WHITEPAPER BVDW

Warum „Advertising Identity“ die zukünftige Antwort für zielgerichtete Auslieferung von Werbung ist
Why "Advertising Identity" is the future answer for targeted advertising delivery

1 Warum sich alle Unternehmen mit Advertising Identities beschäftigen sollten
1 Why all companies should deal with Advertising Identities

Vor mittlerweile 25 Jahren führte Netscape das HTTP Cookie als Möglichkeit ein, Daten dauerhaft für den Browser und letztendlich auch zum Vorteil des Benutzers so abzuspeichern, dass diese auch nach einem Neustart des Browsers genutzt werden konnten. In mehr als zwei Dekaden entwickelten die Adtech-Anbieter auf Basis dieses einfachen Konzepts die Grundlagen für Tracking, Targeting und Frequency-Capping. Kurz gesagt bildet das HTTP Cookie die technische Grundlage für ein funktionsfähiges Ökosystem im Bereich des freien Internets – es ist der gemeinsame Standard für alle Marktteilnehmer.

Meanwhile 25 years ago Netscape introduced the HTTP cookie as a possibility to store data permanently for the browser and ultimately also for the benefit of the user in such a way that it could be used even after a restart of the browser. In more than two decades, adtech providers developed the basics for tracking, targeting and frequency capping based on this simple concept. In short, the HTTP cookie forms the technical basis for a functioning ecosystem in the free Internet sector - it is the common standard for all market participants.

Die Zeiten haben sich jedoch geändert. 52 %[1] aller Nutzer surfen mittlerweile in Apps, deren technologische Basis Cookies zu einem Auslaufmodell machen (da in der App kein Browser mehr zum Einsatz kommt). Darüber hinaus haben die Browserhersteller das Thema Datenschutz für sich entdeckt und blocken zunehmend aktiv und unabhängig von gesetzlich verankerten Vorgaben nun den Einsatz von 3rd Party Cookies. Ganz zu schweigen von dem Umstand, dass die Multi-Device-Nutzung heute gang und gäbe ist, was einer weiteren Fragmentierung des Nutzerprofils gleichkommt.

Times have changed, however. 52% of all users now surf in apps whose technological basis makes cookies a phase-out model (because the app no longer uses a browser). In addition, browser manufacturers have discovered the topic of data protection for themselves and are now increasingly actively blocking the use of 3rd party cookies, independently of statutory requirements. Not to mention the fact that multi-device use is now commonplace, which is tantamount to further fragmentation of the user profile.

Im Ergebnis werden so Geschäftsmodelle, die auf personalisierter Ansprache beruhen, weiter eingeschränkt. Die digitale Industrie versucht daher das Thema Advertising Identity neu und ganzheitlicher (unabhängig von Device, Browser oder App) zu denken und die Frage zu stellen, welche Art der digitalen Profilierung und Werbeauslieferung für alle Beteiligten effizienter und nachhaltiger sein kann als das Setzen von proprietären (Third-Party-)Cookie-Tracking-

As a result, business models based on personalized addressing are further restricted. The digital industry is therefore attempting to rethink the issue of Advertising Identity in a new and more holistic way (independent of device, browser or app) and to ask what kind of digital profiling and advertising delivery can be more efficient and sustainable for all parties involved than the use of proprietary (third-party) cookie tracking mechanisms on individual browsers and devices.

[1] http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

Mechanismen auf einzelnen Browsern und Devices.

Unlängst hat Mozilla mit Firefox v69 einer einjährigen Phase der Ankündigung Taten folgen lassen und Third Party Tracking Cookies per Default geblockt (Enhanced Tracking Protection), was insbesondere im deutschen Markt mit durchschnittlich 26 % Firefox-Anteil am Webtraffic einen weiteren relevanten Schritt in Richtung cookielose Zukunft manifestierte.

With Firefox v69, Mozilla recently followed up a one-year phase of announcements with deeds and blocked third-party tracking cookies by default (Enhanced Tracking Protection), which manifested another relevant step towards a cookie-free future, especially in the German market with an average of 26 % Firefox share of web traffic.

Safari ist diesen Schritt mit seiner Intelligent Tracking Prevention (ITP) bereits vor zwei Jahren gegangen, was aufgrund seiner geringen Marktverbreitung (<7 %)[2] noch überschaubare Auswirkungen hatte.

Safari already took this step two years ago with its Intelligent Tracking Prevention (ITP), which still had a manageable impact due to its low market penetration (<7 %).

Schon jetzt sind Konsequenzen sichtbar: 3rd Party Cookies als technische Grundlage des effizienten programmatischen Einkaufs, Frequency Cappings, nutzerzentrierte Bid-Preise greifen nicht mehr; Targeting ist nicht mehr sinnvoll möglich.

Consequences are already visible: 3rd party cookies as the technical basis for efficient programmatic purchasing, frequency capping, user-centered bid prices are no longer effective; targeting is no longer possible in a meaningful way.

Daraus ergibt sich die Frage: Wie kann vor dem Hintergrund der Marktentwicklung und Wahrung der Nutzerinteressen das System für alle Beteiligten – inkl. der Konsumenten – verbessert und stabiler gemacht werden?
Ziel ist es, persistente, pseudonyme Identities von Nutzern zu schaffen, die mehrere Identifier verschiedener Couleur umfassen können (Login-basiert; Cookie-basiert; Betriebssystem-seitig bereitgestellt; statistisch berechnet).

This leads to the question: Against the background of market development and the protection of user interests, how can the system be improved and made more stable for all parties involved - including consumers?
The aim is to create persistent, pseudonymous identities of users, which can include several identifiers of different kinds (login-based; cookie-based; provided by the operating system; statistically calculated).

Langfristig muss es das Ziel der beteiligten Akteure sein, dass ein einheitliches System von Unified Identifiern etabliert und umfänglich durchgesetzt wird. Ein solcher Ansatz führt zu Vorteilen auf allen Ebenen und wirkt einer weiteren Fragmentierung der Datenverarbeitung und -vorhaltung entgegen, fördert folglich auch den von der DSGVO geforderten Grundsatz der Datensparsamkeit. Hierdurch erhalten Nutzer erneut und wesentlich besser Zugriff auf ihre Daten und können ihre Rechte zielgerichtet geltend machen. Aufsichtsbehörden finden ihre Arbeit erleichtert, da knappe Ressourcen nicht mehr für das Durchforsten unzähliger

In the long term, it must be the goal of the actors involved to establish and comprehensively enforce a uniform system of Unified Identifiers. Such an approach leads to advantages at all levels and counteracts further fragmentation of data processing and data retention, and consequently also promotes the principle of data economy required by the DSGVO. As a result, users gain renewed and much better access to their data and can assert their rights in a targeted manner. Supervisory authorities find their work easier, as scarce resources no longer have to be used for thinning countless cookie forests. Finally, within the framework of a uniform Advertising

[2] https://de.statista.com/statistik/daten/studie/13007/umfrage/marktanteile-der-browser-bei-der-internetnutzung-in-deutschland-seit-2009/

Cookiewälder verbraucht werden müssen. Die Wirtschaft schlussendlich kann im Rahmen einer einheitlichen Advertising-Identifier-Landschaft sowohl für Advertiser als auch für Publisher eine effiziente Aussteuerung von bedarfsgerechten Kampagnen und damit eine dauerhafte Monetarisierung des freien Internets ermöglichen. Dies wiederum kommt den Nutzern erneut zugute, denn Inhalte bleiben frei verfügbar. Zudem wird das werbliche Angebot optimal auf die Bedürfnisse des Nutzers angepasst und wirkt dadurch weniger invasiv und störend.

Identifier Landscape, the economy can enable both advertisers and publishers to efficiently manage campaigns according to demand and thus to achieve a lasting monetization of the free Internet. This in turn benefits users once again, because content remains freely available. In addition, the advertising offer is optimally adapted to the needs of the user and thus appears less invasive and disruptive.

2 Was ist eine Advertising Identity?

2 What is an advertising identity?

Die Advertising Identity soll die Wiedererkennung eines pseudonymisierten Profils zum Zwecke der effizienten Werbeaussteuerung in Form von Personalisierung, Lokalisierung, Verifizierung, Erfolgsmessung und kontakt- und reichweitenoptimierter Budgetallokation von Werbemitteln ermöglichen.
Mit Advertising Identity ist die rein technische, pseudonymisierte Identität des Nutzers in Form der Gesamtheit (Graph) der Identifier (ID) und damit die Zusammenführung der in den unterschiedlichen Devices verwendeten ID-Formen gemeint. Die Advertising Identity hat weiterhin explizit nicht den Zweck der Identifizierung von natürlichen Personen.

The Advertising Identity should enable the recognition of a pseudonymised profile for the purpose of efficient advertising control in the form of personalisation, localisation, verification, performance measurement and contact and reach-optimised budget allocation of advertising media.
Advertising Identity means the purely technical, pseudonymised identity of the user in the form of the entirety (graph) of the identifiers (ID) and thus the combination of the ID forms used in the different devices. Furthermore, Advertising Identity explicitly does not have the purpose of identifying natural persons.

Die IDs werden im Falle der Browser-Nutzung entweder im Cookie oder im Local Storage gespeichert, während im Falle der nativen In-App-Nutzung die IDs systemisch bereitgestellt werden (Mobile-iOS- oder Android-Werbe-ID). Im Falle der Login- oder Fingerprint-basierten Lösungen werden die IDs meist serverseitig inkl. der Nutzdaten verwaltet.

In the case of browser use, the IDs are stored either in the cookie or in local storage, whereas in the case of native in-app use, the IDs are provided systemically (mobile iOS or Android Advertising ID). In the case of login- or fingerprint-based solutions, the IDs are usually managed on the server side including the user data.

3 Wie stehen Unternehmen in der digitalen Wirtschaft zu den aktuellen Entwicklungen?

3 What do companies in the digital economy think about current developments?

Die Customer Journey kann mit Cookies nicht vollständig abgebildet werden und Cookie-Aktivitäten der werbetreibenden Digital-Industrie

The customer journey cannot be fully mapped with cookies and cookie activities of the digital

werden durch diverse Entwicklungen eingeschränkt. Marktteilnehmer spüren einen relevanten Umsatzrückgang für Mozilla-Firefox-Traffic (Stand: Ende September 2019). Trotzdem reagiert der Markt verhalten. Die Gründe dafür sind vielschichtig.

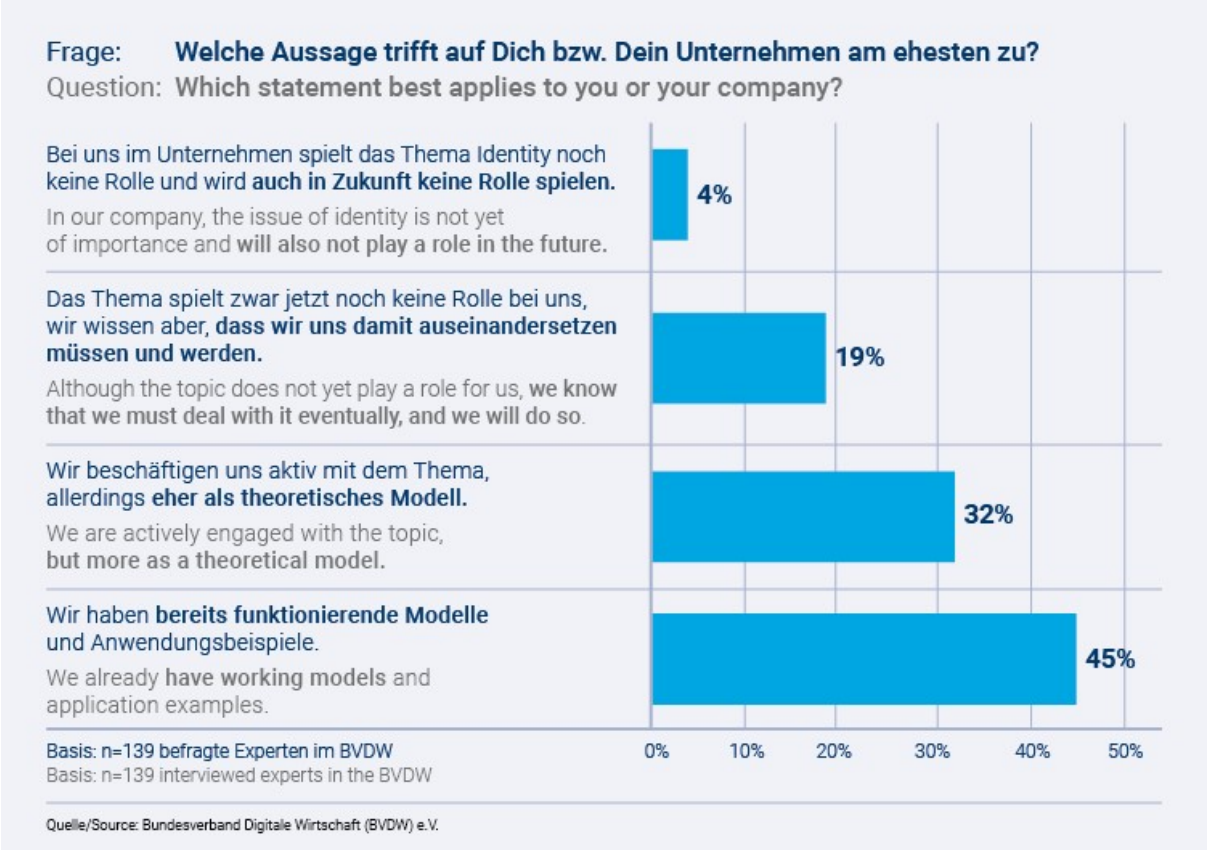
Das Thema Advertising Identity ist sehr technisch und muss trotzdem auf Entscheider-Ebene im Detail verstanden werden, da das Thema das Geschäftsmodell unmittelbar beeinflusst. Des Weiteren erfordert die Advertising Identity eine genaue Auseinandersetzung mit allen wesentlichen Datenschutzanforderungen und involviert zwingend die juristische Perspektive in Hinblick auf den Schutz der personenbezogenen Daten des Nutzers zur Schaffung einer nachhaltigen Lösung.

advertising industry are limited by various developments. Market participants are experiencing a relevant decline in sales for Mozilla Firefox traffic (as of the end of September 2019). Nevertheless, the market is reacting cautiously. The reasons for this are complex.

The topic of Advertising Identity is very technical and must nevertheless be understood in detail at decision-maker level, as the topic directly influences the business model. Furthermore, Advertising Identity requires a precise examination of all essential data protection requirements and necessarily involves the legal perspective with regard to the protection of the user's personal data in order to create a sustainable solution.

Eine Umfrage unter BVDW-Mitgliedsunternehmen soll Einblicke in den Wissensstand zur Advertising Identity geben. Demzufolge beschäftigen sich mehr als drei Viertel der befragten Teilnehmer aktiv mit dem Thema oder haben schon konkrete Anwendungsfälle:

A survey among BVDW member companies is to provide insights into the state of knowledge about Advertising Identity. According to the survey, more than three quarters of the participants questioned are actively involved in the topic or already have concrete use cases:



Je nach Wissensstand wird außerdem die Verantwortung, den Markt mit Lösungen für eine Advertising Identity zu versorgen, unterschiedlich verortet. Befragte mit geringerem Wissensstand sehen die Supply Side (SSPs und Publisher) in der Verantwortung, Befragte mit höherem Wissensstand fordern hingegen Lösungen von Spezialanbietern.

Depending on the level of knowledge, the responsibility to provide the market with solutions for an Advertising Identity is also located differently. Respondents with a lower level of knowledge consider the supply side (SSPs and publishers) to be responsible, while respondents with a higher level of knowledge demand solutions from specialist providers.

Für ein besseres Verständnis hilft dem Großteil, sich mit anderen Marktteilnehmern auszutauschen, sich von Spezialisten beraten zu lassen oder Fachartikel zu lesen.

For a better understanding, the majority of respondents find it helpful to exchange information with other market participants, to seek advice from specialists or to read specialist articles.

Der Umstand, dass Cookies an Bedeutung verlieren werden, ist der Umfrage nach der Mehrheit bewusst (79 % der mit hohem Wissensstand Befragten):

The majority of respondents to the survey are aware that cookies will become less important (79% of those with a high level of knowledge):

Die Motivation des BVDW, sich der Marktaufklärung zur Advertising Identity anzunehmen, korreliert mit den Ergebnissen der Frage, was auf Verbandsseite in den nächsten 12 Monaten am wichtigsten wäre. Neben Sensibilisierung und Aufklärung des Marktes wurden hier auch die Schaffung einheitlicher Standards und Zusammenarbeit genannt.

Alle Ergebnisse der Umfrage sind hier zu finden: https://www.bvdw.org/der-bvdw/gremien/programmatic-advertising/publikationen/#jump

The motivation of the BVDW to take on the market education on Advertising Identity correlates with the results of the question what would be most important on the association side in the next 12 months. In addition to raising awareness and educating the market, the creation of uniform standards and cooperation were also mentioned here.

All results of the survey can be found here: https://www.bvdw.org/der-bvdw/gremien/programmatic-advertising/publikationen/#jump

4 Fazit

4 Summary

Der Aufbau der durch alle Branchenteilnehmer im Digital Advertising gemeinsam genutzten Advertising Identity ist von fundamentaler Bedeutung für die Zukunft des Programmatic Advertising. Eine cookielose Zukunft ist eigentlich weniger eine Bedrohung, sondern vielmehr eine echte Chance für einen neuen und besseren Industriestandard. Dieser neue Standard bringt Vorteile für alle Teilnehmer und wirkt der Identitäts-Fragmentierung der Datenverarbeitung und -vorhaltung entgegen.

Künftig sollten allerdings eher wenige Advertising Identities unterschiedlicher Herkunft – basierend auf offenen Standards – nebeneinander im Markt

Building the advertising identity shared by all industry participants in digital advertising is of fundamental importance for the future of programmatic advertising. A cookie-free future is actually less of a threat than a real opportunity for a new and better industry standard. This new standard brings benefits to all participants and counteracts the identity fragmentation of data processing and storage.

In the future, however, rather few advertising identities of different origins - based on open standards - should coexist in the market to ensure

existieren, um sicherzustellen, dass sich der heutige Aufwand für die Synchronisation unterschiedlicher Identity-Quellen signifikant reduziert (Stichwort Cookie-Sync) und vor allem dem Anspruch der Nutzer nach mehr Kontrolle über seine Daten und deren Nutzung im Ökosystem Rechnung getragen wird.

that today's effort for the synchronization of different identity sources is significantly reduced (keyword cookie-sync) and, above all, that the users' demand for more control over their data and its use in the ecosystem is met.

Generell sollte der Nutzen für den Nutzer beim Aufbau eines einheitlichen Standards im Fokus stehen. Durch die Advertising Identity erhält der Nutzer wesentlich besseren Zugriff auf und Kontrolle über seine Daten. Inhalte bleiben frei verfügbar und das werbliche Angebot wird optimal auf die Bedürfnisse des Nutzers angepasst, so dass es weniger störend wirkt.

In general, the focus should be on the benefit for the user when establishing a uniform standard. Advertising Identity gives the user much better access to and control over his data. Content remains freely available and the advertising offer is optimally adapted to the needs of the user, so that it is less disruptive.

Die Advertising Identity hat klare Vorteile für Advertiser und Publisher, da diesen eine effiziente und effektive Aussteuerung von bedarfsgerechten Kampagnen und eine dauerhafte Monetarisierung im Open Web ermöglicht wird.

The Advertising Identity has clear advantages for advertisers and publishers, as it enables them to efficiently and effectively manage campaigns according to demand and to achieve lasting monetization in the Open Web.

Letztendlich kann durch eine Zusammenarbeit und Schaffung eines einheitlichen Standards mehr Verantwortung, Transparenz und Vertrauen im digitalen Ökosystem und gegenüber der Gesellschaft geschaffen werden. Ein transparentes Handeln und gemeinsame Standards sind der Schlüssel zu Erfolg und Wachstum sowie mehr Nachhaltigkeit im gesamten AdTech-Ökosystem.

Ultimately, by working together and creating a uniform standard, more responsibility, transparency and trust can be created in the digital ecosystem and towards society. Transparent actions and common standards are the key to success and growth as well as more sustainability in the entire AdTech ecosystem.

Glossar
Glossary

Cookies

Ein Cookie (Englisch „Keks“) ist eine Textinformation, die im Browser auf dem Computer des Betrachters jeweils zu einer besuchten Website (Domain und URL-Pfad), versehen mit einem Ablaufdatum, in einer Datei gespeichert werden kann. Die für eine Webseite im Browser gespeicherten Cookies werden mit jedem Seitenaufruf (HTTP Request) im Header der angefragten URL wieder mit übertragen, so dass der die Webseite ausliefernde Adserver auf die Werteinformation des jeweiligen Cookies reagieren kann. Ein Cookie selbst besteht aus einem Namen und einem Wert. Name und Wert sind Folgen von druckbaren US-ASCII-Zeichen, wobei einige Zeichen ausgeschlossen sind. Um komplexere (multiple) Werte speichern zu können, kann man eine base64-Enkodierung vornehmen. Die Wertemenge des Cookies ist begrenzt.

A cookie is a piece of text information that can be stored in a file in the browser on the viewer's computer for each website visited (domain and URL path), provided with an expiration date. The cookies stored in the browser for a website are transferred again with each page call (HTTP request) in the header of the requested URL, so that the ad server delivering the website can react to the value information of the respective cookie. A cookie itself consists of a name and a value. Name and value are sequences of printable US-ASCII characters, some characters are excluded. To be able to store more complex (multiple) values, base64 encoding can be used. The value set of the cookie is limited.

Aufgabe dieser persistenten Cookies (Name-Werte-Kombinationen) ist beispielsweise die pseudonyme Identifizierung des Surfers, das Abspeichern eines Logins bei einer Internetanwendung oder das Zwischenspeichern von Artikeln in einem Warenkorb eines Online-Händlers. Der im Zusammenhang mit diesem Whitepaper wichtigste Anwendungsfall ist die Speicherung von Identifiern zum Zwecke der personalisierten Werbeausspielung in einem Cookie.

The function of these persistent cookies (name-value combinations) is, for example, to identify the surfer pseudonymously, to save a login to an Internet application or to temporarily store items in an online retailer's shopping basket. The most important use case in connection with this white paper is the storage of identifiers in a cookie for the purpose of personalised advertising.

Der Begriff Cookie wird in der aktuellen Datenschutzdiskussion auch als Synonym für Tracking verwendet, unabhängig davon, ob dazu tatsächlich ein physischer Cookie verwendet oder andere Techniken eingesetzt wurden.

The term cookie is also used in the current data protection discussion as a synonym for tracking, regardless of whether a physical cookie was actually used or other techniques were employed for this purpose.

1st vs. 3rd Party Cookies

Cookies (Name-Werte-Informationen) werden automatisch und ausschließlich im HTTP Request einer Seite übertragen und können auch nur so von der Webseite gelesen werden, des Weiteren können Zugriffe auf den Webserver und sichere Verbindungen eingeschränkt werden, diese werden vom Browser umgesetzt. Dadurch wird ausgeschlossen, dass eine Webseite Zugriff auf Cookies anderer Webseiten erhält.

Cookies (name-value information) are transferred automatically and exclusively in the HTTP request of a page and can only be read by the website in this way. Furthermore, access to the web server and secure connections can be restricted, these are implemented by the browser. This prevents a website from accessing cookies from other websites.

Die Definition von 1st und 3rd Party Cookies ergibt sich aus der Art ihrer Erzeugung und der Vorgänge, die zum Lesen der jeweiligen Cookies angewendet werden.

The definition of 1st and 3rd party cookies results from the way they are generated and the processes used to read the respective cookies.

Da eine Webseite (A) Cookies nur innerhalb ihrer eigenen Domain schreiben und lesen darf, wird eine externe Webseite (B) von der initiierenden Webseite (A) ohne Zutun des Nutzers aufgerufen, die dann ihrerseits ihre Cookies liest oder schreibt und diese Information an die initiierende Webseite (A) weiterreicht. Bei der Webseite (B) handelt es sich um eine ausschließlich für Trackingzwecke genutzte Domain (Tracking-Script). Durch diesen Vorgang wird ein „Cross-Domain"-Informations-Sharing ermöglicht, welches für eine Webseiten-übergreifende pseudonyme Nutzer-Identifizierung im Rahmen von personalisierter Werbeausspielung vonnöten ist. Gleichzeitig sind die Cookies der Trackingseite durch die Art des Aufrufs als „3rd Party" Cookie markiert, was Browsern ermöglicht, das Lesen/Schreiben genau dieser Art von Cookies zu unterbinden.

Since a website (A) may only write and read cookies within its own domain, an external website (B) is called up by the initiating website (A) without any action on the part of the user, which in turn reads or writes its cookies and passes this information on to the initiating website (A). The website (B) is a domain used exclusively for tracking purposes (tracking script). This process enables "cross-domain" information sharing, which is necessary for cross-webpage pseudonymous user identification in the context of personalized advertising delivery. At the same time, the cookies of the tracking site are marked as "3rd party" cookies by the type of call, which enables browsers to prevent the reading/writing of exactly this type of cookies.

Unterscheidung Cookie vs. Local Storage // Differentiation cookie vs. local storage

Neben den Cookies fällt zunehmend der Begriff „Local Storage" als Speicherort für zum Beispiel Identifier im Browser. Das Local Storage ist eine Art des (DOM) Web Storage[3]. Hierbei handelt es sich um unterschiedliche Techniken, mit der Daten in einem Webbrowser gespeichert werden können. Web Storage unterstützt die Datenspeicherung, ähnlich Cookies, und ist als lokale (Local Storage) und Session-spezifische Speicherung (Session Storage) verfügbar, die sich in Gültigkeitsbereich und -dauer unterscheiden. Bei Mozilla Firefox werden die Daten in der Datenbankdatei *webappsstore.sqlite* gespeichert.

In addition to cookies, the term "local storage" is increasingly used as a storage location for identifiers in the browser, for example. The Local Storage is a type of (DOM) Web Storage . These are different techniques with which data can be stored in a web browser. Web Storage supports data storage, similar to cookies, and is available as local (Local Storage) and session-specific (Session Storage) storage, which differ in scope and duration. In Mozilla Firefox, data is stored in the webappsstore.sqlite database file.

Warum aber gibt es diese Alternativen zum Cookie? DOM Storage wurde im Kontext von HTML5 entwickelt, um rein clientseitige Applikationen zu ermöglichen, die ohne einen Webserver auskommen abseits deren Auslieferung an den Browser. Die Technik bietet weitaus größere Speicherkapazität (>5 MB pro Domain) und bessere Entwicklungsschnittstellen. In einigen Punkten unterscheidet sie sich jedoch von Cookies. Im Gegensatz zu Cookies, auf die sowohl Server als auch Client zugreifen können,

But why do these alternatives to the cookie exist? DOM Storage was developed in the context of HTML5 to enable purely client-side applications that do not require a web server and are not delivered to the browser. The technology offers much larger storage capacity (>5 MB per domain) and better development interfaces. In some points, however, it differs from cookies. Unlike cookies, which can be accessed by both server and client, DOM Storage is completely controlled by the client. Data is not transferred to the server

[3] https://de.wikipedia.org/wiki/Web_Storage

wird DOM Storage vollständig vom Client gesteuert. Es werden hierbei nicht mit jedem HTTP-Request Daten zum Server übertragen und ein Webserver kann auch nicht direkt Daten ins DOM Storage schreiben. Der Zugriff erfolgt ausschließlich über Skripte auf der Webseite. Dieser Umstand führt dazu, dass meist der Einfachheit halber nach wie vor Cookies statt Web Storage verwendet werden.

with every HTTP request and a web server cannot write data directly to DOM Storage. The access is exclusively done via scripts on the web page. This circumstance leads to the fact that cookies are still used instead of web storage for the sake of simplicity.

ID/Identifier

Eindeutige Identifier (ID) gibt es in vielen Ausprägungen. Im Allgemeinen ist ein Identifier nur eine Reihe eindeutiger Zahlen, Buchstaben oder Symbole, die ein Objekt als eindeutig kennzeichnen. In Datenbanken ist es typischerweise eine lange Zeichenkette, auch in heutigen digitalen Werbesystemen haben IDs keine symbolische Bedeutung, sondern liegen beispielsweise als Hash vor. Ein solcher Hashwert sieht beispielsweise so aus: CE06AC1ED1EA6E7B3254F14F19F515AD77E05871.
In der klassischen Cookie-basierten Webbrowser-Welt wird für jedes Device und den darauf verwendeten Browser eine ID generiert. Diese landet entweder in einem (1st oder 3rd Party) Cookie oder im „Local Storage“[4].

Unique identifiers (ID) exist in many forms. In general, an identifier is just a series of unique numbers, letters or symbols that identify an object as unique. In databases, it is typically a long string of characters. Even in today's digital advertising systems, IDs do not have a symbolic meaning, but are present, for example, as a hash. Such a hash value looks like this: CE06AC1ED1EA6E7B3254F14F19F515AD77E05871.
In the classic cookie-based web browser world, an ID is generated for each device and the browser used on it. This ID is either stored in a (1st or 3rd party) cookie or in the "Local Storage".

Die ID selbst ist somit erst einmal nicht gleichbedeutend mit einer Nutzer-Identität. Vielmehr stellt sie innerhalb der gegebenen Systemgrenzen eine (meist pseudonyme) eindeutige Repräsentation des User Device und des dabei verwendeten Browsers dar. Verwendet der Nutzer ein zweites Device oder einen anderen Browser, wird eine zweite ID generiert. Diese kann mit der ersten ID zunächst nicht zusammengebracht werden, da sich die Gerätegrenzen nicht ohne weiteres überwinden lassen. Eine ID repräsentiert somit erst einmal nur eine Teil-Identität.

The ID itself is therefore not synonymous with a user identity for the time being. Rather, within the given system boundaries, it is a (usually pseudonymous) unique representation of the user device and the browser used. If the user uses a second device or another browser, a second ID is generated. This second ID cannot be combined with the first ID, since the device boundaries cannot be easily overcome. An ID therefore only represents a partial identity.

Die ID selbst ist zunächst nutzlos, sofern sie nicht mit (Nutz-)Daten verknüpft wird. Dies können z. B. Targeting-Profildaten für einen Benutzer (Soziodemografie, Affinitäten etc.), Frequency-Cappings einer Kampagne oder bei Consent-Einholung auch ein Opt-in/-out sein.

The ID itself is initially useless unless it is linked to (useful) data. This can be, for example, targeting profile data for a user (socio-demographics, affinities, etc.), frequency capping of a campaign or, in the case of content collection, an opt-in/out.

[4] https://de.wikipedia.org/wiki/Web_Storage#localStorage

Wird ein Cookie gelöscht, geht auch die darin gespeicherte ID verloren. Weder ID noch Nutzdaten können dann dem Nutzer weiter zugeordnet werden. Das Cookie selbst ist nicht die ID, sondern nur der „Lagerort“ für diese.

If a cookie is deleted, the ID stored in it is also lost. Neither ID nor user data can then be further assigned to the user. The cookie itself is not the ID, but only the "storage location" for it.

Persistenz // Persistence

Persistenz (von lateinisch persistere „durch, über (eine Zeit) hinweg bleiben“) ist in der Informatik der Begriff, der die Fähigkeit bezeichnet, Daten (oder Objekte) oder logische Verbindungen über lange Zeit bereitzuhalten.

Persistence (from Latin persistere "to stay through, over (a time)") is the term used in computer science to describe the ability to hold data (or objects) or logical connections for a long time.

Dafür wird ein nichtflüchtiges Speichermedium benötigt; auch das Cookie im Browser ist ein zunächst nichtflüchtiger Speicherort. Der Begriff wird zunehmend im Zusammenhang mit eindeutigen und dauerhaften Identifikatoren digitaler Objekte verwendet. So eben auch im Zusammenhang mit dem Werbe-Identifier.

This requires a non-volatile storage medium; the cookie in the browser is also an initially non-volatile storage location. The term is increasingly used in connection with unique and permanent identifiers of digital objects. This is also the case with the advertising identifier.

„Persistent“ wird als ein im Kontext wohldefinierter Fachbegriff für „nicht unkontrolliert veränderlich“ verwendet. Das bedeutet beispielsweise, dass die Daten auch nach Beenden des Programms – z. B. des Browsers – vorhanden (gespeichert) bleiben und bei erneutem Aufruf des Programms wieder rekonstruiert und angezeigt werden können.

"Persistent" is used as a technical term for "not uncontrollably variable", which is well defined in the context. This means, for example, that the data remains available (stored) even after the program - e.g. the browser - is closed and can be reconstructed and displayed when the program is called up again.

Daten, die diese Eigenschaft nicht besitzen, existieren beispielsweise nur im Hauptspeicher des Computers und verändern oder verlieren ihren Inhalt, sobald das Programm endet, von dem sie angelegt wurden. Solche „flüchtigen“ Daten werden transient genannt, sie sind gepuffert.

For example, data that does not have this property only exists in the computer's main memory and changes or loses its contents when the program that created it ends. Such "volatile" data is called transient, it is buffered.

War der Cookie bisher immer ein persistenter Speicherort, wird er durch Firefox Enhanced Tracking Protection oder Safaris Intelligent Tracking Protection (ITP) zunehmend transient – überlebt somit nur noch eine Page Impression oder eine Session des Browsers.

While the cookie has always been a persistent storage location, Firefox Enhanced Tracking Protection or Safaris Intelligent Tracking Protection (ITP) makes it increasingly transient - so only one page impression or session of the browser survives.

Mobile Werbe-ID // Mobile advertising ID

Die Werbe-ID ist eine eindeutige ID für Werbezwecke, die von dem jeweiligen mobilen Betriebssystem (Android, iOS oder Windows) bereitgestellt wird und vom Nutzer zurückgesetzt werden kann. Sie findet ausschließlich in nativen Apps Anwendung, da der Zugriff auf diese ID im

The Advertising ID is a unique ID for advertising purposes, which is provided by the respective mobile operating system (Android, iOS or Windows) and can be reset by the user. It is only used in native apps, as access to this ID on the

mobilen Web aktuell von Browsern nicht unterstützt wird.

mobile web is currently not supported by browsers.

Nutzer haben durch die zentrale Bereitstellung über das Betriebssystem und die Möglichkeit, die ID zurückzusetzen, eine bessere Kontrolle und Entwickler können über ein einfaches Standardsystem weiterhin ihre Apps monetarisieren.

Users have better control through centralized deployment via the operating system and the ability to reset the ID, and developers can continue to monetize their apps via a simple standard system.

Die allgemein als Werbe-ID bezeichneten Identifier haben in den unterschiedlichen Betriebssystemen unterschiedliche Bezeichnungen. So nennt Apple bei iOS die Werbe-ID „Identifier for Advertisers" (IDFA)[5], während Google bei Android diese als Advertising-ID[6] (AAID) bezeichnet. Ab Windows 10 steht auch auf dem von Microsoft herausgegebenen Betriebssystem eine Werbe-ID zur Verfügung, die wir als Windows Ad ID bezeichnen wollen (WAID).

The identifiers generally referred to as advertising IDs have different names in the various operating systems. Apple calls the Advertising ID "Identifier for Advertisers" (IDFA) in iOS, while Google calls it the Advertising ID (AAID) in Android. Starting with Windows 10, an Advertising ID is also available on the operating system published by Microsoft, which we will refer to as the Windows Ad ID (WAID).

(ID) Graph

Ein Graph ist in der Graphentheorie eine abstrakte Struktur, die eine Menge von Objekten zusammen mit den zwischen diesen Objekten bestehenden Verbindungen repräsentiert. Die mathematischen Abstraktionen der Objekte werden dabei Knoten (auch Ecken) des Graphen genannt. Die paarweisen Verbindungen zwischen Knoten heißen Kanten (manchmal auch Bögen). Die Kanten können gerichtet oder ungerichtet sein. Häufig werden Graphen anschaulich gezeichnet, indem die Knoten durch Punkte und die Kanten durch Linien dargestellt werden.

In graph theory, a graph is an abstract structure that represents a set of objects together with the connections existing between these objects. The mathematical abstractions of the objects are called nodes (also corners) of the graph. The pairwise connections between nodes are called edges (sometimes arcs). The edges can be directed or undirected. Often graphs are drawn graphically by representing the nodes by points and the edges by lines.

Anschauliche Beispiele für Graphen sind ein Stammbaum oder das U-Bahn-Netz einer Stadt. Bei einem Stammbaum stellt jeder Knoten ein Familienmitglied dar und jede Kante ist eine Verbindung zwischen einem Elternteil und einem Kind. In einem U-Bahn-Netz stellt jeder Knoten eine U-Bahn-Station dar und jede Kante eine direkte Zugverbindung zwischen zwei Stationen.

Examples of graphs are a family tree or the subway network of a city. In a family tree, each node represents a family member and each edge is a connection between a parent and a child. In a subway network, each node represents a subway station and each edge is a direct train connection between two stations.

Gem. Definition der Advertising Identity stellt diese einen Graphen aus Identifiern, sprich einen „ID-Graphen" dar, der mit individuellen Nutzern korreliert.

According to the definition of Advertising Identity, it is a graph of identifiers, i.e. an "ID graph" that correlates with individual users.

[5] https://www.infonline.de/old_glossar/identifier-for-advertising-idfa/

[6] http://www.androiddocs.com/google/play-services/id.html

Frequency Capping

Frequency Capping bedeutet die kontrollierte Auslieferung eines Werbemittels pro Unique-Client / Einzelnutzer nach Anzahl und Zeiteinheit (Tag, Stunde etc.) via Adserver/DSP. Durch Steuerung der Kontaktfrequenz soll u. a. die Werbewirkung beeinflusst werden. Die Möglichkeit des Cappings auf Unique-Client-Basis wird dabei meist über ein Cookie realisiert.

Frequency Capping means the controlled delivery of an advertising medium per Unique Client / individual user according to number and time unit (day, hour etc.) via adserver/DSP. Among other things, the advertising effect is to be influenced by controlling the contact frequency. The possibility of capping on a unique client basis is usually realised via a cookie.

Customer Journey

Weg („Reise") eines Internet-Nutzers vom ersten Werbemittelkontakt bis zum (Online-)Kaufabschluss. Die Customer Journey ist besonders im Online-Marketing bzw. in digitalen Kanälen interessant, da hier das Verhalten der Konsumenten mit Hilfe von Trackingtechnologien gut abgebildet werden kann.

The path ("journey") of an Internet user from the first contact with advertising material to the (online) conclusion of a purchase. The customer journey is particularly interesting in online marketing or digital channels, as the behavior of consumers can be well mapped with the help of tracking technologies.

ePrivacy Richtlinie vs. ePrivacy Verordnung (ePrivVO) // ePrivacy Directive vs. ePrivacy Regulation (ePrivVO)

Die Datenschutzrichtlinie für elektronische Kommunikation[7] , (sog. ePrivacy-Richtlinie), ist eine 2002 erlassene EU-Richtlinie, die ins nationale Recht umgesetzt werden muss. Sie regelt die Vertraulichkeit der Kommunikation, die auch nicht personenbezogene Daten und Daten in Bezug auf juristische Personen enthalten kann. Sie ergänzte ursprünglich die alte Datenschutzrichtlinie von 1995 (Datenschutzrichtlinie)[8] und steht nun neben der neuen EU-Datenschutzgrundverordnung (DSGVO). Seit der letzten Aktualisierung im Jahre 2009 ist sie auch unter der Bezeichnung „Cookie-Richtlinie" (2009/136/EG)[9] bekannt. Im neu gefassten Art. 5 Abs. 3 ist geregelt , "... dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist wenn der betreffende Teilnehmer oder Nutzer (…), seine Einwilligung gegeben hat.".

The ePrivacy Directive, an EU Directive adopted in 2002, must be transposed into national law. It regulates the confidentiality of communications, which may include non-personal data and data relating to legal persons. It originally supplemented the old Data Protection Directive of 1995 (Data Protection Directive) and now stands alongside the new EU Basic Data Protection Regulation (DSGVO). Since the last update in 2009 it is also known as the "Cookie Directive" (2009/136/EC). The new version of Art. 5 (3) stipulates that "... the storage of information or access to information already stored in the terminal equipment of a subscriber or user is only permitted if the subscriber or user concerned has given his consent".

[7] 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); abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058

[8] 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, abrufbar unter: https://eur-lex.europa.eu/legalcontent/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE

[9] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32009L0136

Während die Mehrzahl der EU-Mitgliedsstaaten die Vorgaben des Art. 5 Abs. 3 ePrivacy- Richtlinie mehr oder weniger wortgleich übernommen hatten, war in Deutschland ein Sonderweg eingeschlagen worden. 2004 transformierte Deutschland die Datenschutzrichtlinie für elektronische Kommunikation durch die Novellierung des Telekommunikationsgesetzes in deutsches Recht. Das Telemediengesetz (TMG) blieb jedoch unangetastet. Bis zum aktuellen Zeitpunkt (September 2019) findet daher in Deutschland noch das Telemediengesetz (TMG) Anwendung. §12 stellt klar, dass personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden dürfen, wenn der Gesetzgeber dies ausdrücklich erlaubt.
Für Nutzungsdaten erlaubt der deutsche Gesetzgeber in § 15 Abs. 3 TMG eine einwilligungslose Nutzungsdatenverarbeitung unter besonderen Bedingungen (Pseudonymisierungspflicht, Transparenz, Widerspruchsmöglichkeit). Eine aus Sicht der digitalen Wirtschaft begrüßenswerte Vorschrift, die den Gedanken von “privacy by design” durch abwägende, gesetzgeberische Wertung für Nutzungsdaten und die Bedingungen für deren Verarbeitung festschrieb.

While the majority of the EU member states had adopted the requirements of Art. 5 para. 3 ePrivacy Directive more or less word-for-word, a special path had been taken in Germany. In 2004, Germany transformed the ePrivacy Directive for electronic communications into German law by amending the Telecommunications Act. However, the Telemediengesetz (TMG) remained untouched. Until the current date (September 2019), the Telemediengesetz (TMG) will therefore still apply in Germany. §Section 12 clarifies that personal data in connection with the provision of telemedia may only be processed without consent if the legislator expressly permits this.
For usage data, the German legislator allows in § 15 para. 3 TMG an unapproved processing of usage data under special conditions (obligation to use pseudonyms, transparency, possibility to object). From the point of view of the digital economy, this is a welcome provision which enshrines the idea of "privacy by design" by means of a deliberate, legislative evaluation of usage data and the conditions for their processing.

Mit Anwendbarkeit der DSGVO ab Mai 2018 entbrannte jedoch eine lebhafte Debatte über die Weitergeltung des TMG und namentlich dieser speziellen Vorschrift, deren Regelungsgedanke allerdings auch dem Gedanken aus Art. 6 Abs. 1 f) DSGVO entspricht. Hier ist bestimmt, dass eine Verarbeitung auch ohne Einwilligung erlaubt ist, soweit sie zur Wahrung der berechtigten Interessen des (grundrechtlich ebenfalls geschützten) Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.
Die ePrivacy-Richtlinie aus 2002 und ihre Novellierung aus 2009 sind nicht zu verwechseln mit der ePrivacy-Verordnung. Am 10.Januar 2017 hat die EU-Kommission offiziell den Entwurf für eine neue ePrivacy-Verordnung (ePV) vorgestellt. Die neue Verordnung nimmt die alte Regelungsmaterie auf und erweitert sie. Im Mittelpunkt steht neben dem Schutz der Vertraulichkeit der Kommunikation nun vor allem

With the applicability of the DSGVO from May 2018, however, a lively debate broke out about the continued validity of the TMG and in particular of this specific provision, the regulatory idea of which, however, also corresponds to the idea in Art. 6 (1) f) DSGVO. Here it is stipulated that processing is permitted even without consent if it is necessary to safeguard the legitimate interests of the controller (who is also protected by fundamental rights) or of a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data outweigh the interests or fundamental rights and freedoms of the data subject.
The ePrivacy Directive from 2002 and its amendment from 2009 should not be confused with the ePrivacy Regulation. On January 10, 2017, the EU Commission officially presented the draft for a new ePrivacy Regulation (ePV). The new regulation takes up and expands on the old regulatory material. In addition to the protection of the confidentiality of communications, the

ein erweiterter Endgeräteschutz. Der Entwurf wird noch immer kontrovers diskutiert. Aktuelle Informationen zum Fortschritt finden sich auf den Info-Seiten des BVDW.

focus is now primarily on extended terminal equipment protection. The draft is still being controversially discussed. Current information on progress can be found on the BVDW info pages.

Tracking Prevention über Browser // Tracking prevention with the browser

Die Idee ist nicht neu. Browser werden zunehmend zu „Gate Keepern" beim Thema Privacy. Nachdem sich in den vergangenen Jahren ein blühender Markt für Privacy-Plugins entwickelt hat, greifen die Browser nun zunehmend selbst in das Thema ein und integrieren bestimmte Funktionen direkt in den Browser. Neben Ad-Blocking wird hierbei vor allem auch auf Anti-Tracking-Features gesetzt. In der konkreten Ausprägung bedeutet das die Verhinderung von Tracking-Script-Ausführungen oder aber das Blocken von Cookies und Web Storage.

The idea is not new. Browsers are increasingly becoming "gate keepers" when it comes to privacy. After a flourishing market for privacy plug-ins has developed over the past few years, browsers are now increasingly intervening in the topic themselves and integrating certain functions directly into the browser. In addition to ad-blocking, anti-tracking features are a key factor here. In concrete terms, this means the prevention of tracking script executions or the blocking of cookies and web storage.

Safari Intelligent Tracking Protection (ITP)[10]

Safari Intelligent Tracking Protection (ITP)

Mit ITP ist Safari seit 2017 Vorreiter beim Thema 3rd Party Cookie Blocking. ITP sammelt Statistiken über Ressourcen-Ladevorgänge als auch Nutzer-Interaktionen mit Seitenelementen, ein Machine-Learning-Modell klassifiziert daraufhin diese Events, identifiziert, welche Top Level Domains/Skripte Nutzer cross-site tracken können und beginnt bei diesen das Blocken von 3rd Party Cookies.

With ITP, Safari has been a pioneer in 3rd Party Cookie Blocking since 2017. ITP collects statistics about resource loading as well as user interaction with page elements, a machine learning model then classifies these events, identifies which top level domains/scripts users can track cross-site and starts blocking 3rd party cookies.

Dabei werden drei wesentliche Muster identifiziert: Sub-Resource in Anzahl von Unique Domains, Sub-frame in Anzahl von Unique Domains und Anzahl von Unique Domain Redirections zu einem Ziel.

Three main patterns are identified: sub-resource in number of unique domains, sub-frame in number of unique domains and number of unique domain redirections to a target.

In seiner Version 1.0 (06/2017) begann Safari daraufhin den Zugriff auf 3rd Party Cookies nach 24 Stunden einzuschränken (partitioniert) und die Cookies nach 30 Tagen zu löschen.

In its version 1.0 (06/2017), Safari started to restrict (partition) access to 3rd party cookies after 24 hours and delete the cookies after 30 days.

In der Version 1.1 (03/2018) folgte die Einführung einer Storage Access API für partitionierte

Version 1.1 (03/2018) introduced a Storage Access API for partitioned cookies. Partitioned

[10] https://webkit.org/blog/category/privacy/

Cookies. Partitionierte Cookies konnten daraufhin nicht mehr persistiert werden (nur noch Session).

Seit der Version 2.0 (06/2018) wurden 3rd Party Cookies dann direkt partitioniert und nicht persistiert als auch der Zugriff nur noch auf Storage Access API eingeschränkt.

Doch die Entwicklung geht weiter. Nachdem Version 2.1 auch 1st Party Cookies mit einem Ablaufdatum von 7 Tagen versehen hatte, reduziert die Version 2.2 (04/2019) die Laufzeit der über Javascript gesetzten Cookies in der 1st Party nun auf 24 Stunden.

Firefox Enhanced Tracking Protection (ETP)

Firefox stellt bereits seit einigen Jahren mit der Möglichkeit der Plugins umfangreiche Tools zum Ad-Blocking aber auch Anti-Tracking über Dritte zur Verfügung. Als Zwischenschritt wurde auch ein Private Mode eingeführt, mit dem Passwörter, Cookies, Downloadliste oder Chronik nicht gespeichert werden.

Seit der Version v63 (10/2018) hat Firefox darüber hinaus ETP in seiner initialen Version bereitgestellt, allerdings war die Funktion per Default deaktiviert. ETP hat die Aufgabe das Blocking von “langsam ladenden Trackern” oder “Cross-Site Tracking” über 3rd Party Cookies zu verhindern. Es werden hierbei nur die Skripte betrachtet, welche in der sogenannten disconnect.me Liste auf Github[11] gepflegt werden. Hierin sind mittlerweile alle wesentlichen AdTech Marktteilnehmer enthalten.

Mit seinem Release im Juni 2019 aktivierte Firefox ETP dann für alle Neuinstallationen per Default[12]. Schlussendlich wurde mit der Version 69 im September 2019 ETP für alle Bestandsinstallationen per Default aktiviert. Mittlerweile (10/2019) werden mit jedem Firefox-Update eventuell vom User angepasste Einstellungen, die z.B. das Setzen von Cookies erlauben, wieder mit dem Browser-Update

cookies could no longer be persisted (session only).

Since version 2.0 (06/2018), 3rd party cookies were directly partitioned and not persisted and access was restricted to Storage Access API only.

But the development continues. After version 2.1 had also provided 1st Party Cookies with an expiration date of 7 days, version 2.2 (04/2019) now reduces the runtime of cookies set via Javascript in 1st Party to 24 hours.

Firefox Enhanced Tracking Protection (ETP)

Firefox has been providing extensive tools for ad-blocking but also for anti-tracking via third parties for several years with the possibility of plugins. As an intermediate step, a private mode was also introduced, with which passwords, cookies, download list or chronicle are not stored.

Since version v63 (10/2018) Firefox has also provided ETP in its initial version, but the function was disabled by default. ETP has the task to prevent the blocking of "slow loading trackers" or "cross-site tracking" via 3rd party cookies. Only the scripts that are maintained in the disconnect.me list on Github are considered. This list contains all important AdTech market participants.

With its release in June 2019 Firefox ETP is activated for all new installations by default. Finally, with version 69 in September 2019, ETP was activated by default for all existing installations. In the meantime (10/2019), with each Firefox update, any user-adapted settings, e.g. allowing the setting of cookies, are overwritten with the browser update and reset to the default settings.

[11] https://github.com/disconnectme/disconnect-tracking-protection

[12] https://blog.mozilla.org/blog/2019/06/04/firefox-now-available-with-enhanced-tracking-protection-by-default/

überschrieben und auf die Standard-Einstellungen zurückgesetzt[13].

[13] https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/