter. Davon beschreibt nur krone.at in seinen Allgemeinen Nutzungsbedingungen detailliert den Einsatz von Facebook-Social-Plug-ins, Google-Plus, Pinterest und Twitter. Bei allen vier Anwendungen formuliert krone.at in den Nutzungsbedingungen *”Durch die Nutzung dieser Plattform erklärt sich der Nutzer mit der Bearbeitung der Daten durch [die jeweilige soziale Plattform] einverstanden.”*. Wie zu Beginn der Analyse beschrieben, erklärt sich ein User durch das bloße Laden einer Webseite rechtlich zu nichts. Womit die Datenweitergabe an Facebook, Google, Pinterest und Twitter nicht datenschutzkonform ist.

Orf.at, bmf.gv.at und raiffeisen.at setzen auf die Zwei-Klick-Lösung bei der Anzeige von Social-Media-Buttons.

Derstandard.at, kurier.at und sparkasse.at haben eigene Social-Media-Button-Implementierungen im Einsatz, wo beim initialen Laden keine Userdaten weitergegeben werden.

Karriere.at selbst hat keine Social-Media-Buttons integriert, jedoch werden auf den Webseiten der einzelnen Stellenangebote, abhängig von der jeweiligen Gestaltung des Unternehmens, welche angezeigt und somit Benutzerdaten weitergegeben.

Sieben Websites finanzieren ihren Online-Auftritt teilweise durch Werbung. Davon verlangen derstandard.at und kurier.at in ihren AGBs ein Deaktivieren eines eingesetzten Werblockers von ihren Lesern, kontrollieren jedoch nicht, ob ein dementsprechendes Add-on im Browser aktiv ist. Vier Websites, kurier.at, krone.at, willhaben.at und herold.at blenden teilweise das AdChoice Icon am Rand von Werbeanzeigen ein. Davon erklärt keine in ihren AGBs oder Datenschutzbestimmungen, was das AdChoice Icon bedeutet. Drei Websites, karriere.at, bmf.gv.at und sparkasse.at, verzichten vollständig auf Werbeinserate durch Drittanbieter.

Sechs Websites informieren ihre Besucher mittels eines Banners am oberen oder unteren Rand der jeweiligen Website, dass sie auf ihren Seiten Cookies einsetzen und verlinken zu ihren Datenschutzbestimmungen oder AGBs. Davon holen fünf anhand der eingeblendeten Information vom User die Zustimmung ein, dass er mit dem Setzen von Cookies einverstanden ist. Dies ist nicht im Sinne der gesetzlichen Verordnung und gilt nicht als Zustimmung durch den User. Wie in Kapitel 3.1.2 *Telekommunikationsgesetz* ab Seite 72 beschrieben, muss ein Benutzer zuerst gründlich über eine Datenverarbeitung informiert werden. Weiters hat eine Zustimmung aktiv zu erfolgen. Das Laden einer Webseite oder Lesen eines Informationsbanners ist keine Zustimmung.

Unabhängig von der Anzeige eines Informationsbanners, erklären neun von zehn Websites in ihren Datenschutzbestimmungen, AGBs oder Impresen den Einsatz von Cookies

und dass diese mittels entsprechender Browser-Einstellung blockiert oder gelöscht werden können. Eine Ausnahme ist das Bundesministerium für Finanzen, welches ohnehin nur drei First-Party- und keine Third-Party-Cookies speichert.

Darüber hinaus bieten fünf der untersuchten Websites selektive Opt-Out-Möglichkeiten an. Selektiv bedeutet, dass der Besucher nicht alle eingesetzten Tracking-Elemente einer Website deaktivieren kann, sondern nur teilweise. Orf.at verlinkt auf [www.youronlinechoices.com](http://www.youronlinechoices.com), gibt aber keine Liste seiner Drittanbieter an und somit keine Kontrollmöglichkeit, ob ein Benutzer durch den Präferenzmanager der Seite alle externen Dienstleister blockieren kann. Krone.at, die mit einer Vielzahl an Kooperationspartner zusammenarbeitet, informiert ihre User nur über das Browser-Add-on für Google Analytics. Herold.at verlinkt ebenfalls zur Browser-Erweiterung von Google-Analytics, wie auch zu Googles Werbeinformationen in Zusammenhang mit dem Einsatz von Cookies durch Googles Tochterunternehmen DoubleClick. Karriere.at verweist direkt auf die Einstellungsseite von Google-Anzeigen und auf die Opt-Out-Liste der Network Advertising Initiative. Auch raiffeisen.at stellt einen Link zum Google Analytics Browser-Add-on zur Verfügung.

Sparkasse.at bietet als einzige der untersuchten Websites direkte Opt-Out-Optionen aller ihrer eingesetzten Tracking-Elemente an. Mittels Klick können zwei Opt-Out-Cookies gesetzt werden, die einerseits die Analyse der Benutzung der Website durch Webtrekk vermeiden und andererseits Retargeting und Tracking, um personalisierte Werbung zu generieren, blockieren. Abschließend soll darauf hingewiesen werden, dass sich die angebotenen Opt-Out-Möglichkeiten rein auf Cookies und keine anderen Tracking-Techniken beziehen. Cookies können ohnehin am einfachsten durch Einstellungen im Browser unterbunden werden, indem das generelle Setzen von Third-Party-Cookies untersagt wird und beim Beenden des Browsers alle gespeicherten Cookies gelöscht werden. Wie Anfangs erwähnt, erklären neun der analysierten Websites, dass das Speichern von Cookies mittels dem Browser verhindert werden kann. Dies stellt im Zusammenhang mit dem Abwehren von Cookies von Drittanbietern die relevanteste Information für den User dar.

Keine der analysierten Websites besitzt eine Zertifizierung durch ein Datenschutz-Gütesiegel.

In der abschließenden Tabelle werden die erfassten Daten der Website-Analyse noch einmal zusammengefasst. Die Website des Bundesministeriums für Finanzen verhält sich am datenschutzkonformsten. Alle erhobenen Daten werden anonymisiert. Die geringe Anzahl an Tracking-Elementen ist gelb hervorgehoben. Das Kleinanzeigenportal Willhaben, der Online-Stellenmarkt Karriere und die Gelben Seiten HEROLD setzen die meisten Tracking-Komponenten ein, ihre Werte sind grün markiert.

Tracking	ORF	Standard	KURIER	Krone	Willhaben
First Party Cookies Startseite	1	6	9	6	15
Third Party Cookies Startseite	3	8	9	15	25
Cookies insgesamt Startseite	4	14	18	21	40
First Party Cookies Unterseite	2	7	11	8	21
Third Party Cookies Unterseite	10	19	36	53	42
Cookies insgesamt Unterseite	12	26	47	61	63
Drittanbieter insgesamt	5	10	14	22	13
Cookie Banner	Nein	Nein	Nein	Ja	Ja
Google Analytics	Nein	Ja	Ja	Ja	Nein
DoubleClick	Ja	Ja	Ja	Ja	Ja
ÖWA	Ja	Ja	Ja	Ja	Ja
AdChoice Icon	Nein	Nein	Ja	Ja	Ja
Social-Media-Plug-ins	2-Klick-Lösung	Nein	Nein	Ja	Ja
Opt-Out-Möglichkeit	Ja	Nein	Nein	Ja	Nein
Datenschutz-Gütesiegel	Nein	Nein	Nein	Nein	Nein
Tracking	HEROLD	Karriere	BMF	Raiffeisen	Erste Bank
First Party Cookies Startseite	10	8	3	13	6
Third Party Cookies Startseite	23	3	-	15	1
Cookies insgesamt Startseite	33	11	3	28	7
First Party Cookies Unterseite	16	13	-	13	6
Third Party Cookies Unterseite	28	52	-	15	2
Cookies insgesamt Unterseite	44	65	3	28	8
Drittanbieter insgesamt	24	17	1	7	2
Cookie Banner	Ja	Ja	Nein	Ja	Ja
Google Analytics	Ja	Ja	Nein	Ja	Nein
DoubleClick	Ja	Ja	Nein	Ja	Ja
ÖWA	Ja	Ja	Nein	Nein	Nein
AdChoice Icon	Ja	Nein	Nein	Nein	Nein
Social-Media-Plug-ins	Ja	Ja	2-Klick-Lösung	2-Klick-Lösung	Nein
Opt-Out-Möglichkeit	Ja	Ja	Nein	Ja	Ja
Datenschutz-Gütesiegel	Nein	Nein	Nein	Nein	Nein

Abbildung 4.7: Die Grafik zeigt die Tracking-Daten der zehn analysierten österreichischen Websites.

## 5 Fazit und Best Practice

Ziel dieser Diplomarbeit ist es, ein Grundwissen über Online-Tracking im Allgemeinen und vorherrschende Tracking-Praktiken im Internet bereitzustellen, einen Einblick in rechtliche Rahmenbedingungen zu geben, technische Möglichkeiten zum Schutz personenbezogener Daten vorzustellen und die Problematik des invasiven Online-Trackings, massiven Datensammelns, weitreichenden Profilings und die Personalisierung des Internets zu thematisieren.

Es war erschreckend festzustellen, in welchem Ausmaß Web-Tracking und das Sammeln persönlicher Informationen stattfindet und wie technisch ausgereift, fortschrittlich und hartnäckig die dafür eingesetzten Tracking-Technologien sind.

Die größte Herausforderung der Arbeit lag an der Erarbeitung der Schutzmaßnahmen und dem Verständnis der einzelnen nationalen und internationalen Gesetze und Richtlinien. Ohne die Konsultation eines Rechtsexperten ist es für Laien schwierig, die Auslegung des rechtlichen Rahmens richtig zu erfassen. Durch das Inkrafttreten der neuen Datenschutz-Grundverordnung der EU, wird es auch innerhalb Österreichs in den nächsten zwei Jahren zu Datenschutzreformen kommen. Der Inhalt des offiziellen Textes lässt auf strengere Richtlinien und härtere Konsequenzen bei Nichteinhaltung der Vorschriften und somit auf eine Verbesserung des Datenschutzes hoffen. Auch die Umsetzung des neuen "EU-US Privacy Shield" bezüglich eines datenschutzkonformen und sicheren internationalen Datenaustauschs ist derzeit ein anhaltender Prozess, dessen Weiterentwicklung spannend bleibt.

Besonders missverständlich war der Bereich der organisatorischen Maßnahmen und Selbstregulierungssysteme. Nach außen hin lassen umfangreiche Nutzungsbedingungen, AGBs und Datenschutzbestimmungen den Eindruck entstehen, Unternehmen wären an höchstmöglicher Transparenz und bestmöglicher Informierung ihrer Kunden bemüht. In Wirklichkeit ist oft das Gegenteil der Fall, AGBs werden gezielt mit juristischen,

ungewohnten Fachausdrücken formuliert und umständlich, langwierig, mit kleiner Schrift und über mehrere Seiten hinweg entworfen, um Anwender zur Resignation zu bringen. Datenschutz-Gütesiegel machen einen guten ersten Eindruck, aber bei genauerer Betrachtung fehlt die Kontrolle durch öffentliche Organe und Firmen zahlen für eine Zertifizierung sowie den Erhalt eines Gütesiegels.

Die Umsetzung von Opt-Out-Möglichkeiten ist noch nicht ausgereift. Es ist positiv, dass es Initiativen gibt, die um Opt-Out-Optionen bemüht sind und Firmen auch eigene Vorgehen anbieten. Ein Opt-Out macht jedoch nur Sinn, wenn es persistent und unabhängig von etwaigen Browser- und Cookieeinstellungen hinterlegt wird und erhalten bleibt, wenn Cookies gelöscht werden.

Obwohl das Senden eines "Do Not Track"-Signals erst bei den technischen Maßnahmen erwähnt wird, kann es auch zu den organisatorischen gezählt werden und ist eine Art von Selbstregulierung. Es ist lobenswert, dass alle gängigen Browser die Auswahl der "Do Not Track"-Einstellung anbieten und Websites somit darauf reagieren können. Jedoch fehlt auch hier ein eindeutiger und international gültiger Standard, der beschreibt, was geschehen soll, wenn ein User "Do Not Track" mitsendet und welche Konsequenzen es für Websites hat, wenn es ignoriert wird.

Um das Sammeln, Speichern, Auswerten und Vermarkten von Daten selbst zu bestimmen und Tracking im Internet unterbinden zu können, sind entsprechende Browsererweiterungen wesentlich. Add-ons wie Adblock Plus und Ghostery verlieren an Glaubwürdigkeit, wenn sie Einträge in ihre Whitelist verkaufen oder ebenfalls vom Anwender erhobene Daten vermarkten.

Die Diplomarbeit zeigt auf, dass das untersuchte Themengebiet sehr komplex und vielschichtig ist. Es ist nicht ausreichend, wenn einzelne politische, gesellschaftliche oder technische Lösungen für die Datenschutzproblematik im Internet gefunden werden. Alle drei Parameter müssen harmonisieren und aufeinander abgestimmt werden, um einen sinnvollen Konsens mit der Wirtschaft finden zu können.

Es braucht weltweit einheitlich gültige Datenschutzgesetze, Kontrollorgane und entsprechende Konsequenzen bei Verletzung oder Nichteinhaltung der Gesetze und Richtlinien. Gesellschaftlich müsste im Bereich der Bildung an einem Grundverständnis der Tracking-Problematik und der Förderung einer umfassenden Medienkompetenz gearbeitet werden. Internetanwender sind sich der möglichen negativen Auswirkungen umfassender Personenprofile oft nicht bewusst und benötigen eine sachgemäße Sensibilisierung, um kompetente Entscheidungen bei der Weitergabe personenbezogener oder sensibler Daten treffen zu können.

Der deutsche Chaos Computer Club bietet seit 2007 die Bildungsinitiative "Chaos macht Schule" an. Das wienerische Pendant versucht aktuell (Stand Juni 2016) dieses Projekt ebenfalls in Österreich zu starten. In Zusammenarbeit mit Schulen sollen Lehrer, Schüler und Eltern über relevante Internet- und Technikthemen informiert werden.<sup>1</sup> Investigative Berichterstattung wie die Serie "What They Know" vom amerikanischen Wall Street Journal oder die interaktive Online-Dokumentationsreihe "donottrack-doc.com"<sup>2</sup> der französischen Produktionsfirma Upiant<sup>3</sup> sollten stärker gefördert werden.

Als Best Practice wäre u.a. eine Unterstützung durch die eingesetzte Technik, aber auch ein Entgegenkommen vonseiten der Wirtschaft wünschenswert.

Beim erstmaligen Starten eines Browsers könnte der Anwender durch die einzelnen Browsereinstellungen zu Datenschutz und Privatsphäre geführt werden und pro Auswahlmöglichkeit eine Art Einschulung erhalten, was das jeweilige Aktivieren bzw. Deaktivieren beim Internetsurfen bewirkt. Die Entscheidung des Deaktivierens sollte beim Benutzer liegen. Drittanbietercookies sollten, so wie es bei Apples Browser Safari gelehrt wird, per Default blockiert werden. Beim Beenden des Browsers sollten alle Cookies, Cache, Chronik und Formulareinträge gelöscht werden. Browserinformationen, die für den Aufbau einer Webseite irrelevant sind, sollten immer anonymisiert mitgesendet werden. "Do Not Track" sollte von Haus aus aktiv sein und tatsächlich als solches ausgelegt werden, nicht wie oft üblich, als "Do Not Target". Dies hat zur Folge, dass keine Personalisierung stattfindet, aber der User weiterhin getrackt und Daten gesammelt werden. Beim Aufrufen einer Website sollte ein Benutzer nicht vor vollendete Tatsachen gestellt werden, sondern tatsächlich Entscheidungen betreffend der Erhebung und Verarbeitung seiner Daten fällen können. Infobanner sollten detaillierte, vollständige und einfach verständliche Informationen zu den Datenschutz- und Nutzungsbedingungen der Website liefern. Im Gegensatz zum derzeitigen Opt-Out, sollte das Opt-In zu allen Tracking-Techniken Standard sein. "Do Not Track"- und Opt-Out-Einstellungen sollten einheitlich respektiert werden. Der Benutzer sollte die Wahl haben, ob er den Nutzungsbestimmungen der Website zustimmt, ob Cookies oder andere Trackingtechniken eingesetzt werden dürfen oder nicht und wenn nicht, sollte ihm eine Alternative angeboten werden. Zum Beispiel könnte der Besuch einer von Drittanbieter freien Website mittels passender Bezahlmodelle ermöglicht werden.

Dem Internetuser sollte generell die Selbstbestimmung und die Macht über seine Daten zurückgegeben werden.

---

<sup>1</sup>vgl. [Chaos Computer Club Wien 2016]

<sup>2</sup>Der Bayerische Rundfunk, Arte und der National Filmboard of Canada haben in einer Koproduktion sieben Folgen zum Thema Tracking gestaltet, woran der Zuseher aktiv teilnehmen und so Tracking persönlich wahrnehmen kann.

<sup>3</sup>vgl. [UPIAN 2015]

## 6 ANHANG

### Fragenkatalog

Anschließend der Fragenkatalog wurde beim Interview mit ao. Univ.-Prof. Dr. Markus Haslinger an der Technischen Universität Wien am 14. April 2016 eingesetzt:

#### Allgemeine Fragen:

1.) Folgende Gesetze wurden im Rahmen dieser Diplomarbeit herangezogen, fehlt ein wichtiges Gesetz zum Verständnis des Themas?

- Österr. Datenschutzgesetz
- Telekommunikations-Gesetz, EU-Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), wird auch Cookie- oder E-Privacy-Richtlinie genannt
- E-Commerce-Gesetz
- neue EU-Datenschutz-Grundverordnung
- "Safe Harbor"-Abkommen bzw. "EU-US Privacy Shield"

2.) Welche Privacy-/Datenschutzgesetze gelten für österreichische Portale internationaler Unternehmen wie zum Beispiel google.at, facebook.at, amazon.at, ebay.at, etc.?

3.) Gibt es eine Behörde, die Websites und deren Einhaltung der Datenschutzgesetze kontrolliert? Welche Möglichkeiten gibt es einen Missstand zu melden, kann ich als Privatperson Einfluss nehmen?



4.) Ist ein Websitebetreiber dazu verpflichtet, AGBs, Datenschutzbestimmungen etc. regelmäßig zu aktualisieren? Wenn ja, gibt es hier Vorgaben wie zum Beispiel jährlich? ZB. AGB der Sparkasse aus 2006.

5.) Ist die IP-Adresse ein personenbezogenes Datum? Laut Artikel 29 Datenschutzgruppe JA, wie ist die Regelung in Österreich?

6.) Laut E-Commerce-Gesetz, muss Werbung als solche gekennzeichnet sein. Gibt es Vorgaben, wie genau? Gibt es Vorgaben zur Kennzeichnung von personalisierter Werbung? Wird zw. personenbezogener und nicht personenbezogener Werbung unterschieden? Müssen Unternehmen bei der Schaltung von Werbung angeben, ob diese personalisiert ist?

7.) Was bedeutet die Ungültigkeit des "Safe Harbor"-Abkommens? Datenverarbeitung findet basierend darauf weiterhin statt. Gibt es Konsequenzen? Gibt es andere internationale Regelungen, die hier für Datenschutz sorgen?

8.) Muss der "Do Not Track"-Header berücksichtigt werden? Gibt es Konsequenzen wenn er nicht berücksichtigt wird?

**Fragen zum TKG 2003, Abschnitt 12, §96:** Die beiden relevantesten Erneuerungen bezüglich der EU-Richtlinie im TKG 2003 sind durch die allgemeinen Datenschutzbestimmungen in Abschnitt 12, §96 beschrieben:

*"Die Übermittlung von [...] Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, [...] erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. [...]"*[TKG 2003 Abschnitt 12, §96, Absatz (2)]

*”Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft [...], sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat. [...]. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen [...] zu erfolgen. [...]”*[TKG 2003 Abschnitt 12, §96, Absatz (3)]

1.) Ist es datenschutzkonform, wenn ich eine Homepage initial lade und darauf ist zum Beispiel ein Facebook-Like-Button aktiv, der Daten von mir an Facebook sendet oder Google Analytics ist aktiv, das ebenfalls Daten von mir an Google sendet, etc.?

2.) Müssen alle Kooperationspartner bzw. Drittanbieter einer Website namentlich genannt werden?

3.) Muss generell und auch pro Drittanbieter angegeben werden, welche Daten verarbeitet werden und zu welchem Zweck? Muss ein Unternehmen angeben, für wie lange Daten gespeichert werden? Sind Angaben wie für Marketingzwecke, für Werbung bzw. zur Website-Analyse ausreichend? Muss die Datenerhebung ganz genau beschrieben werden? Ist es in Ordnung, wenn nur angegeben wird, dass einige technische Daten erhoben werden?

4.) Ist es datenschutzkonform, wenn eine Website angibt, dass sie keinen Einfluss auf die Nutzung werbebezogener Cookies durch seine Vermarktungsunternehmen hat bzw. dass die Datenschutzbestimmungen des Drittanbieters gelten und der User diese heranzuziehen hat? Kann ein Unternehmen die Verantwortung des Datenschutzes auf das Drittunternehmen schieben? Siehe zum Beispiel AGBs von orf.at und krone.at: Der ORF schreibt u.a. bei Werbecookies, dass sich die externen Unternehmen beim Verarbeiten der Userdaten an österreichische bzw. europäische Datenschutzbestimmungen halten, obwohl Doubleclick und Google Analytics im Einsatz sind? Wird dem User bei solchen Angaben nicht etwas vorgetäuscht?

5.) Muss ein Websitebetreiber genau auflisten, welche Techniken eingesetzt werden, also Cookies, Drittanbieter-Cookies (muss eine Unterscheidung zw. First und Third Party Cookies gemacht werden?), Zählpixel, andere Trackingtechnologien?

6.) Dürfen über Datenschutzbestimmung/ AGBs/ Impressum/ Nutzungsbedingungen Zustimmungen der User eingeholt werden?

7.) Sind folgende Formulierungen datenschutzkonform?

- Mit der Nutzung der Website stimmen Sie den folgenden Bedingungen uneingeschränkt zu.
- Mit der Nutzung dieser Website stimmen Sie der oben beschriebenen Vorgangsweise zur Analyse der Benutzung dieser Website zu.
- Mit dem Aufruf der Website unterwirft sich der User den nachstehenden Bedingungen.
- Nachfolgend bestätigen Sie, dass sie Nutzungs... zur Kenntnis genommen haben und mit diesen einverstanden sind.
- Nutzung der Website ist an AGB gebunden, nicht registrierte User akzeptieren AGB durch Nutzung der Website.

8.) Wie sollte ein "Best Practice" für das Einholen einer Online-Zustimmung aussehen?

9.) Kommt durch das Bestätigen eines Cookie-Banners eine Zustimmung zustande? Was, wenn der User den Banner ignoriert und nicht darauf reagiert? Müsste dem User auch ein "Nicht einverstanden" angeboten werden, wenn der User dem Setzen von Cookies widersprechen möchte?

10.) Wie genau kommt eine Zustimmung zustande? Gilt das Laden einer Webseite schon als Zustimmung? Gelten Browsereinstellungen als Zustimmung? (Manche Daten werden zum Teil schon beim Laden einer Homepage erhoben, noch bevor der User die Gelegenheit hatte, AGBs zu lesen)?

11.) Ist ein User dazu verpflichtet AGBs/ Nutzungsbedingungen/ Datenschutzerklärungen etc. zu lesen? Muss eine Website den User dazu auffordern bzw. darauf hinweisen diese Unterlagen zu lesen? Bei einer Registrierung ist das der Fall, wie ist es ohne Registrierung?

**Fragen zu den untersuchten Webseiten:**

Auf der Homepage von kurier.at wird auf der rechten Seite ein großer Werbebanner geladen. Im Hauptteil werden im Bereich "Special" bezahlte Artikel neben tatsächlichen Kurier-Beiträgen angezeigt. Diese sind mit "POWERED BY CONTENT GARDEN" gekennzeichnet. Content Garden ist ein Dienstleister, der sich auf die Verbreitung digitaler Inhalte und Content Marketing spezialisiert hat. Bei aktivem Ghostery oder Disconnect wird dieser Artikel nicht angezeigt. Klickt man den Artikel an, wird eine Unterseite geladen, die sich kaum vom Aussehen echter Kurier-Nachrichtenartikel unterscheidet. Lediglich das "powered by Content Garden" zu Beginn des Beitrags deutet auf einen externen Inhalt hin. Weiters kann der bezahlte Artikel nicht via soziale Netzwerke geteilt werden, die Buttons fehlen. Ein weiterer Artikel mit dem Untertitel "LESESTOFF" ist eine Kooperation mit Morawa und präsentiert neue Bucherscheinungen.

**FRAGE:** Muss "LESESTOFF" als Werbung gekennzeichnet werden? Muss die Artikel-seite von "POWERED BY CONTENT GARDEN" als Werbung gekennzeichnet werden?

Bei den Nutzungsbedingungen von willhaben.at ist kein Datum angegeben und der User weiß nicht, wie aktuell diese Daten sind. Willhaben.at gibt darin unter anderem an, Website-Analyse-Software zu verwenden, dass Third-Party-Cookies von Kooperationspartnern gespeichert und Daten ausgewertet werden und wie das Verhalten von Cookies anhand des Browsers gesteuert werden kann. In den AGBs wird in Absatz 3.1 erklärt, dass der Benutzer zustimmt, dass alle User-Daten einerseits von willhaben.at gespeichert und verarbeitet und andererseits an Dritte weitergegeben werden.

**FRAGE:** Darf willhaben.at User-Daten an Dritte weitergeben. Ist die Art der Zustimmung gültig?

In den AGBs von herold.at wird mehrmals wiederholt, dass man sich durch die Nutzung der Website zur beschriebenen Datenverarbeitung einverstanden erklärt. Es gibt die Option, sich über das Facebook-Konto des Users bei herold.at anzumelden. Wird diese Möglichkeit genutzt, stellt Facebook eine Vielzahl an Userdaten herold.at zur Verfügung: darunter Name, Geburtsdatum, Freundesliste, Wohnort, Ausbildung, Interessen, "Gefällt mir"-Angaben. Laut den AGB von herold.at erklärt sich der User damit einverstanden, dass seine Facebook-Daten von *"HEROLD zu eigenen Werbe- und Marketingzwecken sowie zu Werbe- und Marketingzwecke von Werbekunden und Kooperationspartner von HEROLD verwendet werden"* [AGB, Abschnitt 6.4, e)].

**FRAGE:** Ist das Verwenden von Facebook-Daten datenschutzkonform?

Ein auf herold.at registrierter User kann der Verarbeitung seiner Daten widersprechen, worauf laut AGB das Kundenkonto von HEROLD gelöscht wird.

**FRAGE:** Ist die Löschung des Kundenkontos aufgrund des Widerspruchs rechtlich in Ordnung?

Das Bundesministerium für Finanzen informiert über Datenschutz mittels ihres Impressums: *”Um unser Informationsangebot zu verbessern wird Ihr Besuch in unserer Statistik festgehalten. Sämtliche Daten werden anonymisiert gespeichert”*.

**FRAGE:** Muss das eingesetzte Analysetool namentlich genannt werden?

Das Bundesministerium für Finanzen hat das geringste Cookie-Aufkommen, beim Laden der Homepage werden drei First-Party-Cookies und keine Third-Party-Cookies gesetzt. Ein Tracker, ”PiWiK Analytics”, ist aktiv, dieser wird für Website-Analysen eingesetzt. Dem Besucher wird dafür keine Opt-Out-Option geboten, jedoch werden laut den Datenschutzbestimmungen des BMFs nur anonymisierte Daten gespeichert. Welche Benutzerdaten im Detail verarbeitet und wie deren Anonymisierung stattfindet, wird nicht angegeben.

**FRAGE:** Muss das BMF ein Opt Out anbieten und den Vorgang der Datenverarbeitung und der Anonymisierung erklären?

Standard.at und kurier.at verlangen in ihren AGBs von ihren Lesern das Deaktivieren von Werbeblockern.

**FRAGE:** Ist dieses Vorgehen rechtlich in Ordnung?

Im Footer wird zu den Unternehmensseiten von karriere.at auf YouTube, Instagram, Twitter und Facebook verlinkt. Social-Media-Buttons sind nur auf Inseratsseiten integriert, die Art und Weise ist von der jeweiligen Firma, von der das Inserat stammt, abhängig. Jede Inseratsseite scheint externe Inhalte zu laden. Darauf wird in den Datenschutzbestimmungen von karriere.at nicht hingewiesen.

**FRAGE:** Muss in den AGBs darauf hingewiesen werden, dass jedes Inserat unterschiedliche Social Media Buttons lädt bzw. pro Inseratsseite andere Datenschutzbestimmungen gelten?

---

In der Datenschutzerklärung von karriere.at beschreibt ein eigener Absatz "Interensbasierte Werbeschaltung durch Retargeting", wie auf karriere.at hinterlegte Third-Party-Cookies auf externen Websites dazu verwendet werden, um Werbeanzeigen aufbauend auf dem Besuch von karriere.at zu schalten. Dafür werden zwei Opt-Out-Möglichkeiten geboten: Das Deaktivieren der Google Anzeigeeinstellungen und durch das Blockieren der Mitglieder der Network Advertising Initiative (NAI). Es ist davon auszugehen, dass nicht alle Dienstleister, die mit karriere.at zusammenarbeiten, auch Mitglieder der NAI sind.

**FRAGE:** Ist Retargeting datenschutzkonform, da es eigentlich eine Datenweitergabe an Dritte darstellt?

## Literaturverzeichnis

- [Acar et al. 2013] Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens und Bart Preneel - FPDetective: Dusting the Web for Fingerprinters. . Technical report, Kooperation der KU Leuven, IIIA-CSIC und New York University, veröffentlicht im Rahmen der CCS'13, USA, November 2013. Online verfügbar unter <https://securewww.esat.kuleuven.be/cosic/publications/article-2334.pdf>.
- [Acar et al. 2014a] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan und Claudia Diaz - The Web Never Forgets: Persistent Tracking Mechanisms in the Wild . Technical report, Kooperation der KU Leuven und Princeton University, veröffentlicht im Rahmen der CCS'14, USA, November 2014a. Online verfügbar unter [https://securehomes.esat.kuleuven.be/gacar/persistent/the\\_web\\_never\\_forgets.pdf](https://securehomes.esat.kuleuven.be/gacar/persistent/the_web_never_forgets.pdf).
- [Acar et al. 2014b] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan und Claudia Diaz - The Web Never Forgets: Persistent Tracking Mechanisms in the Wild - Results , November 2014b. <https://securehomes.esat.kuleuven.be/gacar/persistent/index.html#results>.
- [Acxiom 2016a] Acxiom - Accurately Identify Relevant Audiences for All of Your Media Campaigns , 2016a. URL <http://www.acxiom.com/data-packages/>, Zugriffsdatum: 8. Juni 2016.
- [Acxiom 2016b] Acxiom - Americans are packing up, are you cashing in? , 2016b. URL <https://d21532kvzc3714.cloudfront.net/wp-content/uploads/2016/05/AC-0431-16-Collateral-Flyer-DataGuru-Seasonal-Flyer-Summer-Season.pdf>, Zugriffsdatum: 8. Juni 2016.

- [AddThis 2014] Privacy - Privacy & Data Practices - Terms of Service , Februar 2014. URL <http://www.addthis.com/tos\#section-10>, Zugriffsdatum: 31. Jänner 2016.
- [AddThis Privacy Office 2014] Privacy - Privacy & Data Practices - What you should know , April 2014. URL <http://www.addthis.com/privacy>, Zugriffsdatum: 31. Jänner 2016.
- [AddThis Privacy Office 2016] Privacy - Privacy & Data Practices - Targeting Opt-Out , 2016. URL <http://www.addthis.com/privacy/opt-out>, Zugriffsdatum: 31. Jänner 2016.
- [Adobe Corporate Communications 2015] Adobe News - Flash, HTML5 and Open Web Standards , November 2015. URL [https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html?scid=social\\_20151201\\_55826586&adbid=671559505906282496&adbpl=tw&adbpr=63786611](https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html?scid=social_20151201_55826586&adbid=671559505906282496&adbpl=tw&adbpr=63786611), Zugriffsdatum: 15. Februar 2016.
- [Adobe Systems 2016] Hilfe zu Flash Player - Globale Speichereinstellungen , 2016. URL [http://www.macromedia.com/support/documentation/de/flashplayer/help/settings\\_manager03.html](http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html), Zugriffsdatum: 31. Jänner 2016.
- [Adobe Systems Software Ireland Ltd. 2016] Adobe Datenschutzzentrum - Safe Harbor , 2016. URL <https://www.adobe.com/at/privacy/safe-harbor.html>, Zugriffsdatum: 12. Mai. 2016.
- [AdWords 2016] Google display ads go 100% HTML5 , Februar 2016. URL <https://plus.google.com/+GoogleAds/posts/dYSJRrrgNjk>, Zugriffsdatum: 15. Februar 2016.
- [Alexa Internet, Inc. 2016a] Alexa - The Web Information Company - Top Sites by Country - Top Sites in Austria , 2016a. URL <http://www.alexa.com/topsites/countries/AT>, Zugriffsdatum: 31. Jänner 2016.
- [Alexa Internet, Inc. 2016b] Alexa Internet, Inc. - Top Sites, The top 500 sites on the web , 2016b. URL <http://www.alexa.com/topsites>, Zugriffsdatum: 31. Jänner



2016.

- [Altaweel et al. 2014] Ibrahim Altaweel, Jaime Cabrera, Hen Su Choi, Katie Ho, Nathan Good und Chris Jay Hoofnagle - Web Privacy Census: HTML5 Storage Takes the Spotlight As Flash Returns . Technical report, 2014. Online verfügbar unter [https://www.truststc.org/education/reu/14/Papers/Altaweel\\_Cabrera\\_Choi\\_Ho\\_Paper14.pdf](https://www.truststc.org/education/reu/14/Papers/Altaweel_Cabrera_Choi_Ho_Paper14.pdf).
- [Altaweel et al. 2015] Ibrahim Altaweel, Nathaniel Good und Chris Jay Hoofnagle - Web Privacy Census . Technical report, Technology Science, Dezember 2015. Online verfügbar unter [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2703814](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703814).
- [Amazon.de 2014] Amazon.de-Datenschutzerklärung , Juli 2014. URL [http://www.amazon.de/gp/help/customer/display.html/ref=footer\\_privacy?ie=UTF8&nodeId=3312401](http://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=3312401), Zugriffsdatum: 31. Jänner 2016.
- [Amy Chang 2010] Google Analytics Blog - Greater choice and transparency for Google Analytics , Mai 2010. URL <https://analytics.googleblog.com/2010/05/greater-choice-and-transparency-for.html>, Zugriffsdatum: 25. Juni. 2016.
- [Andrew Y. 2016] ScriptSafe , 2016. URL <https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbgdgdf>, Zugriffsdatum: 21. Jänner 2016.
- [Apple Inc. 2016] Safari 9 (El Capitan): Verwenden von Fenstern mit der Funktion Privates Surfen , 2016. URL [https://support.apple.com/kb/PH21413?locale=de\\_DE&viewlocale=de\\_DE](https://support.apple.com/kb/PH21413?locale=de_DE&viewlocale=de_DE), Zugriffsdatum: 25. Juni 2016.
- [Ayenson et al. 2011] Mika Ayenson, Dietrich James Wambach, Ashkan Soltani, Nathan Good und Chris Jay Hoofnagle - Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning . Technical report, Juli 2011. Online verfügbar unter <http://ssrn.com/abstract=1898390>.
- [BfDI 2016] Datenschutz-Wiki - Safe Harbor , Februar 2016. URL [https://www.bfdi.bund.de/bfdi\\_wiki/index.php/Safe\\_Harbor](https://www.bfdi.bund.de/bfdi_wiki/index.php/Safe_Harbor), Zugriffsdatum: 22. Februar. 2016.
- [BILD.de 2016] Homepage von bild.de - Warum sehe ich BILD.de nicht? ,

2016. URL <http://www.bild.de/wa/11/bild-de/unangemeldet-42925516.bild.html>, Zugriffsdatum: 25. Juni 2016.
- [BlueCava, Inc. 2011] BlueCava - where devices rule , 2011. URL <http://www.bluecava.com>, Zugriffsdatum: 27. August 2011.
- [BlueCava, Inc. 2016a] BlueCava- how it works , 2016a. URL <http://bluecava.com/how-it-works/>, Zugriffsdatum: 31. Jänner 2016.
- [BlueCava, Inc. 2016b] BlueCava Opt-out Preferences , 2016b. URL <http://bluecava.com/opt-out/>, Zugriffsdatum: 31. Jänner 2016.
- [Bujlow et al. 2015] Tomasz Bujlow, Valentín Carela-Español, Josep Solé-Pareta und Pere Barlet-Ros - Web Tracking: Mechanisms, Implications, and Defenses . Technical report, Broadband Communications Research Group, Department of Computer Architecture, Universitat Politècnica de Catalunya, Barcelona, Spanien, Juli 2015. Online verfügbar unter <http://arxiv.org/pdf/1507.07872v1.pdf>.
- [Bundeskanzleramt Österreich 1978] Datenschutzgesetz (DSG), BGBl. Nr. 565/1978 , 1978. URL [https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978\\_565\\_0/1978\\_565\\_0.pdf](https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf), Zugriffsdatum: 31. Jänner. 2016.
- [Bundeskanzleramt Österreich 2015a] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) , November 2015a. URL <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>, Zugriffsdatum: 31. Jänner. 2016.
- [Bundeskanzleramt Österreich 2015b] E-Commerce-Gesetz (ECG), BGBl. I Nr. 152/2001 , Februar 2015b. URL <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703>, Zugriffsdatum: 31. Jänner. 2016.
- [Bundeskanzleramt Österreich 2015c] Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003 , November 2015c. URL <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849>, Zugriffsdatum: 31. Jänner. 2016.

- [Bundeskanzleramt Österreich 2015d] Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV) StF: BGBl. II Nr. 521/1999 , 2015d. URL <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000312>, Zugriffsdatum: 31. Jänner. 2016.
- [Bundeskanzleramt Österreich 2016] Fachinhalte Datenschutz , 2016. URL <https://www.bka.gv.at/site/3462/default.aspx>, Zugriffsdatum: 31. Jänner. 2016.
- [Chaos Computer Club Wien 2016] Chaos macht Schule' , 2016. URL <https://c3w.at/schule/>, Zugriffsdatum: 25. Juni 2016.
- [Charley Heuertz] Doris Gansterer, dorisgansterer@gmx.at (2016): Cookies [E-Mail E-Mail an den EUR-Lex Helpdesk, eurlex@publications.europa.eu, Amt für Veröffentlichungen der Europäischen Union (16. März 2016) .
- [Christian Stöcker 2016] Spiegel Online - Einfluss auf die Gesellschaft: Radikal dank Facebook , Jänner 2016. URL <http://www.spiegel.de/netzwelt/netzpolitik/filterblase-radikalisierung-auf-facebook-a-1073450.html>, Zugriffsdatum: 8. Juni 2016.
- [Claudia Glechner, ORF.at 2011] Ministerrat beschließt lang erwartete TKG-Novelle , August 2011. URL <http://help.orf.at/stories/1687297/>, Zugriffsdatum: 31. Jänner. 2016.
- [Clausen Lars R. 2004] Concerning Etags and Datestamps . Technical report, The State and University Library, Denmark, 2004. Online verfügbar unter <http://iwaw.europarchive.org/04/Clausen.pdf>.
- [compvid30 2016] ScriptBlock , 2016. URL <https://chrome.google.com/webstore/detail/scriptblock/hcdjknjpbnhdoabngpmfekaecnpajba>, Zugriffsdatum: 21. Jänner 2016.
- [Constanze Kurz und Frank Rieger 2011] Constanze Kurz und Frank Rieger . *Die Datenfresser - Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*. Frankfurt am Main: S.

- Fischer Verlag GmbH, 2011.
- [Content Garden 2016] Content Garden - Über Uns - Das Team , 2016. URL <http://www.content-garden.com/about/>, Zugriffsdatum: 11. März 2016.
- [Content Garden 2016] Mehr Flair im Bad mit Dusch-WCs , 2016. URL <http://kurier.at/contented/4223832>, Zugriffsdatum: 16. März 2016.
- [Dana Mattioli 2012] Wall Street Journal - On Orbitz, Mac Users Steered to Pricier Hotels , August 2012. URL <http://www.wsj.com/articles/SB10001424052702304458604577488822667325882>, Zugriffsdatum: 28. Mai 2016.
- [Daniel Baulig 2015] Why we chose to move to HTML5 video , Dezember 2015. URL <https://code.facebook.com/posts/159906447698921>, Zugriffsdatum: 15. Februar 2016.
- [Daniel Berger 2014] heise online - Social-Media-Buttons datenschutzkonform nutzen , November 2014. URL <http://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html>, Zugriffsdatum: 31. Jänner 2016.
- [davec 2016] Flashcontrol , 2016. URL <https://chrome.google.com/webstore/detail/flashcontrol/mfidmkgfnfngkihnjeklbekckimkipmoe?hl=de>, Zugriffsdatum: 19. Jänner 2016.
- [David Baron 2010] Preventing attacks on a user's history through CSS :visited selectors , März 2010. URL <http://dbaron.org/mozilla/visited-privacy>, Zugriffsdatum: 31. Jänner 2016.
- [derstandard.at 2015] derstandard.at - Netzpolitik - Big Brother Awards gehen an Mikl-Leitner und Facebook , Oktober 2015. URL <http://derstandard.at/2000024499523/Big-Brother-Awards-gehen-an-Mikl-Leitner-und-Facebook>, Zugriffsdatum: 8. Juni 2016.
- [derstandard.at GmbH 2011a] derstandard.at - Impressum , 2011a. URL

- <http://derstandard.at/2004778/derstandardat---Impressum>, Zugriffsdatum: 27. September 2011.
- [derstandard.at GmbH 2011b] derstandard.at - Web - Innovationen - Social Media , 2011b. URL <http://derstandard.at/r1253807948086/Social-Media>, Zugriffsdatum: 27. September 2011.
- [derstandard.at Redaktion 2008] derstandard.at - Web - IT Business - UK-Provider wollen Stück vom Online-Werbekuchen , Februar 2008. URL <http://derstandard.at/3229897>, Zugriffsdatum: 04. Mai 2012.
- [Die Presse, Oliver Grimm 2009] DiePresse.com - Politik - Europa - Werben, spionieren und der Datenschutz in der EU - Der Fall Phorm , April 2009. URL <http://diepresse.com/home/politik/eu/470484/Werben-spionieren-und-der-Datenschutz-in-der-EU?from=suche.intern.portal>, Zugriffsdatum: 04. Mai 2012.
- [Digital Advertising Alliance] Digital Advertising Alliance Consumer Choice Page . URL <http://www.aboutads.info/choices/>.
- [Digital Advertising Alliance 2010] Homepage des Self-Regulatory Program for Online Behavioral Advertising , 2010. URL <http://www.aboutads.info/>, Zugriffsdatum: 31. Jänner 2016.
- [Digitalcourage e.V. 2016] Verbraucherschutz: die General Versicherung - Big-BrotherAwards , APRIL 2016. URL <http://bigbrotherawards.de/2016/verbraucherschutz-generali-versicherung>, Zugriffsdatum: 8. Juni 2016.
- [Disconnect 2016a] FAQ - Desktop Browser Extensions - Private Browsing , 2016a. URL <https://disconnect.me/help#private-browsing>, Zugriffsdatum: 26. Jänner 2016.
- [Disconnect 2016b] Visuelle Tracker Darstellung des Kronen Zeitung Artikels - Gegen Wahlbeobachter, Kern: 'Es geht jetzt um den Ruf unseres Landes!' mittels Disconnect , 2016b. URL [http://www.krone.at/Oesterreich/Kern\\_Es\\_geht\\_jetzt\\_um\\_den\\_Ruf\\_unseres\\_Landes!-Gegen\\_Wahlbeobachter-Story-518034](http://www.krone.at/Oesterreich/Kern_Es_geht_jetzt_um_den_Ruf_unseres_Landes!-Gegen_Wahlbeobachter-Story-518034),

Zugriffsdatum: 2. Juli 2016.

[dpa 2011a] Datenschützer erhöht Druck gegen Like-Button , Oktober 2011a. URL <http://futurezone.at/netzpolitik/5287-datenschuetzer-erhoeht-druck-gegen-like-button.php>, Zugriffsdatum: 14. Oktober 2011.

[dpa 2011b] Datenschützer erhöht Druck gegen Like-Button , Oktober 2011b. URL <http://futurezone.at/netzpolitik/5287-datenschuetzer-erhoeht-druck-gegen-like-button.php>, Zugriffsdatum: 31. Jänner 2016.

[dr34polw 2016] NoFlash-Erweiterung - Opera Add-ons , 2016. URL <https://addons.opera.com/de/extensions/details/noflash/?display=en>, Zugriffsdatum: 19. Jänner 2016.

[Eckersley Peter 2010] How unique is your web browser? . Technical report, Electronic Frontier Foundation, Mai 2010. Online verfügbar unter <https://panopticklick.eff.org/static/browser-uniqueness.pdf>.

[EHI Retail Institute GmbH 2016a] Euro-Label - safe web shopping , 2016a. URL <http://www.euro-label.com/>, Zugriffsdatum: 31. Jänner. 2016.

[EHI Retail Institute GmbH 2016b] Zertifikat Euro-Label - Wiener Linien GmbH & Co KG , 2016b. URL <http://www.euro-label.com/zertifizierte-shops/zertifikat/index.html?memberkey=WK0&shopurl=shop.wienerlinien.at>, Zugriffsdatum: 31. Jänner. 2016.

[Electronic Frontier Foundation 2015] Panopticklick - Is your browser safe against tracking? - About Panopticklick , 2015. URL <https://panopticklick.eff.org/about>, Zugriffsdatum: 31. Jänner 2016.

[Electronic Frontier Foundation 2016] Privacy Badger , 2016. URL <https://www.eff.org/privacybadger>, Zugriffsdatum: 25. Jänner 2016.

[Eli Pariser 2011] Eli Pariser . *The Filter Bubble - What the Internet Is Hiding from*

*You*. Großbritannien: Penguin Group, 2011.

[Emmy Huang 2011] Adobe Flash Platform Blog - On Improving Privacy: Managing Local Storage in Flash Player , Jänner 2011. URL <https://blogs.adobe.com/digitalmedia/2011/01/on-improving-privacy-managing-local-storage-in-flash-player/>, Zugriffsdatum: 31. Jänner 2016.

[Englehardt et al. 2016] Steven Englehardt und Arvind Narayanan - Online tracking: A 1-million-site measurement and analysis . Technical report, Princeton University, Teil des WebTAP Projekts, USA, Mai 2016. Online verfügbar unter [http://randomwalker.info/publications/OpenWPM.1\\_million\\_site\\_tracking\\_measurement.pdf](http://randomwalker.info/publications/OpenWPM.1_million_site_tracking_measurement.pdf).

[EPIC 2005] Electronic Privacy Information Center, Local Shared Objects - Flash Cookies , 2005. URL <http://epic.org/privacy/cookies/flash.html>, Zugriffsdatum: 23. August 2011.

[European Advertising Standards Alliance 2011] New standards for Online Behavioural Advertising , April 2011. URL <http://www.easa-alliance.org/page.aspx/386>, Zugriffsdatum: 31. Jänner 2016.

[EuroPriSe] EuroPriSe - European Privacy Seal . URL <https://www.european-privacy-seal.eu/>, Zugriffsdatum: 31. Jänner 2016.

[Europäische Kommission 2015a] Entscheidungen der Kommission zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten , Dezember 2015a. URL [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm), Zugriffsdatum: 31. Jänner. 2016.

[Europäische Kommission 2015b] Europäische Kommission - Pressemitteilung - Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen , Dezember 2015b. URL [http://europa.eu/rapid/press-release\\_IP-15-6321\\_de.htm](http://europa.eu/rapid/press-release_IP-15-6321_de.htm), Zugriffsdatum: 31. Jänner. 2016.

[Europäische Kommission 2016] Reform of EU data protection rules , Mai 2016. URL [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm), Zu-

griffsdatum: 11. Mai. 2016.

[Europäische Union 1995-2012] Europa - Zusammenfassung der EU-Gesetzgebung - Datenschutz, Urheberrecht und verwandte Schutzrechte , 1995-2012. URL [http://europa.eu/legislation\\_summaries/information\\_society/data\\_protection/index\\_de.htm](http://europa.eu/legislation_summaries/information_society/data_protection/index_de.htm), Zugriffsdatum: 13. Oktober. 2012.

[Europäische Union 2016] Cookies - EUR-Lex , 2016. URL <http://eur-lex.europa.eu/content/cookies/cookies-notice.html>, Zugriffsdatum: 31. Jänner. 2016.

[Europäisches Parlament, Rat der Europäischen Union 2002] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) , Juli 2002. URL <http://eur-lex.europa.eu/legal-content/DE/TXT/\?uri=CELEX:32002L0058>, Zugriffsdatum: 31. Jänner. 2016.

[Europäisches Parlament und Rat der Europäischen Union 2016] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES , Mai 2016. URL <http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE>, Zugriffsdatum: 11. Mai. 2016.

[Export.gov 2016] Export.gov - Helping U.S. Companies Export - Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks (Übersicht über das Safe Harbor-Abkommen durch das amerikanische Handelsministerium) , Februar 2016. URL <https://build.export.gov/main/safeharbor/index.asp>, Zugriffsdatum: 22. Februar. 2016.

[Fabian Schmid 2015] derstandard.at - Wenn der Vorname über die Kreditwürdigkeit entscheidet , August 2015. URL <http://derstandard.at/2000019676871/Bonitaet-Wenn-der-Vorname-ueber-die-Kreditwuerdigkeit-entscheidet>, Zugriffsdatum: 8. Juni 2016.

[Facebook 2013] Facebook - Partner Categories, a New Self-Serve Targeting Feature , April 2013. URL <https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature>, Zugriffsdatum: 8. Juni 2016.



- [Facebook 2015a] Facebook - Datenrichtlinie , Jänner 2015a. URL <https://www.facebook.com/privacy/explanation>, Zugriffsdatum: 31. Jänner 2016.
- [Facebook 2015b] Hilfebereich - Privatsphäre - Cookies, Pixel & ähnliche Technologien , Jänner 2015b. URL <https://www.facebook.com/help/cookies/?ref=sitefooter>, Zugriffsdatum: 31. Jänner 2016.
- [Facebook 2016] Facebook - Registrieren , 2016. URL <http://www.facebook.com/>, Zugriffsdatum: 31. Jänner 2016.
- [Federal Trade Commission 2007] FTC Staff Proposes Online Behavioral Advertising Privacy Principles , Dezember 2007. URL <http://www.ftc.gov/opa/2007/12/principles.shtml>, Zugriffsdatum: 31. Jänner 2016.
- [Fitbit, Inc. 2016] Fitbit - Lösungen von Fitbit für Gesundheit im Unternehmen , 2016. URL <https://www.fitbit.com/de/product/corporate-solutions>, Zugriffsdatum: 8. Juni 2016.
- [Futurezone GmbH ] Futurezone GmbH .
- [Futurezone GmbH] Allgemeine Geschäftsbedingungen (AGB) des Portals FUTUREZONE.at . URL <https://community.futurezone.at/agb.php>, Zugriffsdatum: 31. Jänner 2016.
- [Gabriel Weinberg 2012] DuckDuckGo-Datenschutz , April 2012. URL <https://duckduckgo.com/privacy>, Zugriffsdatum: 15. Jänner 2016.
- [Gaudet Dean 2003] tracking without cookies , Februar 2003. URL <http://www.arctic.org/~dean/tracking-without-cookies.html>, Zugriffsdatum: 31. Jänner 2016.
- [Ghostery, Inc. 2016a] About Ghostery , 2016a. URL <https://www.ghostery.com/about-us/about-ghostery/>, Zugriffsdatum: 25. Juni 2016.
- [Ghostery, Inc. 2016b] Company Database , 2016b. URL <https://www.ghostery.com/support/database/>, Zugriffsdatum: 22. Jänner 2016.

- [Ghostery, Inc. 2016c] Ghostery Browser Extension , 2016c. URL <https://www.ghostery.com/our-solutions/ghostery-browser-extension/>, Zugriffsdatum: 22. Jänner 2016.
- [Gibson Research Corporation 2008a] Security Now! - Episode 149 - ISP Betrayal , Juni 2008a. URL <http://www.grc.com/sn/sn-149.pdf>, Zugriffsdatum: 04. Mai 2012.
- [Gibson Research Corporation 2008b] Security Now! - Episode 151 - Phracking Phorm , Juli 2008b. URL <https://www.grc.com/sn/sn-151.pdf>, Zugriffsdatum: 31. Jänner 2016.
- [Gibson Research Corporation 2016] GRC Visitor Browser & Cookie Demographics , 2016. URL <http://www.grc.com/cookies/stats.htm>, Zugriffsdatum: 25. Juni 2016.
- [Giorgio Maone 2016] NoScript , 2016. URL <https://addons.mozilla.org/de/firefox/addon/noscript/>, Zugriffsdatum: 21. Jänner 2016.
- [Google 2014] Datenschutzerklärung & Nutzungsbedingungen - Rahmen zur Selbstregulierung , November 2014. URL <https://www.google.at/intl/de/policies/privacy/frameworks/>, Zugriffsdatum: 12. Mai 2016.
- [Google 2015a] Datenschutzerklärung & Nutzungsbedingungen - Wichtige Begriffe - Cookies und ähnliche Technologien , August 2015a. URL <https://www.google.at/intl/de/policies/privacy/key-terms/#toc-terms-cookie>, Zugriffsdatum: 31. Jänner 2016.
- [Google 2015b] Google Datenschutzerklärung & Nutzungsbedingungen , August 2015b. URL <https://www.google.at/intl/de/policies/privacy/>, Zugriffsdatum: 31. Jänner 2016.
- [Google 2016a] Anzeigen Hilfe - Interessenbezogene Werbung deaktivieren , 2016a. URL <https://support.google.com/ads/answer/2662922?hl=de/>, Zugriffsdatum: 31. Jänner 2016.
- [Google 2016b] Chrome Hilfe - Im Inkognitomodus privat surfen , 2016b. URL <https://>

- [support.google.com/chrome/answer/7005900?rd=1](https://support.google.com/chrome/answer/7005900?rd=1), Zugriffsdatum: 25. Jänner 2016.
- [Google 2016c] Gmail-Hilfe - So funktionieren Anzeigen in Gmail , 2016c. URL <https://support.google.com/mail/answer/6603?hl=de>, Zugriffsdatum: 31. Jänner 2016.
- [Google 2016d] Google Trends Hilfe - Trends-Daten - Herkunft der Trends-Daten , 2016d. URL <https://support.google.com/trends/?hl=de#topic=>, Zugriffsdatum: 14. Mai 2016.
- [Google Analytics 2016] Google Analytics - Professionelle Webanalysen , 2016. URL [https://www.google.com/intl/de/\\_ALL/analytics/index.html](https://www.google.com/intl/de/_ALL/analytics/index.html), Zugriffsdatum: 25. Juni 2016.
- [Graham Greenleaf 2015] Global data privacy laws 2015: 109 countries, with European laws now a minority , Februar 2015. URL [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2603529](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529), Zugriffsdatum: 25. Februar. 2016.
- [Handelsverband 2016] Mit dem Trustmark Austria zertifizierte Shops , 2016. URL <https://www.handelsverband.at/trustmark-austria/zertifizierte-shops/>, Zugriffsdatum: 31. Jänner. 2016.
- [heise online, Stefan Krempl 2014] US-Handelsaufsicht straft Privatsphäre-Gütesiegelfirma TRUSTe ab , November 2014. URL <http://www.heise.de/newsticker/meldung/US-Handelsaufsicht-straft-Privatsphaere-Guetesiegelfirma-TRUSTe-ab-2459865.html>, Zugriffsdatum: 12. Mai. 2016.
- [HEROLD 2016] Allgemeine Nutzungsbedingungen für HEROLD Portale , Februar 2016. URL <http://www.herold.at/fileadmin/herold/docs/agb/agb-herold-portale.pdf>, Zugriffsdatum: 11. März 2016.
- [Heute 2016] Startseite - Heute.at , März 2016. URL <http://www.heute.at/>, Zugriffsdatum: 2. März 2016.

- [Hiten Shah 2011] Kissmetrics Blog - Official KISSmetrics Response to Data Collection Practices , 2011. URL <https://blog.kissmetrics.com/official-kissmetrics-response-to-data-collection-practices/>, Zugriffsdatum: 31. Jänner 2016.
- [IHS Automotive 2016] Dataium - About Us , 2016. URL <http://www.dataium.com/about/>, Zugriffsdatum: 28. Mai 2016.
- [Interactive Advertising Bureau] Self-Regulatory Program for Online Behavioral Advertising . URL [http://www.iab.net/public\\_policy/self-reg](http://www.iab.net/public_policy/self-reg), Zugriffsdatum: 31. Jänner 2016.
- [Interactive Advertising Bureau 2011] IAB Member Code of Conduct , April 2011. URL [http://www.iab.net/public\\_policy/codeofconduct](http://www.iab.net/public_policy/codeofconduct), Zugriffsdatum: 31. Jänner 2016.
- [Jackson et al. 2006] Collin Jackson, Dan Boneh, Andrew Bortz und John C. Mitchell - Protecting Browser State from Web Privacy Attacks . Technical report, Proceedings of the 15th ACM World Wide Web Conference, Mai 2006. Online verfügbar unter <http://crypto.stanford.edu/safecache/>.
- [Jang et al. 2010] Dongseok Jang, Ranjit Jhala, Sorin Lerner und Hovav Shacham - An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications . Technical report, Proceedings of the 17th ACM Computer and Communications Security Conference, Oktober 2010. Online verfügbar unter <http://cseweb.ucsd.edu/hovav/papers/jjls10.html>.
- [Jason Lee 2012] The Wall Street Journal - How They Know , Dezember 2012. URL <http://www.wsj.com/news/interactive/ANONYMITY1208>, Zugriffsdatum: 28. Mai 2016.
- [Jürgen Schmidt 2011] heise online - 2 Klicks für mehr Datenschutz , September 2011. URL <http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html>, Zugriffsdatum: 14. Oktober 2011.

- [Kamkar Samy 2010] Evercookie - never forget , Oktober 2010. URL <http://samy.pl/evercookie/>, Zugriffsdatum: 31. Jänner 2016.
- [Kamkar Samy 2016] GitHub - samyk/evercookie , 2016. URL <https://github.com/samyk/evercookie>, Zugriffsdatum: 31. Jänner 2016.
- [Kissmetrics Privacy Office 2014] Kissmetrics' Privacy Policy , März 2014. URL <https://www.kissmetrics.com/privacy/>, Zugriffsdatum: 31. Jänner 2016.
- [Knyrim Rainer 2003] Knyrim Rainer . *Datenschutzrecht : Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmung, Outsourcen, Werben uvm.* Wien: Manz Verlag, 2003.
- [KronenZeitung 2016] Faymann legt zu, Strache auf persönlichem Bestwert , 2016. URL <http://kurier.at/politik/ausland/bulgarien-koennte-grenze-zu-griechenland-mit-zaun-abriegeln/186.274.320>, Zugriffsdatum: 11. März 2016.
- [KURIER ] Werner Faymann: .
- [KURIER 2016] Bulgarien könnte Grenze zu Griechenland mit Zaun abriegeln , 2016. URL [http://www.krone.at/Oesterreich/Faymann\\_legt\\_zu.\\_Strache\\_auf\\_persoentlichem\\_Bestwert-Vertrauensindex-Story-500291](http://www.krone.at/Oesterreich/Faymann_legt_zu._Strache_auf_persoentlichem_Bestwert-Vertrauensindex-Story-500291), Zugriffsdatum: 11. März 2016.
- [Kurier 2016] Kurier.at-Startseite , März 2016. URL <http://kurier.at>, Zugriffsdatum: 02. März 2016.
- [KURIER 2016] Startseite - KURIER , 2016. URL <http://kurier.at/>, Zugriffsdatum: 11. März 2016.
- [LinkedIn Corp. 2016] LinkedIn Hilfe - EU-Datenübertragung und das Safe Harbor-Abkommen , März 2016. URL <https://www.linkedin.com/help/linkedin/answer/62533?lang=de>, Zugriffsdatum: 12. Mai 2016.
- [Marc Hoyois 2016] Safari Extensions Gallery - ClickToFlash , 2016. URL

- <https://extensions.apple.com/details/?id=com.hoyois.safari.clicktoflash-GY5KR7239Q>, Zugriffsdatum: 19. Jänner 2016.
- [Marshall Jack 2011a] ClickZ - Device Fingerprinting Could Be Cookie Killer , März 2011a. URL <http://www.clickz.com/clickz/news/2030243/device-fingerprinting-cookie-killer>, Zugriffsdatum: 27. August 2011.
- [Marshall Jack 2011b] ClickZ - Device Fingerprinting Raises Privacy Fears , März 2011b. URL <http://www.clickz.com/clickz/news/2035579/device-fingerprinting-raises-privacy-fears>, Zugriffsdatum: 03. September 2011.
- [Mayer Jonathan 2011a] Tracking the Trackers: AdChoice Icon , August 2011a. URL <http://cyberlaw.stanford.edu/node/6714>, Zugriffsdatum: 31. Jänner 2016.
- [Mayer Jonathan 2011b] Tracking the Trackers: Microsoft Advertising , August 2011b. URL <http://cyberlaw.stanford.edu/node/6715>, Zugriffsdatum: 10. September 2011.
- [Mayer Jonathan 2011c] Valentino-DeVries Jennifer, The Wall Street Journal - What You Can Do About the New Web Tracking Tools , August 2011c. URL <http://blogs.wsj.com/digits/2011/08/19/what-you-can-do-about-the-new-web-tracking-tools/>, Zugriffsdatum: 03. September 2011.
- [Mayer Jonathan und Narayanan Arvind 2010] Do Not Track - Universal Web Tracking Opt Out , 2010. URL <http://donottrack.us/>, Zugriffsdatum: 21. September 2011.
- [Mayer-Schönberger and Brandl2006] Viktor Mayer-Schönberger and Ernst O. Brandl. *Datenschutzgesetz: Grundsätze und europarechtliche Rahmenbedingungen; Gesetzestext mit Materialien; Datenschutz-Verordnungen und Richtlinien im Anhang*. Wien: Linde Verlag, 2006. 2., überarb. Aufl.
- [McKinley Kate 2008] Cleaning Up After Cookies . Technical report, iSEC Partners, Inc., Dezember 2008. Online verfügbar <http://www.isecpartners.com/white>

- papers/2010/7/22/cleaning-up-after-cookies.html.
- [Michael Gundlach 2016] AdBlock , 2016. URL <https://getadblock.com/>, Zugriffsdatum: 21. Jänner 2016.
- [Microsoft ] msn Österreich Homepage . URL <http://www.msn.com/de-at>, Zugriffsdatum: 1. März 2016.
- [Microsoft] Microsoft - Infos zu unseren Anzeigen . URL <http://choice.microsoft.com/de-DE/opt-out>, Zugriffsdatum: 31. Jänner 2016.
- [Microsoft 2015] Datenschutzbestimmungen von Microsoft - Cookies und ähnliche Technologien , Oktober 2015. URL <https://www.microsoft.com/de-at/privacystatement/default.aspx?Componentid=pspMainCookiesSimilarTechnologiesModule&View=Description>, Zugriffsdatum: 31. Jänner 2016.
- [Microsoft 2016] Datenschutzbestimmungen von Microsoft , Jänner 2016. URL <https://privacy.microsoft.com/de-de/privacystatement>, Zugriffsdatum: 31. Jänner 2016.
- [Microsoft Corporate Blogs 2012] Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8 , Mai 2012. URL <https://blogs.microsoft.com/on-the-issues/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8/>, Zugriffsdatum: 25. Jänner 2016.
- [Microsoft Corporate Blogs 2015] An update on Microsoft's approach to Do Not Track , April 2015. URL <https://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/>, Zugriffsdatum: 25. Jänner 2016.
- [Microsoft Corporation] Datenschutzbestimmungen für Windows Internet Explorer 8 . URL <http://windows.microsoft.com/de-de/internet-explorer/ie11-win8-privacy-statement>, Zugriffsdatum: 15. Jänner 2016.

- [Microsoft Corporation 2014] Datenschutzbestimmungen zu Windows Internet Explorer 9 , Juli 2014. URL <http://windows.microsoft.com/de-DE/internet-explorer/products/ie-9/windows-internet-explorer-9-privacy-statement>, Zugriffsdatum: 15. Jänner 2016.
- [Microsoft Corporation 2016a] Internet Explorer: Hilfe , 2016a. URL <https://support.microsoft.com/de-de/products/internet-explorer>, Zugriffsdatum: 25. Jänner 2016.
- [Microsoft Corporation 2016b] Microsoft Edge und Datenschutz: FAQ , 2016b. URL <http://windows.microsoft.com/de-de/windows-10/edge-privacy-faq>, Zugriffsdatum: 15. Jänner 2016.
- [Mike Tigas 2014] Meet the Online Tracking Device That is Virtually Impossible to Block , Juli 2014. URL <https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block>, Zugriffsdatum: 31. Jänner 2016.
- [Mowery et al. 2011] Mowery Keaton, Bogenreif Dillon, Yilek Scott und Shacham Hovav - Fingerprinting Information in JavaScript Implementations . Technical report, Proceedings of W2SP 2011, IEEE Computer Society, Mai 2011. Online verfügbar unter <http://cseweb.ucsd.edu/hovav/papers/mbys11.html>.
- [Mowery et al. 2012] Keaton Mowery und Hovav Shacham - Pixel Perfect: Fingerprinting Canvas in HTML5 . Technical report, Department of Computer Science and Engineering University of California, San Diego, USA, veröffentlicht im Rahmen der W2SP 2012, IEEE Computer Society, Mai 2012. Online verfügbar unter <http://w2spconf.com/2012/papers/w2sp12-final4.pdf>.
- [Mozilla Corporation 2016] Firefox - Gesperrte Add-ons , 2016. URL <https://addons.mozilla.org/de/firefox/blocked/>, Zugriffsdatum: 31. Jänner 2016.
- [Mozilla Firefox 2011] Firefox 4 Release Notes , März 2011. URL <http://www.mozilla.org/en-US/firefox/4.0/releasenotes/>, Zugriffsdatum: 20. September 2011.



- [Mozilla Firefox 2016a] Firefox 42.0 Release Notes , Jänner 2016a. URL <https://www.mozilla.org/en-US/firefox/42.0/releasesnotes/>, Zugriffsdatum: 14. Jänner 2016.
- [Mozilla Firefox 2016b] Firefox Hilfe - Privater Modus - Kontrolle über die von Firefox gespeicherten Daten behalten , 2016b. URL <https://support.mozilla.org/de/kb/privater-modus>, Zugriffsdatum: 25. Jänner 2016.
- [Mozilla Foundation 2016] Beliebteste Erweiterung - Add-ons für Firefox , 2016. URL <https://addons.mozilla.org/de/firefox/extensions/?sort=users>, Zugriffsdatum: 19. Jänner 2016.
- [MyBrowserAddon 2016] NoScript Suite Lite , 2016. URL <http://mybrowseraddon.com/noscript-lite.html#>, Zugriffsdatum: 21. Jänner 2016.
- [Natasha Singer 2012] New York Times - Technology - You For Sale - Mapping, and Sharing, the Consumer Genome , Juni 2012. URL <http://www.nytimes.com/2012/06/17/technology/axiom-the-quiet-giant-of-consumer-database-marketing.html>, Zugriffsdatum: 8. Juni 2016.
- [Network Advertising Initiative 2016] Understanding Online Advertising , 2016. URL <https://www.networkadvertising.org/understanding-online-advertising/>, Zugriffsdatum: 25. Juni 2016.
- [Nicholas Carr 2010] The Wall Street Journal - Tracking Is an Assault on Liberty, With Real Dangers , August 2010. URL <http://www.wsj.com/articles/SB10001424052748703748904575411682714389888>, Zugriffsdatum: 28. Mai 2016.
- [Norris David, CEO von BlueCava 2010] Angwin Julia und Valentino-DeVries Jennifer, The Wall Street Journal - Race Is On to 'Fingerprint' Phones, PCs , November 2010. URL <http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html>, Zugriffsdatum: 31. August 2011.
- [nugg.ad 2011] nugg.ad AG - predictive behavioral targeting . URL <http://www.nugg.ad>

- ad/de, Zugriffsdatum: 21. August 2011.
- [nugg.ad 2015] Allgemeine Informationen - Datenschutz . URL <https://www.nugg.ad/de/datenschutz/allgemeine-informationen.html>, Zugriffsdatum: 31. Jänner 2016.
- [OEWA] Österreichische Webanalyse (ÖWA) - Organisation . URL <http://www.oewa.at/organisation>, Zugriffsdatum: 11. März 2016.
- [Opera Software ASA 2016] Opera Hilfe - Erweiterte Einstellungen - Tabs - Private Tabs , 2016. URL <http://help.opera.com/Mac/11.50/de/tabs.html>, Zugriffsdatum: 25. Juni 2016.
- [Opsahl et al. 2013] Kurt Opsahl und Rainey Reitman - The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads , April 2013. URL <https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads/#info-flow>, Zugriffsdatum: 31. Jänner 2016.
- [Oracle 2014] Oracle and BlueKai , Februar 2014. URL <http://www.oracle.com/us/corporate/acquisitions/bluekai/index.html>, Zugriffsdatum: 31. Jänner 2016.
- [outbrain 2016] Outbrain Amplify , 2016. URL <http://www.outbrain.com/de/amplify>, Zugriffsdatum: 11. März 2016.
- [PageFair Team 2013] Acceptable Ads Soothe Google Pain , August 2013. URL <https://pagefair.com/blog/2013/acceptable-ads-soothe-google-pain/?cmp=17>, Zugriffsdatum: 25. Juni 2016.
- [Parks Associates 2014] Consumers Unaware Of Opt-Out Settings with Online Ads , Jänner 2014. URL <https://www.parksassociates.com/blog/article/pr-jan2014-online-ads>, Zugriffsdatum: 31. Jänner 2016.
- [Peissl et al. 2014] Walter Peissl, Robert Rothmann, Karo Sterbik-Lamina - Credit Scoring in Österreich . Technical report, Institut für Technikfolgen-Abschätzung der

Österreichischen Akademie der Wissenschaften in Kooperation mit der Bundesarbeitskammer, April 2014. Online verfügbar unter <http://epub.oeaw.ac.at/ita/ita-projektberichte/a66.pdf>.

[Peter Schaar 2007] Peter Schaar . *Das Ende der Privatsphäre: der Weg in die Überwachungsgesellschaft*. München: Bertelsmann Verlag, 2007.

[Peter Steiner 1993] The New Yorker - Cartoon - On the Internet, nobody knows you're a dog. , Juli 1993. URL [https://www.cartoonbank.com/search?p\\\_p\\\_id=listenersearchresults\\\_WAR\\\_searchportlet&p\\\_p\\\_lifecycle=0&p\\\_p\\\_state=normal&p\\\_p\\\_mode=view&p\\\_p\\\_col\\\_id=column-2&p\\\_p\\\_col\\\_pos=2&p\\\_p\\\_col\\\_count=3&\\\_listenersearchresults\\\_WAR\\\_searchportlet\\\_struts.portlet.action=%2Fview%2FshowDetail&\\\_listenersearchresults\\\_WAR\\\_searchportlet\\\_pageNumber=1&\\\_listenersearchresults\\\_WAR\\\_searchportlet\\\_resCount=&\\\_listenersearchresults\\\_WAR\\\_searchportlet\\\_search=TCB-22230.jpg&\\\_listenersearchresults\\\_WAR\\\_searchportlet\\\_tagId=cncartoons005912](https://www.cartoonbank.com/search?p\_p\_id=listenersearchresults\_WAR\_searchportlet&p\_p\_lifecycle=0&p\_p\_state=normal&p\_p\_mode=view&p\_p\_col\_id=column-2&p\_p\_col\_pos=2&p\_p\_col\_count=3&\_listenersearchresults\_WAR\_searchportlet\_struts.portlet.action=%2Fview%2FshowDetail&\_listenersearchresults\_WAR\_searchportlet\_pageNumber=1&\_listenersearchresults\_WAR\_searchportlet\_resCount=&\_listenersearchresults\_WAR\_searchportlet\_search=TCB-22230.jpg&\_listenersearchresults\_WAR\_searchportlet\_tagId=cncartoons005912).

[Philip Chee 2016] Flashblock , 2016. URL <https://addons.mozilla.org/de/firefox/addon/flashblock/>, Zugriffsdatum: 19. Jänner 2016.

[Phorm 2012] Phorm Service Privacy Policy , April 2012. URL <http://www.phorm.com/phorm-service-privacy-policy>, Zugriffsdatum: 04. Mai 2012.

[Phorm 2015] Phorm Privacy , Jänner 2015. URL <http://www.phorm.com/privacy/>, Zugriffsdatum: 31. Jänner 2016.

[Piwik 2016] Configure Privacy Settings in Piwik - Include a Web Analytics Opt-Out Feature on Your Site , 2016. URL <http://piwik.org/docs/privacy/#step-3-include-a-web-analytics-opt-out-feature-on-your-site-using-an-iframe>, Zugriffsdatum: 11. März 2016.

[Porter Felt et al. 2015] Adrienne Porter Felt, Emily Schechter und Ke Wang - Chrome Blog - Faster, smoother and safer videos on Chrome , Oktober 2015. URL [http://chrome.blogspot.co.at/2015\\_10\\_01\\_archive.html](http://chrome.blogspot.co.at/2015_10_01_archive.html), Zugriffsdatum: 31. Jänner 2016.

- [Projekt Leiter, Hugo Roy] Terms of Service; Didn't Read - Ratings . URL <https://tosdr.org/index.html#services>, Zugriffsdatum: 31. Jänner. 2016.
- [quintessenz 2015a] Big Brother Awards , Oktober 2015a. URL <http://www.bigbrotherawards.at>, Zugriffsdatum: 31. Jänner 2016.
- [quintessenz 2015b] Big Brother Awards - In der Kategorie 'Weltweiter Datenhunger' wurden nominiert: , Oktober 2015b. URL [http://bigbrotherawards.at/2015/global\\_3.php](http://bigbrotherawards.at/2015/global_3.php), Zugriffsdatum: 31. Jänner 2016.
- [Ramirez et al. 2014] Edith Ramirez, Julie Brill, Maureen K. Ohlhausen, Joshua D. Wright und Terrell McSweeney - Data Brokers, A Call for Transparency and Accountability . Technical report, Federal Trade Commission, USA, Mai 2014. Online verfügbar unter <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.
- [Raymond Hill 2016] uBlock Origin , 2016. URL <https://github.com/gorhill/uBlock#ublock-origin>, Zugriffsdatum: 21. Jänner 2016.
- [Red Bull Media House 2015] Cookies Policy , August 2015. URL <https://www.redbullmediahouse.com/cookies-policy>, Zugriffsdatum: 31. Jänner 2016.
- [Reddit, Inc. 2016] Reddit, Inc. Privacy Policy - International Data Transfers , Jänner 2016. URL [https://www.reddit.com/help/privacypolicy#section\\_international\\_data\\_transfers](https://www.reddit.com/help/privacypolicy#section_international_data_transfers), Zugriffsdatum: 12. Mai. 2016.
- [Rich LaBarca 2014] AddThis Blog - The Facts About Our Use of a Canvas Element in Our Recent R&D Test , Juli 2014. URL <https://www.addthis.com/blog/2014/07/23/the-facts-about-our-use-of-a-canvas-element-in-our-recent-rd-test/#.Vrc0qim78nU>, Zugriffsdatum: 31. Jänner 2016.
- [Richard Leider 2015] YouTube Engineering and Developers Blog - YouTube now defaults to HTML5 video , Jänner 2015. URL [http://youtube-eng.blogspot.de/2015/01/youtube-now-defaults-to-html5\\_27.html](http://youtube-eng.blogspot.de/2015/01/youtube-now-defaults-to-html5_27.html), Zugriffsdatum:

31. Jänner 2016.

[Roosendaal Arnold 2010] Facebook tracks and traces everyone: Like this! . Technical report, Tilburg Law School Legal Studies Research Paper Series No. 03/2011, November 2010. Online verfügbar unter <http://ssrn.com/abstract=1717563>.

[Rösner et al. 2014] Homepage von ShareMeNot entwickelt von Franziska Rösner, Tadayoshi Kohno und David Wetherall , Juli 2014. URL <http://sharemenot.cs.washington.edu/>, Zugriffsdatum: 26. Jänner 2016.

[Sascha Pallenberg 2014] Adblock Plus Zahltag - \$30 Mio. von Amazon, Ebay, Google und Yahoo , Jänner 2014. URL <http://www.mobilegeeks.de/adblock-plus-zahltag-30-mio-von-amazon-ebay-google-und-yahoo/>, Zugriffsdatum: 25. Juni 2016.

[Schneider et al. 2014] Markus Schneider, Matthias Enzmann und Martin Stopczynski - Web-Tracking-Report 2014 . Technical report, Fraunhofer Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland, Februar 2014. Online verfügbar unter [https://www.sit.fraunhofer.de/fileadmin/dokumente/studien\\_und\\_technical\\_reports/Web\\_Tracking\\_Report\\_2014.pdf](https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf)

[Scoot Morrison 2009] The Wall Street Journal - Google Searches for Staffing Answers , Mai 2009. URL <http://www.wsj.com/articles/SB124269038041932531>, Zugriffsdatum: 25. Juni 2016.

[Shore et al. 2015] Jennifer Shore und Jill Steinman, Technology Science - Did You Really Agree to That? The Evolution of Facebook's Privacy Policy , August 2015. URL <http://techscience.org/a/2015081102/>, Zugriffsdatum: 31. Jänner 2016.

[Sid Stamm 2010] Plugging the CSS History Leak , März 2010. URL <https://blog.mozilla.org/security/2010/03/31/plugging-the-css-history-leak/>, Zugriffsdatum: 31. Jänner 2016.

[Smith Richard M. 1999] The Web Bug FAQ , November 1999. URL [https://w2.eff.org/Privacy/Marketing/web\\_bug.html](https://w2.eff.org/Privacy/Marketing/web_bug.html), Zugriffsdatum: 14. September 2011.

- [Soltani Ashkan 2009] Ryan Singel, Wired - You Deleted Your Cookies? Think Again , August 2009. URL <http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/>, Zugriffsdatum: 10. September 2011.
- [Soltani Ashkan 2011] RESPAWN REDUX - Follow up to Flash Cookies and Privacy II , August 2011. URL [http://ashkansoltani.org/docs/respawn\\_redux.html](http://ashkansoltani.org/docs/respawn_redux.html), Zugriffsdatum: 10. September 2011.
- [Soltani et al. 2009] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas und Chris Jay Hoofnagle - Flash Cookies and Privacy . Technical report, Summer Undergraduate Program in Engineering Research at Berkeley, University of California, August 2009. Online verfügbar unter <http://ssrn.com/abstract=1446862>.
- [Sprenger Walter 2011] Fingerprintr - Identifying Users with Browser Fingerprinting , Mai 2011. URL [http://media.hacking-lab.com/scs3/scs3\\_pdf/SCS3\\_2011\\_Sprenger.pdf](http://media.hacking-lab.com/scs3/scs3_pdf/SCS3_2011_Sprenger.pdf), Zugriffsdatum: 31. Jänner 2016.
- [StatCounter 2015a] StatCounter Global Stats - Top 5 Browsers in Austria in 2015 , 2015a. URL <http://gs.statcounter.com/#desktop-browser-AT-monthly-201501-201512-bar>, Zugriffsdatum: 15. Jänner 2016.
- [StatCounter 2015b] StatCounter Global Stats - Top 5 Desktop Search Engines in Austria in 2015 , 2015b. URL [http://gs.statcounter.com/#desktop-search\\_engine-AT-monthly-201501-201512-bar](http://gs.statcounter.com/#desktop-search_engine-AT-monthly-201501-201512-bar), Zugriffsdatum: 15. Jänner 2016.
- [StatCounter 2015c] StatCounter Global Stats - Top 5 Desktop Search Engines worldwide in 2015 , 2015c. URL [http://gs.statcounter.com/#desktop-search\\_engine-ww-monthly-201501-201512-bar](http://gs.statcounter.com/#desktop-search_engine-ww-monthly-201501-201512-bar), Zugriffsdatum: 15. Jänner 2016.
- [StatCounter 2016] StatCounter Global Stats - Top 5 Desktop Browsers in Austria from Aug 2015 to Jan 2016 , 2016. URL <http://gs.statcounter.com/#desktop-browser-AT-monthly-201508-201601-bar>, Zugriffsdatum: 15. Jänner 2016.
- [Surfboard Holding B.V.a] DATENSCHUTZ - Wir schützen Sie , a. URL <https://www.>

- startpage.com/deu/protect-privacy.html?hmb=1, Zugriffsdatum: 18. Jänner 2016.
- [Surfboard Holding B.V.b] DATENSCHUTZ - Wir schützen Sie , b. URL <https://www.ixquick.com/deu/protect-privacy.html?hmb=1>, Zugriffsdatum: 18. Jänner 2016.
- [Tanzina Vega 2010] The New York Times - New Web Code Draws Concern Over Privacy Risks , Oktober 2010. URL [http://www.nytimes.com/2010/10/11/business/media/11privacy.html?\\_r=1&hp](http://www.nytimes.com/2010/10/11/business/media/11privacy.html?_r=1&hp), Zugriffsdatum: 24. August 2011.
- [Tatjana Rauth 2011] derstandard.at - Google über sinnvolle Personalisierung und freie Wahl , August 2011. URL <http://derstandard.at/1313025276833/Aktion-Filter-Bubbles-Google-ueber-sinnvolle-Personalisierung-und-freie-Wahl>, Zugriffsdatum: 8. Juni 2016.
- [The Wall Street Journal 2010] The Tracking Ecosystem , 2010. URL <http://graphicsweb.wsj.com/documents/divSlider/ecosystems100730.html>, Zugriffsdatum: 10. September 2011.
- [The Wall Street Journal 2010 - 2012] The Wall Street Journal - What they know , 2010 - 2012. URL <http://www.wsj.com/public/page/what-they-know-2010.html>, Zugriffsdatum: 31. Jänner 2016.
- [Tom Simonite 2013] MIT Technology Review - A Popular Ad Blocker Also Helps the Ad Industry , Juni 2013. URL <https://www.technologyreview.com/s/516156/a-popular-ad-blocker-also-helps-the-ad-industry/>, Zugriffsdatum: 25. Juni 2016.
- [Torsten Klein 2015] Acceptable Ads: Auch Adblock lässt 'nicht-nervende' Werbung durch , Oktober 2015. URL <http://www.heise.de/newsticker/meldung/Acceptable-Ads-Auch-Adblock-laesst-nicht-nervende-Werbung-durch-2836888.html>, Zugriffsdatum: 21. Jänner 2016.
- [Torsten Klein 2016] Werblocker: Eyeo gewinnt vor Gericht gegen Süddeutsche Zeitung , März 2016. URL <http://www.heise.de/newsticker/meldung/>

- Werbeblocker-Eyeo-gewinnt-vor-Gericht-gegen-Sueddeutsche-Zeitung-3157096.html, Zugriffsdatum: 25. Juni 2016.
- [TRUSTe] TRUSTe . URL <http://www.truste.com>, Zugriffsdatum: 25. September 2011.
- [TRUSTe 2016] TRUSTe-Zertifizierung von Zynga , Februar 2016. URL <https://privacy.truste.com/privacy-seal/Zynga/validation?rid=e081f453-268e-40e4-8141-c9ce06c94824>, Zugriffsdatum: 28. Februar 2016.
- [ULD 2010] Kunden-Scoring - Wie bewertet mich die Wirtschaft? . Technical report, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Mai 2010. Online verfügbar unter <https://www.datenschutzzentrum.de/uploads/blauereihe/blauereihe-scoring.pdf>.
- [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2008] Datenschützer prüfen Google Analytics , Juli 2008. URL <https://www.datenschutzzentrum.de/artikel/580-.html>, Zugriffsdatum: 25. Juni. 2016.
- [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2009] Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics , Jänner 2009. URL [https://www.datenschutzzentrum.de/uploads/it/20090123\\\_GA\\\_stellungnahme.pdf](https://www.datenschutzzentrum.de/uploads/it/20090123\_GA\_stellungnahme.pdf), Zugriffsdatum: 25. Juni. 2016.
- [Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein 2011] Hinweise und Empfehlungen zur Analyse von Internet-Angeboten mit Piwik , März 2011. URL <https://www.datenschutzzentrum.de/uploads/projekte/verbraucherdatenschutz/20110315-webanalyse-piwik.pdf>, Zugriffsdatum: 25. Juni. 2016.
- [UNIQA 2016a] UNIQA - SafeLine - das Notfall-Servicepaket - die erste Autoversicherung, die Leben retten kann , 2016a. URL [https://www.uniqa.at/versicherung/cms/privatkunden/kfz/safeline\\\_notfallservice/SafeLine\\\_-\\\_Notfallservice.de.html](https://www.uniqa.at/versicherung/cms/privatkunden/kfz/safeline\_notfallservice/SafeLine\_-\_Notfallservice.de.html), Zugriffsdatum: 8. Juni 2016.
- [UNIQA 2016b] UNIQA - VitalPlan und VitalPlan PLUS. Die Vorsorge- und Fitnesspa-



- kete , 2016b. URL <https://www.uniqe.at/versicherung/cms/privatkunden/gesundheit/VitalPlan.de.html>, Zugriffsdatum: 8. Juni 2016.
- [unwatched.org , sac 2009] unwatched.org - Das Datenschutzportal - Britische ISPs geben Phorm auf , Juli 2009. URL <http://www.unwatched.org/node/1462>, Zugriffsdatum: 04. Mai 2012.
- [UPC Austria Services GmbH 2014] Allgemeine Geschäftsbedingungen , Juni 2014. URL [http://www.upc.at/pdf/agb/allgemein/AGB\\_KABEL.pdf](http://www.upc.at/pdf/agb/allgemein/AGB_KABEL.pdf), Zugriffsdatum: 31. Jänner 2016.
- [UPIAN 2015] ALLGEMEINE GESCHÄFTSBEDINGUNGEN DER WEBSITE 'DO NOT TRACK' , 2015. URL <https://donottrack-doc.com/de/cgu/>, Zugriffsdatum: 25. Juni 2016.
- [Valentino-DeVries et al. 2012] Jennifer Valentino-DeVries, Jeremy Singer-Vine und Ashkan Soltani, The Wall Street Journal - They Know What You're Shopping For , Dezember 2012. URL <http://www.wsj.com/articles/SB10001424127887324784404578143144132736214>, Zugriffsdatum: 28. Mai 2016.
- [Valentino-DeVries Jennifer 2010] The Wall Street Journal - 'Evercookies' and 'Fingerprinting': Are Anti-Fraud Tools Good for Ads? , Dezember 2010. URL <http://blogs.wsj.com/digits/2010/12/01/evercookies-and-fingerprinting-finding-fraudsters-tracking-consumers/>, Zugriffsdatum: 31. August 2011.
- [Verbraucher sicher online 2011] Cookies - Einführung Teil 1 und Teil 2 , 2011. URL <http://www.verbraucher-sicher-online.de/thema/cookies>, Zugriffsdatum: 22. August 2011.
- [Verein zur Förderung der kundenfreundlichen Nutzung des Internet 2016] Österreichisches E-Commerce-Gütesiegel - Seriöse Onlineshops sofort erkennen! , 2016. URL <https://www.guetezeichen.at/zertifizierte-shops/guetezeichen/>, Zugriffsdatum: 31. Jänner. 2016.
- [W3C 2014] Web storage - User privacy , Oktober 2014. URL <https://www.w3.org/>

- TR/html5/, Zugriffsdatum: 31. Jänner 2016.
- [W3C 2016] W3C Tracking Protection Working Group , 2016. URL <https://www.w3.org/2011/tracking-protection/>, Zugriffsdatum: 25. Juni 2016.
- [W3Techs 2016a] Technologies - Usage of server locations for websites , Februar 2016a. URL [http://w3techs.com/technologies/overview/server\\_location/all](http://w3techs.com/technologies/overview/server_location/all), Zugriffsdatum: 25. Februar. 2016.
- [W3Techs 2016b] Usage of traffic analysis tools for websites , 2016b. URL [http://w3techs.com/technologies/overview/traffic\\_analysis/all](http://w3techs.com/technologies/overview/traffic_analysis/all), Zugriffsdatum: 25. Juni. 2016.
- [Wiener Linien 2016] Wiener Linien - Tickets online kaufen , 2016. URL <http://shop.wienerlinien.at/>, Zugriffsdatum: 31. Jänner. 2016.
- [willhaben 2016] Startseite von willhaben.at , 2016. URL <https://www.willhaben.at>, Zugriffsdatum: 25. Juni 2016.
- [Wladimir Palant 2016a] Adblock Plus , 2016a. URL <https://adblockplus.org/>, Zugriffsdatum: 19. Jänner 2016.
- [Wladimir Palant 2016b] Akzeptable Werbung in Adblock Plus zulassen , 2016b. URL <https://adblockplus.org/de/acceptable-ads>, Zugriffsdatum: 19. Jänner 2016.
- [Wolfie Christl 2014] Studie im Auftrag der österreichischen Bundesarbeitskammer - Kommerzielle Digitale Überwachung im Alltag . Technical report, Cracked Labs - Institut für Kritische Digitale Kultur, November 2014. Online verfügbar unter [http://crackedlabs.org/dl/Studie\\_Digitale\\_Ueberwachung.pdf](http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf).
- [Wondracek et al. 2010] Gilbert Wondracek, Thorsten Holz, Engin Kirda und Christopher Kruegel - A Practical Attack to De-Anonymize Social Network Users . Technical report, IEEE Symposium on Security and Privacy, Mai 2010. Online verfügbar unter <http://seclab.nu/static/publications/ssp2010osn.pdf>.

- [World Legal Information Institute 2016] International Privacy Law Library , Februar 2016. URL <http://www.worldlii.org/int/special/privacy/>, Zugriffsdatum: 25. Februar. 2016.
- [Xu Jimson und Nguyen Tom 2010] Adobe Flash Player Developer Center - Private browsing in Flash Player 10.1 , Juni 2010. URL [http://www.adobe.com/devnet/flashplayer/articles/privacy\\_mode\\_fp10\\_1.html](http://www.adobe.com/devnet/flashplayer/articles/privacy_mode_fp10_1.html), Zugriffsdatum: 24. August 2011.
- [Yahoo 2015] Yahoo Privacy Center , November 2015. URL <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>, Zugriffsdatum: 12. Mai. 2016.
- [Yahoo 2016] Datenschutzcenter - Drittanbieter auf Yahoo , 2016. URL <https://policies.yahoo.com/ie/de/yahoo/privacy/topics/thirdparties/index.htm>, Zugriffsdatum: 31. Jänner 2016.
- [Your Online Choices 2016] Your Online Choices , 2016. URL <http://www.youronlinechoices.com/at>, Zugriffsdatum: 31. Jänner 2016.
- [Zynga, Inc. 2016] Zynga Homepage , Februar 2016. URL <https://www.zynga.com/>, Zugriffsdatum: 28. Februar 2016.
- [Österreichische Datenschutzbehörde] Gesetze zum Datenschutzrecht . URL <http://www.dsb.gv.at/site/6200/default.aspx>, Zugriffsdatum: 31. Jänner. 2016.
- [Österreichisches Institut für angewandte Telekommunikation 2015] Studie im Auftrag der Kammer für Arbeiter und Angestellte für Wien - Dynamic Pricing - Die Individualisierung von Preisen im E-Commerce . Technical report, Österreichisches Institut für angewandte Telekommunikation, November 2015. Online verfügbar unter [https://media.arbeiterkammer.at/wien/PDF/studien/Dynamic\\_Pricing\\_2015.pdf](https://media.arbeiterkammer.at/wien/PDF/studien/Dynamic_Pricing_2015.pdf).