Identitätskrise

Die Zukunft des Tracking zwischen Komfort und Datenschutz

Browserhersteller, Datenschutzadvokaten, Online-Werbeunternehmen und viele weitere Interessengruppen der Web-Welt diskutieren derzeit, wie Third-Party-Cookies ersetzt werden können. Dabei stehen auch wesentlich invasivere Verfahren zur Diskussion, als es Third-Party-Cookies jemals waren.

Von Jo Bager

Safari schmeißt Third-Party-Cookies nach 24 Stunden weg; Firefox sperrt Cookies in Website-spezifische Container ein; Google wird sich vom Tracking mit Third-Party-Cookies verabschieden – das bevorstehende Ende der Cookies erschüttert die Online-Werbebranche, weil sie die Axt an eine wichtige Erlösquelle anlegt: Ein immer größerer Anteil der Online-Werbung wird als sogenanntes Programmatic Advertising vermarktet, das dem Surfer zielgenau auf ihn abgestimmte Werbung präsentiert. Dies setzt aber möglichst akkurate Nutzerprofile voraus. Um Profile anlegen zu können, müssen die Werbetreibenden den Surfer bei seinen Streifzügen im Netz wiedererkennen, wofür sie Third-Party-Cookies nutzen.

Ein für alle Seiten akzeptabler Nachfolger für Third-Party-Cookies ist noch nicht gefunden. So gut wie jede Interessengruppe hat unterschiedliche Vorstellungen, wie Tracking in Zukunft funktionieren soll, seien es Browserhersteller, Adtech-Unternehmen, Standardisierungsgremien, Werbevermarkter, Datenschützer oder die Politik: eine sehr unüberschaubare Melange sich widersprechender Interessen.

Wie über Kreuz die Vorstellungen der verschiedenen Gruppen liegen, lässt sich gut am prominentesten Vorschlag festmachen: Googles FLoC (Federated Learning of Cohorts). Dabei wertet der Browser aus, welche Sites der Nutzer besucht, und weist ihn daraufhin einer Werbe-Kohorte von mehreren Tausend Nutzern zu.

Das soll keine Rückschlüsse auf den einzelnen Nutzer zulassen, aber dennoch zielgruppengenaue Werbung ermöglichen – grundsätzlich eine deutliche Verbesserung beim Datenschutz im Vergleich zu Cookies. Google testet das neue Verfahren bereits bei einem kleinen Nutzerkreis, allerdings nicht im Geltungsbereich der DSGVO.

Facebook hat sich kürzlich in einem Hintergrundgespräch positiv zu FLoC geäußert und will den Vorschlag offenbar unterstützen. Viele andere Unternehmen und Interessenvertreter lehnen FLoC dagegen ab. Die Browserhersteller Mozilla, Microsoft, Apple, Vivaldi und Brave wollen FLoC in ihren Browsern nicht umsetzen, ihnen geht der Datenschutz nicht weit genug. Das sagt auch die Bürgerrechtsorganisation Electronic Frontier Foundation. Sie befürchtet, dass sich auch bei FLoC einzelne Nutzer identifizieren lassen.

Kein vollwertiger Ersatz

In der Online-Marketing- und Adtech-Branche herrscht eine große Unsicherheit, weil durch einen Umstieg auf FLoC ganze Branchenzweige wegfallen könnten – zum Beispiel diejenigen Anbieter, die beim Programmatic Advertising dabei zusammenspielen, dem Nutzer passende Werbung zuzuordnen.

Viele Werbeunternehmen sehen es zudem kritisch, dass der Werberiese Google mit FLoC in seinem Browser Chrome auch die technische Ausgestaltung der Werbeauslieferung kontrollieren würde. Das hat die britische Aufsichtsbehörde Competition and Markets Authority (CMA) auf den Plan gerufen, die die Neuerungen in Chrome untersucht.

Darüber hinaus gibt es Kritik aus der Branche, weil sich mit FLoC nicht alle Anwendungsszenarien abdecken lassen, für die bisher Cookies zum Einsatz kamen. Es ist zum Beispiel unklar, wie sich mit FLoC Provisionen für Affiliate-Werbung zuordnen oder Retargeting verwirklichen lassen sollen. Letzteres ist die Werbeform, die einen im Netz verfolgt: Hat man sich einmal für Drucker interessiert, bekommt man per Retargeting tage- oder wochenlang Druckerwerbung angezeigt.

Bei beiden Verfahren geht es ja letztendlich darum, einen einzelnen Nutzer über einen längeren Zeitraum wiederzuerkennen, um ihm personalisierte Werbung zu präsentieren beziehungsweise einem Affiliate-Werbepartner eine Provision zukommen zu lassen. Auch setzen einige Lösungen gegen sogenanntes Ad Fraud, also den „Abrechnungsbetrug“ zum Beispiel mit automatischen Klicks auf Anzeigen, auf Cookies.

Es verwundert daher nicht, dass es diverse Alternativvorschläge zu FLoC gibt, unter anderem von Apple und Microsoft. Von Google selbst stammt noch ein weiterer Vorschlag namens Fledge. Wie Branchendienste berichten, soll auch Amazon an einer Alternative zu FLoC arbeiten.

Kommt der „First-Party“-Datenabfluss?

Bei Unternehmen und Publishern stehen Alternativen hoch im Kurs, die unter dem Oberbegriff „First Party Data“ zusammengefasst werden. Das ist ein Euphemismus: Die First Parties, also zum Beispiel die Websites, die ein Surfer besucht, sollen die

Daten ihrer Besucher festhalten – und sie an einen zentralen Server übertragen.

Es wird also wie bei den Third-Party-Cookies eine oder mehrere zentrale Stellen geben, die Nutzerdaten Site-übergreifend einsammeln und speichern. Statt eines Third-Party-Cookies, das den einzelnen Surfer wiedererkennbar macht, kommt stattdessen ein anderer Identifier zum Einsatz, den alle teilnehmenden Websites benutzen.

Konkret lässt sich die Funktionsweise einer solchen First-Party-Strategie am besten am Beispiel von Unified ID fassen (UID). Diese Lösung wurde ursprünglich von der Werbeplattform The Trade Desk entwickelt. Mittlerweile hat es seine Spezifikationen in Version 2.0 (UID2) als Open Source auf GitHub veröffentlicht und die Kontrolle an eine Arbeitsgruppe des International Advertising Bureau (IAB) übergeben. Der Wirtschaftsverband IAB sorgt für die Standardisierungen in der Werbebranche. Unter seiner Federführung soll aus Unified ID ein Industriestandard entstehen. The Trade Desk konnte schon Dutzende Partner von Unified ID überzeugen.

Im einzelnen läuft ein typischer Anwendungsfall so ab wie in der Grafik rechts. Damit die First-Party-Site den Anwender (wieder-)erkennen kann, muss er dort eingeloggt sein, zum Beispiel mit seiner E-Mail-Adresse oder seiner Mobilfunknummer. Der Entwurf für den Standard spricht hier Personally Identifiable Information (PII).

Der Website-Betreiber sendet die PII an einen UI Operator, der dazu ein Token zurückliefert, das den Besucher eindeutig identifiziert. Dieses Token speichert der Website-Betreiber in der Folge im Browser des Nutzers oder in einer App als First-Party-Cookie. Es lässt sich dann wie ein Third-Party-Cookie verwenden, um dem Nutzer wiederzuerkennen und ihm zielgerichtet Werbung zukommen zu lassen.

Third-Party-Cookies sind mit einem einzelnen Browser assoziiert. UID2s dagegen, warnt die EFF, „sind mit Personen verbunden, nicht mit Geräten. Das bedeutet, dass ein Werbetreibender, der UID2 von einer Website sammelt, diese mit den UID2s verknüpfen kann, die er über Apps, verbundene Fernsehgeräte und verbundene Fahrzeuge sammelt, die derselben Person gehören.“ Es gebe zudem noch eine Reihe offener Fragen zu UID2, zum Beispiel, wer eigentlich die UID-Dienste betreibt und welche Pflichten den Teilnehmern in Bezug auf die Nutzerdaten auferlegt werden.

Werbeunternehmen trommeln derzeit mit Verve für Unified ID und ähnliche First-Party-Rezepte und versuchen, sie Publishern und anderen Website-Betreibern schmackhaft zu machen. Eher im Stillen dürften sie wohl auch vermehrt andere Trackingverfahren ausbauen, etwa das Browser-Fingerprinting.

Immerhin gibt es stellenweise Gegenbewegungen zur immer größeren Datengier der Online-Werber. Einige Medien haben erkannt, dass nicht jeder Surfer getrackt werden will und bieten sogenannte Pur-Abos an. Für ein paar Euro im Monat erhält man Zugriff auf die Inhalte ohne eingebundenes Tracking und mit sehr viel weniger oder komplett ohne Werbung.

Ein weiterer kleiner Hoffnungsschimmer am Horizont: Einige Medien experimentieren mit Werbeformen, die ohne externe Daten auskommen, die New York Times etwa. Aber solche Vorhaben sind eher die Ausnahme als die Regel. Es ist fraglich, ob sich so etwas auf breiter Basis durchsetzen kann. Kleinere Publisher werden sich kaum eine Datenabteilung, wie sie für die Werbeaussteuerung notwendig ist, leisten können wie die New York Times.

Fazit

FLoC, First Party, Fingerprinting: Es ist noch nicht abzusehen, welche Technik an Stelle der Cookies treten werden – möglicherweise alle parallel. FLoC ist dabei am unkritischsten. Es schützt den Nutzer besser als bisher und es wird für den Nutzer sicherlich Wege geben, die Zuordnung zu Kohorten ganz abzuschalten.

First-Party-Data-Lösungen laufen aus Nutzersicht auf eine Verschlechterung hinaus. Es bleibt abzuwarten, ob technische Mittel alleine helfen werden, sie zu blockieren. Es ist auf jeden Fall eine gute Wahl, den Browser auch heute bereits hochzurüsten, um die eigenen Daten so gut wie möglich zu schützen, indem man zum Beispiel Third-Party-Tracking so gut es geht blockiert. *(jo@ct.de)* **ct**

Weitere Dokumentationen: ***ct.de/ymzq***

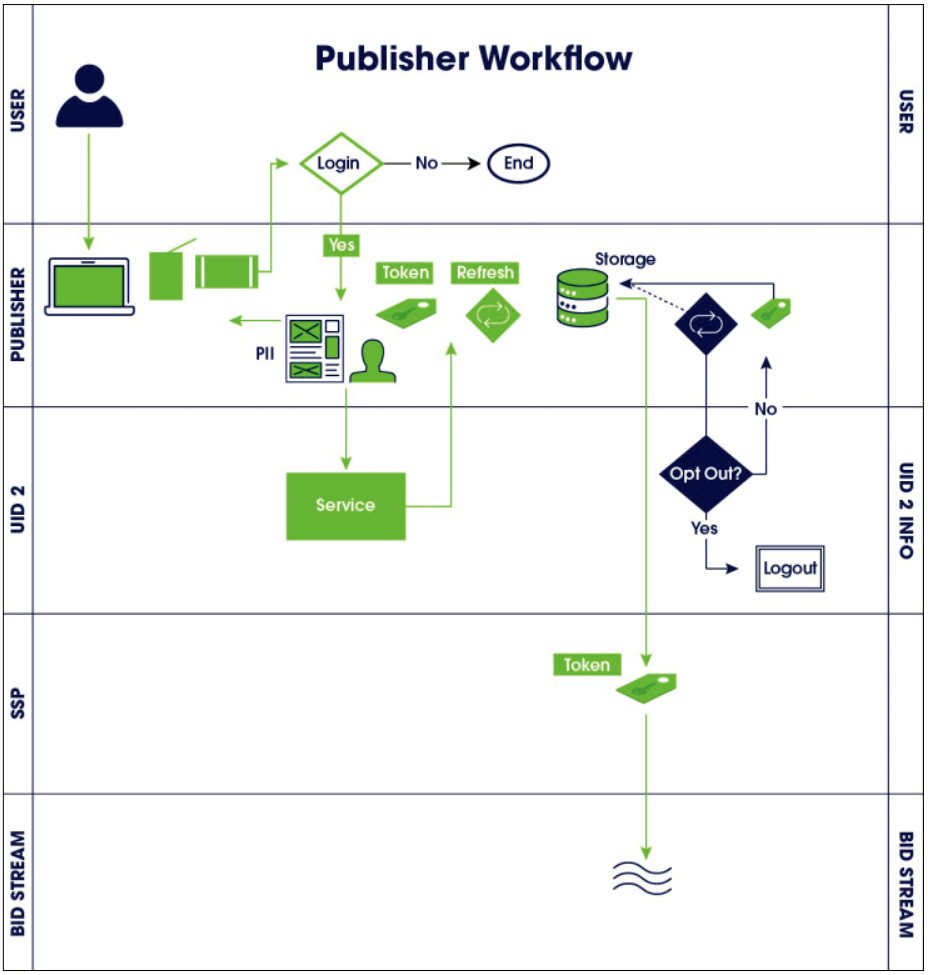

Bild: github.com/UnifiedID2/uid2docs

Unified ID verwendet Token, die auf personenbeziehbare Informationen (PII) aufsetzen, zum Beispiel E-Mail-Adressen oder Telefonnummern.