MMR
Zeitschrift für IT-Recht und Recht der Digitalisierung

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

CHRISTIAN-HENNER HENTSCH / KONSTANTIN EWALD / ROLF SCHWARTMANN (Hrsg.)

Datenschutz in der Games-Branche. Datenschutzrechtliche Voraussetzungen für ein interaktives Spielerlebnis

Osborne Clarke
Kölner Forschungsstelle für Medienrecht
Technology Arts Sciences TH Köln
game Verband der deutschen Games-Branche

MMR-Beilage
8/2021

Seiten 1–32
24. Jahrgang · 16. August 2021
Verlag C.H.BECK München

1830202108

PATRICK MITSCHING / CHRISTIAN RAUDA

Zeitenwende beim Tracking des Nutzungsverhaltens durch Spiele-Apps

Bedeutung von Apples App Tracking Transparency Framework (ATT-Framework) für Spiele-Entwicklerstudios aus datenschutzrechtlicher Perspektive

Benutzer- und Gerätedaten

Der Beitrag widmet sich der datenschutzrechtlichen Einordnung des im April 2021 auf Apple-Geräten ab iOS 14.5 eingeführten App Tracking Transparency-Framework (ATT-Framework). Obgleich Apple kein Gesetzgeber und das ATT-Framework kein Gesetz ist, stellt ATT doch eine faktisch Rechtssetzung mittels globaler Plattform-AGB gegenüber Spiele-Entwicklerstudios und Spieler*innen dar. Erstmalig wird für mobile Endgeräte eines Herstellers ein unumgänglicher Mechanismus geschaffen, um von Spieler*innen die Erlaubnis für das Tracking über die Spiel-App hinaus in anderen Apps und Websites einzuholen. Dies hat weitreichende Folgen vor allem für die Bewerbung und Monetarisierung von Spiele-Apps, die auf Tracking angewiesen sind. Lesedauer: 18 Minuten

I. Einleitung

Apple hat die Welt der App-Entwicklerstudios ins Wanken gebracht. In den Betriebssystemen iOS 6 bis iOS 13 hatten sie freien Zugriff auf die eindeutige Werbe-ID des Apple-Geräts (IDFA). Die IDFA ist eine jedem Apple-Gerät innewohnende eindeutige und weltweit gültige Identifikationsnummer bestehend aus 32 Zeichen (z.B. EA7583CD-A667-48BC-B806-42ECB2B48606). Der Nutzer hatte die Möglichkeit, den Zugriff durch Modifikationen in den Datenschutzeinstellungen zu ändern und konnte zunächst die IDFA zurücksetzen oder sperren. Seit iOS 14 war ein Zurücksetzen nicht mehr möglich, man konnte den Zugriff auf die IDFA allerdings manuell ganz sperren, indem man den Menüpunkt „Apps erlauben, Tracking anzufordern" deaktivierte. Viele Nutzer*innen hatten von dieser Option allerdings keine Kenntnis. Dies führte dazu, dass die Mehrheit der Nutzer*innen ohne Weiteres „trackbar" waren. *Apple* hat nun die Möglichkeit des Trackings eingeschränkt und dafür viel Lob von Datenschützer*innen geerntet, sich aber auch viel Kritik ausgesetzt. Unter der Flagge des Datenschutzes verfolgt *Apple* nämlich durchaus eigene wirtschaftliche Interessen.

II. App Tracking Transparency Framework

Mit dem Update des Betriebssystems iOS auf die Version 14.5 am 26.4.2021 wurde das sog. App Tracking Transparency Framework (ATT-Framework) eingeführt. *Apple* schreibt nun vor, dass App-Entwicklerstudios das ATT-Framework verwenden müssen, wenn ihre App Daten über Endbenutzer*innen sammeln und diese mit anderen Unternehmen zum Zweck des Trackings über Apps und Websites hinweg teilen. Dieses Zusammenführen geschieht regelmäßig in zwei Fällen: Wenn der App-Entwickler bei einem digitalen Werbeunternehmen Werbung für seine eigene App schaltet (Nutzergewinnung). Oder wenn der App-Entwickler Werbefläche in seiner App an Werbeunternehmen gegen Entgelt zur Verfügung stellt (Werbevermarktung). In beiden Fällen tauschen der App-Entwickler und das Werbeunternehmen die IDFA erfolgreich geworbener Nutzer*innen aus (Attribution). Dies ermöglicht eine klare Messung und Vergütung des Werbeerfolgs. Es wird i.Ü. Betrug verhindert. Andernfalls bestünde die Gefahr, dass der App-Entwickler für die Gewinnung von fiktiven Nutzer*innen bezahlt, also Nutzer*innen, die ihm durch das Werbeunternehmen gar nicht zugeführt wurden (Werbebetrug).

III. Was ist für Apple „Tracking"?

Unter „Tracking" versteht *Apple* die Verknüpfung von Benutzer- oder Gerätedaten, die von den Apps, Websites oder Offline-Eigenschaften anderer Unternehmen gesammelt wurden, um gezielte Werbung oder Werbemessung zu betreiben. Tracking bezieht sich auch auf die Weitergabe von Benutzer- oder Gerätedaten an Datenbroker[1]. *Apple* nennt auch Beispiele für Tracking, nämlich

- Anzeigen von gezielter Werbung in der App, die auf Benutzerdaten basiert, die von Apps und Websites anderer Unternehmen gesammelt wurden.
- Teilen von Gerätestandortdaten oder E-Mail-Listen mit einem Datenbroker.
- Weitergabe einer Liste von E-Mails, Werbe-IDs oder anderen IDs an ein Werbenetzwerk eines Drittanbieters, das diese Informationen verwendet, um diese Nutzer*innen in den Apps anderer Entwickler erneut anzusprechen oder ähnliche Benutzer*innen zu finden.
- Platzieren eines Software Development Kit (SDK) eines Drittanbieters in der App, das Nutzerdaten aus der App mit Nutzerdaten aus den Apps anderer App-Entwickler kombiniert, um Werbung gezielt zu platzieren oder die Werbeeffizienz zu messen, auch wenn das SDK nicht für diese Zwecke verwendet wird.

Nicht als Tracking eingeordnet wird dagegen, wenn Benutzer- oder Gerätedaten aus der App ausschließlich auf dem Gerät der Nutzer*innen mit Daten Dritter verknüpft werden und nicht auf eine Weise vom Gerät gesendet werden, die die Nutzer*innen oder das Gerät identifizieren kann oder wenn ein Datenbroker, mit dem Daten geteilt werden, die Daten ausschließlich zur Betrugserkennung, Betrugsprävention oder zu Sicherheitszwecken und ausschließlich im Namen des App-Entwicklers verwendet.

IV. Implementierung des ATT-Framework

Technisch setzt die Implementierung des ATT-Framework voraus, dass App-Entwicklerstudios einen von *Apple* vorgegebenen und für alle Apps einheitlichen Programmcode in ihre App einbauen. Dieser Code führt beim Start der App zur Anzeige eines Systemdialogs („ATT-Prompt"). In diesem ATT-Prompt wird der Nutzer um Erlaubnis dafür gebeten, dass „die App ihre Aktivitä-

1 https://developer.apple.com/app-store/user-privacy-and-data-use/.

ten in Apps und auf den Websites anderen Unternehmen erfassen" darf. Außerdem muss vom App-Entwickler eine Beschreibung des Grunds für das Tracking angezeigt werden (usage-description string). Die Nutzer*innen der App sind frei darin, ob sie die Erlaubnis erteilen oder nicht. *Apple* weist darauf hin, dass die App beim ersten Start durch einen Nutzer abstürzen kann, sofern kein usage-description string implementiert ist. Nachdem der Nutzer die Erlaubnis erteilt oder verweigert hat, speichert die App dies (Tracking-Autorisierungsstatus). Der App-Entwickler hat insofern nur einen „Schuss", um eine Erlaubnis zu erhalten. Dies hat dazu geführt, dass viele App-Entwickler nach Einführung des ATT-Framework erst einmal abgewartet haben und zunächst kein ATT-Prompt aktiviert haben.[2] Wenn der Nutzer der App ihre Erlaubnis nicht gibt, kann der App-Entwickler nicht erneut um Erlaubnis fragen. Der Nutzer muss vielmehr in den Systemeinstellungen aktiv die Erlaubnis zu Gunsten des App-Entwicklers erteilen. *Apple* verbietet es App-Entwickler, die Regelung des „einen Schusses" zu umgehen. So ist es etwa verboten, dem nativen ATT-Prompt ein eigenes Fenster vorzuschalten, in dem die Nutzer*innen „Ich entscheide mich später" auswählen und so die Entscheidung zurückstellen können. Auch ist es verboten, die Nutzung der App an die Erteilung der Erlaubnis zu koppeln (gating) oder durch Anreize wie z.B. Gratisleistungen oder Rabatte die Erteilung der Erlaubnis attraktiver zu gestalten (incentivization).[3]

Für Nutzer*innen gibt es wenig erkennbare Anreize, einem Tracking zuzustimmen. Vielen Nutzer*innen ist nicht einmal klar, dass es einen Unterschied zwischen Tracking im Internet und dem Anzeigen von Werbung gibt. Die Verweigerung der Erlaubnis in das Tracking verhindert nämlich natürlich nicht, dass den Nutzer*innen Werbung angezeigt wird. Ohne Tracking ist die angezeigte Werbung nur nicht mehr auf die Nutzer*innen zugeschnitten. Dies kann z.B. dazu führen, dass Veganer*innen Fleischprodukte angeboten werden oder Männern Hygieneartikel für Frauen. Dass Tracking also auch Vorteile für die Nutzer*innen hat, ist kaum jemandem klar. Dies führt dazu, dass viele die Erlaubnis verweigern werden. Historisch betrachtet waren vor der ATT-Einführung im April 2021 ca. 90% aller IDFA frei verfügbar, da nur wenige Nutzer*innen das Tracking in den Systemeinstellungen deaktivierten. Neueste Erhebungen seit der ATT-Einführung ab Juni 2021 deuten darauf hin, dass sich die effektive IDFA-Verfügbarkeitsquote abhängig von App-Kategorie und geografischer Region bei 15 bis 20% oder weniger einpendelt.[4] Die Folge davon für die App-Entwickler sind hohe Streuverluste bei der Nutzergewinnung und sinkende Werbeeinnahmen bei der Werbevermarktung. Denn der Vorteil von Online-Werbung gegenüber etwa Außen- oder Fernsehwerbung liegt darin, dass die Zielgruppe viel genauer identifiziert und angesprochen werden kann. Damit werden Streuverluste minimiert und die Bereitschaft der Hersteller und Händler erhöht, hohe Preise für gezielte Werbung auszugeben. Die mit Abstand größten Werbeunternehmen *Facebook* und *Google* behaupten, dass die Einnahmen von Werbeflächenanbietern – hier: App-Entwicklern – ohne personalisierte Werbung um 50% (Angabe von *Facebook*) bzw. 52-64% (Angabe von *Google*) zurückgehen würden.[5] Diese Größenordnung wird auch von deutschen Werbeverbänden in deren aktueller ATT-Kartellbeschwerde gegen *Apple* vor dem *Bundeskartellamt* angeführt.[6] Allerdings ist zu beachten, dass unabhängige empirische Studien einen deutlich geringeren Rückgang der Einnahmen prognostizieren, nämlich um nur ca. 4%.[7] Spiele-Entwicklerstudios, die in ihren Spielen überwiegend nur noch Werbung anbieten können, welche nicht auf die Interessen des Nutzers zugeschnitten sind, erlösen also weniger Werbeeinnahmen.

V. Datenschutzrechtliche Einordnung

1. Einordnung der ATT-Erlaubnis als Einwilligung

Ob es sich bei der von dem Entwickler über das ATT-Framework erbetene „Erlaubnis" um eine Einwilligung im datenschutzrechtlichen Sinne handelt, ist umstritten. Die Frage hat Relevanz für das Ausspielen von Werbung an Nutzer*innen auf anderen Geräten und Plattformen, insbesondere solchen außerhalb von *Apples* digitalem Ökosystem.

Nach der Einwilligungs-Theorie kann es sich bei der angeforderten Erlaubnis um eine Einwilligung i.S.d. Art. 6 Abs. 1 lit. a DS-GVO handeln, die sich insgesamt auf die Befugnis zum Tracking durch den App-Entwickler bezieht.[8] Demnach messen die Nutzer*innen dem ATT-Prompt eine rechtliche Qualität zu und entscheiden gegenüber dem App-Entwickler, ob sie mit einem Tracking über alle Geräte und Plattformen hinweg einverstanden sind, auf denen das Spiel angeboten wird. Dafür spricht, dass *Apple* in seiner ATT-Richtline der Entscheidung des Nutzers über Erlaubnis oder Verweigerung des Trackings eine sehr umfassende Geltung beimisst, die sich abstrakt auf die „App" als universelles Produkt bezieht, welche auf verschiedenen Geräten und Plattformen genutzt werden kann.[9]

Die Gegenmeinung vertritt die Gerätespezifische Theorie. Danach handele es sich bei der Erteilung oder Verweigerung der Erlaubnis um eine reine Geräteeinstellung, die keine allgemeine Rechtsqualität aufweist und damit auch keine Rechtswirkung gegenüber dem App-Entwickler entfaltet.[10] Die Nutzer*innen verstünden das ATT-Prompt als reine Abfrage einer nur für dieses eine Gerät gültigen Systemeinstellung. Eine DS-GVO-konforme Einwilligung liege nicht vor, weil schon die Aufklärungspflichten aus Art. 7 DS-GVO nicht erfüllt seien, da im ATT-Prompt nicht auf die Datenschutzerklärung verlinkt werden kann.[11] Die Nutzer*innen verbieten damit dem App-Entwickler nicht das Tracking jenseits des konkreten *Apple*-Geräts, auf dem die Einstellung vorgenommen werde.

Welcher Meinung man folgt, hat weitereichende Konsequenzen in Bezug auf Spiele, die auf mehreren Geräten und Plattformen gespielt werden können (Cross-Plattform-Spiele). Cross-Plattform-Spiele zeichnen sich dadurch aus, dass sie auf unterschiedlichen Endgeräten und Betriebssystemen genutzt werden

2 https://www.businessinsider.com/why-you-are-not-seeing-ios-145-privacy-pop-ups-2021-4; https://www.fastcompany.com/90632354/ios-14-5-privacy-pop-up-requests-not-showing-up.

3 S. Fußn. 1.

4 *Flurry*: 15%, abrufbar unter: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/; *Singular*: 20%, abrufbar unter: https://www.singular.net/blog/ios-14-5-by-the-numbers-adoption-att-permission-ad-spend-trends-install-volume-impact-on-android-vs-ios/.

5 *Facebook*: -50%, abrufbar unter: https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem/; *Google*: -52-64%, abrufbar unter: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf.

6 *Pettinger*, Zwingt Apples Datenschutz Unternehmen in die Knie?, abrufbar unter: https://www.dr-datenschutz.de/zwingt-apples-datenschutz-unternehmen-in-die-knie/.

7 *Marotta* et al., Online Tracking and Publisher's Revenues: An Empirical Analysis, abrufbar unter: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

8 *Obereck/Frank*, iOS 14.5 – Apple gibt Nutzern Wahlrecht bei App-Tracking, abrufbar unter: https://www.datenschutzkanzlei.de/ios-14-5-apple-gibt-nutzern-wahlrecht-bei-app-tracking/; *Isaacson*, Apple iOS14 Changes: „Your App" May No Longer Mean „Your Data", abrufbar unter: https://www.adexchanger.com/data-driven-thinking/apple-ios14-changes-your-app-may-no-longer-mean-your-data-2/.

9 S. Fußn. 1.

10 Apples ATT: Was es bedeutet, wenn kaum einer Tracking will, abrufbar unter: https://www.dr-datenschutz.de/apples-att-was-es-bedeutet-wenn-kaum-einer-tracking-will; *McChannel*, Be Cautious App Developers: ATT and GDPR are not the same, abrufbar unter: https://appgrowthsummit.com/be-cautious-app-developers-att-and-gdpr-are-not-the-same/.

11 S. Fußn. 10.

können. Wer also ein Spiel mobil im Zug gespielt hat, kann nach der Ankunft zuhause dieselbe Partie nahtlos auf dem heimischen PC weiterspielen. Spielt ein Nutzer das Cross-Plattform-Spiel „Forge of Empires" auf seinem iPhone, iPad und PC, kann die Tracking-Erlaubnis durchaus auseinanderfallen. Für das iPhone hat er etwa das Tracking abgelehnt, für das iPad hat er das Tracking akzeptiert und für den PC wurde er zum Tracking gar nicht gefragt, da dieser nicht das Betriebssystem iOS nutzt und somit dort das ATT-Framework nicht existiert.

Für die Gerätespezifische Theorie spricht, dass Nutzer*innen bei der Auswahl im ATT-Prompt nur das konkrete Gerät vor Augen haben, das sie gerade nutzen. Sie machen sich keine Vorstellungen darüber, ob die Erlaubnis irgendeine Auswirkung auf die Nutzung des Spiels auf anderen Geräten oder Plattformen haben könnte. Eine andere Ansicht ist praxisfern und konstruiert einen Rechtswillen, den die Nutzer*innen nicht haben. Allerdings missversteht die Gerätespezifische Theorie, dass der Nutzerentscheidung sehr wohl eine Rechtsqualität bezogen auf das betroffene Gerät innewohnt: Die Nutzer*innen bringen durch ihre Auswahl im ATT-Prompt zum Ausdruck, dass sie mit Tracking einverstanden oder nicht einverstanden sind. Die Abfrage im ATT-Prompt geschieht in bewusst einfacher und klarer Sprache, so wie es u.a. Erwägungsgrund 58 DS-GVO erfordert. Die Datenschutzerklärung können die Nutzer*innen unkompliziert vor oder während der Installation auf der App-Store-Seite der App nachlesen. An den Inhalt und Umfang des ATT-Prompts sollten insofern keine überzogenen Forderungen gestellt werden – das ATT-Prompt ist deutlich und warnend. Überzeugend ist es daher, die Gerätespezifische Theorie so zu modifizieren, dass sie eine gerätebezogene Einwilligung im ATT-Prompt ermöglicht.

Unter datenschutzrechtlichen Gesichtspunkten ist die Implementierung einer solchen dem Tracking vorgeschalteten Erlaubnis mit Einwilligungscharakter zu begrüßen.

2. Einordnung der IDFA als personenbezogenes Datum nach DS-GVO

Die IDFA ermöglicht die Verknüpfung mit weiteren personenbezogenen Daten, durch die ein Personenbezug hergestellt werden kann, nicht jedoch mit dauerhaft dem Gerät zugeordneten Daten.[12] In der Praxis ist die IDFA in ihrer Funktion einem Cookie sehr ähnlich: Der im Browser gesetzte Cookie erlaubt ebenso wie die im iOS-Betriebssystem vergebene IDFA eine Nachverfolgung des Nutzerverhaltens. So wie der Cookie die von Nutzer*innen aufgerufenen Websites und dortigen Eingaben protokolliert, werden anhand der IDFA die von Nutzer*innen aufgerufenen Apps und Websites und darin getätigten Handlungen protokolliert. Ein technischer Unterschied besteht nur darin, dass der Cookie manuell vom Website-Anbieter in den Quellcode seiner Website eingebunden werden muss, während die IDFA bereits im iOS-Gerät ab Werk vorhanden ist. Letztlich werden die aus Cookie-Setzung und IDFA-Zuordnungen erhobenen Daten gleichrangig wie Wirtschaftsgüter gehandelt: Ein Website- oder App-Anbieter, der Trackingdaten zu Nutzungs- und Kaufverhalten liefern kann, erhält von Werbeunternehmen eine erheblich höhere Werbevergütung als ein Anbieter, der keine Trackingdaten bereitstellen kann oder will. In der Werbebranche werden Cookies und IDFA einheitlich als „audience identifiers" behandelt, wobei Cookies für den Bereich „Web" und IDFA für den Bereich „Non-Web" relevant sind.[13]

Es ist immer noch umstritten, ob die IDFA als personenbezogenes Datum unter der DS-GVO einzuordnen ist. Erwägungsgrund 30 DS-GVO legt fest, dass Personen „unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet" werden. Dies könne dann „Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren". Zwar konnte man die IDFA zunächst zurücksetzen oder deaktivieren und seit iOS 13 ausschalten (Limited Ad Tracking – LAT). Wird dies indes nicht getan, spricht viel dafür, die IDFA als personenbezogenes Datum anzusehen.[14]

3. Einordnung der IDFA als geschützte Information nach ePrivacy-RL

Nachdem der *EuGH* in der Rs. Planet49[15] entschieden hat, dass bei der Nutzung von Cookies auf Webseiten grundsätzlich eine Einwilligung erforderlich ist, stellt sich natürlich die Frage, wie dies bei anderen Tracking-Technologien zu beurteilen ist. Die IDFA ist praktisch für iOS-Mobilgeräte das, was Cookies für Websites sind. Cookies waren deswegen jahrelang so umstritten, weil durch sie Tracking von Nutzer*innen beim Surfen von Website zu Website möglich wurde, was wiederum Profilbildung und damit gezielte Werbung ermöglichte. Bei Mobilgeräten ersetzen Werbe-IDs (u.a. IDFA) die dort technisch bedingt nicht vorhandenen Cookies praktisch vollständig und ermöglichen das Tracking von Nutzer*innen bei Interaktion in den verschiedenen Apps und Websites, sodass auch dort Profilbildung und gezielte Werbung möglich werden. Als Faustregel gilt, dass man bei der Nutzung solcher Technologien immer dann eine Einwilligung braucht, wenn dies nach der ePrivacy-Richtlinie (ePrivacy-RL) vorgesehen ist.

Art. 5 Abs. 3 ePrivacy-RL befasst sich mit der „Speicherung von Informationen oder dem Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind." Es muss sichergestellt sein, dass Nutzer*innen auf die Möglichkeit hingewiesen werden, diese Verarbeitung zu verweigern. In der Planet49-Entscheidung macht der *EuGH* deutlich, dass das Einwilligungserfordernis in Art. 5 Abs. 3 S. 1 ePrivacy-RL unabhängig davon gelte, ob es sich bei den in einem Cookie gespeicherten Informationen um personenbezogene oder um anonyme Daten handele. Auch Art. 5 Abs. 2 ePrivacy-RL setze nicht voraus, dass sich die Speicherung oder der Zugriff auf personenbezogene Daten beziehen müsse.[16] Es gehe um den Schutz von sämtlichen in Endgeräten von Nutzer*innen gespeicherte Informationen, ohne dass dabei zwischen personenbezogenen und anderen Informationen zu differenzieren sei.[17]

Da die IDFA im Gerät des Nutzers gespeichert wird, bedarf es also einer Einwilligung. In diesem Zusammenhang ist auch zu beachten, dass der *Bundestag* am 20.5.2021 den Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) verabschiedet hat. § 25 TTSDG-E soll Art. 5 Abs. 3 ePrivacy-RL umsetzen. Nach der Vorschrift soll die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig sein, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Regelung orientiert sich unmittelbar am Wortlaut der europäischen Vorgaben.[18] § 25 TTDSG-E soll laut der Begründung des Regierungsentwurfs indes nur auf nicht-perso-

12 *Koreng/Lachenmann*, Formularhdb. Datenschutzrecht, 2018, F. I. 2. Rn. 7.
13 https://support.google.com/admanager/answer/6280452?hl=en.
14 *Weichert*, SVR 2014, 201 (204); *Hoffmann*, MMR 2013, 631 (634).
15 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
16 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
17 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
18 *Schwartmann/Benedikt/Reif*, MMR 2021, 99.

nenbezogene Daten Anwendung finden, in Bezug auf personenbezogene Daten sei die DS-GVO einschlägig.

VI. Kritik am ATT-Framework

Die Einführung von *Apples* ATT-Framework wurde u.a. von *Facebook* und Werbeverbänden stark und öffentlichkeitswirksam kritisiert mit dem Argument, dass *Apple* die Entwickler von Apps dazu zwinge, von Werbung auf Abomodelle und In-App-Käufe umzustellen, an denen *Apple* mitverdient. In Frankreich legten die Werbeverbände eine Beschwerde bei der Kartellbehörde ein, die jedoch erfolglos blieb.[19] In Deutschland legten die Werbeverbände ebenfalls Beschwerde beim *Bundeskartellamt* ein, über die zum Zeitpunkt der Schriftlegung noch nicht entschieden ist.[20] *Apple* erhebt auf alle im App-Store im B2C-Verhältnis erworbenen Abos und In-App-Käufe mit wenigen Ausnahmen eine Gebühr von 30% des Transaktionsvolumens. Demgegenüber profitiert *Apple* von werbefinanzierten Apps nicht, da die Werbevergütung im B2B-Verhältnis zwischen App-Entwickler und Werbeanbieter außerhalb des App-Stores abgewickelt wird.[21] Zudem wird *Apple* vorgeworfen, selbst verstärkt Werbeplätze in den Suchergebnislisten im App-Store verkaufen zu wollen, analog zu *Googles* erfolgreichen Werbeplätzen neben den Suchergebnissen bei Google Search.[22] *Apple* gehe es also im Kern nicht um den Datenschutz, sondern um die Erhöhung der eigenen Umsätze und die Ausweitung seiner Kontrolle über die App-Entwickler.

Apple hat nämlich parallel zur ATT-Einführung seine eigenen Werbeflächen im App-Store stark ausgebaut.[23] Dort verarbeitet *Apple* die im eigenen iOS-Ökosystem erhobenen First-Party-Daten für Werbeplätze, die Dritte buchen können. Eine gezielte Ansprache einzelner Nutzer*innen ist zwar nicht möglich, allerdings eine Ansprache von Kohorten ab 5.000 Personen, bei denen die Einzelpersonen ähnliche Merkmale aufweisen.[24] Somit wird letztlich das individuelle Tracking durch ein neues Kohorten-Tracking ersetzt. Noch anspruchsvollere Ansätze sind die AI-basierte Auswertung von Nutzerverhalten mittels „Differential Privacy" und „Federated Learning", die etwa bei der Personalisierung von *Apples* Sprachassistent Siri eingesetzt werden.[25] Zu beachten ist allerdings, dass auch ein solches Kohorten-Tracking der DS-GVO unterliegt, solange Daten in diesem Rahmen auf einzelne Personen rückbezogen werden können. Da *Apple* diesen „Datenschatz" mit niemandem teilen muss, ist er besonders wertvoll. Sog. „First-Party-Tracking" ist gegenüber „Third-Party-Tracking" privilegiert.[26] *Schwartmann* bezeichnete *Apple* daher als „selbsternannten Zöllner mit Eigeninteressen"[27].

VII. Fazit

Die Spiele-Entwicklerstudios müssen ihre Herangehensweise bei der Nutzergewinnung und Werbevermarktung innovativ verändern. Der Trend geht dahin, nicht mehr das Verhalten einzelner Nutzer*innen zu erfassen, sondern auf der Ebene von Nutzergruppen mit gemeinsamen Merkmalen (Kohorten) aggregierte Daten zu erheben. Zudem ist eine Abkehr vom Tracking anhand deterministischer Marker wie Werbe-IDs hin zu Annahmen auf Grund probabilistischer Marker wie Gerätetyp, Nutzungszeitpunkt und Werbekontext zu erwarten. Parallel wird der Wert von First-Party-Daten bei Entwicklerstudios und Werbeunternehmen zunehmen, da Third-Party-Daten auf Grund fehlender Tracking-Einwilligungen nicht mehr beliebig erhoben und ausgetauscht werden können. Dies wird zu verstärkter vertikaler Integration von Entwicklerstudios und Werbeunternehmen führen, um einen gemeinsamen Bestand an First-Party-Daten aufzubauen. Die weitere Entwicklung wird auch Aufschluss darüber geben, wie abhängig Spiele-Entwicklerstudios und Werbewirtschaft tatsächlich vom Tracking individueller Nutzer*innen sind.

Schnell gelesen ...

- Unter „Tracking" versteht Apple die Verknüpfung von Benutzer- oder Gerätedaten, die von den Apps, Websites oder Offline-Eigenschaften anderer Unternehmen gesammelt wurden, um gezielte Werbung oder Werbemessung zu betreiben.
- Der App-Entwickler muss einen von Apple vorgegebenen und für alle Apps einheitlichen Programmcode (App Tracking Transparency Framework – ATT-Framework) in seine App einbauen. Durch diesen wird eine Erlaubnis zum Tracking abgefragt. Die effektive Erlaubnisrate zum Tracking bei Spiele-Apps liegt inzwischen nur noch bei ca. 15-20%. Die Folge davon für die Spiele-Entwicklerstudios sind hohe Streuverluste bei der Nutzergewinnung und sinkende Werbeeinnahmen bei der Werbevermarktung.
- Bei der Erteilung der Erlaubnis handelt es sich um eine auf das konkrete Apple-Gerät bezogene Einwilligung. Sie erfüllt indes nicht die Voraussetzungen einer für alle Geräte und Plattformen gültigen allgemeinen Einwilligung gegenüber dem Spiele-Entwicklerstudio. Diese Unterscheidung ist wichtig für Cross-Plattform-Spiele. Da die IDFA im Gerät des Nutzers gespeichert wird, bedarf es nach Art. 5 Abs. 3 ePrivacy-RL einer Einwilligung.
- Die Spiele-Entwicklerstudios müssen ihre Herangehensweise bei der Nutzergewinnung und Werbevermarktung innovativ verändern. Der Trend geht dahin, nicht mehr das Verhalten einzelner Nutzer*innen zu erfassen, sondern auf der Ebene von Nutzergruppen mit gemeinsamen Merkmalen (Kohorten) aggregierte Daten zu erheben. Zudem steigt die Bedeutung von probabilistischen Daten und First-Party-Daten.

Patrick Mitsching, LL.M. (Durham), M.A. (London),
ist Leiter der Rechtsabteilung bei der InnoGames GmbH in Hamburg.

RA Dr. Christian Rauda
ist Fachanwalt für Informationstechnologierecht, für Urheber- und Medienrecht und für gewerblichen Rechtsschutz und Partner der Medienrechtskanzlei GRAEF Rechtsanwälte (Hamburg/Berlin) sowie Lehrbeauftragter an der Bucerius Law School und der Hochschule für Technik und Wirtschaft Berlin.

19 https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-solicitation-autorite-does-not-issue.
20 https://zaw.de/missbrauchsbeschwerde-der-medien-und-werbewirtschaft-gegen-apple-beim-bundeskartellamt/.
21 S. Fußn. 20.
22 S. Fußn. 20.
23 https://9to5mac.com/2021/05/04/apple-emails-search-ads-app-store/.
24 https://searchads.apple.com/help/advanced/0021-set-campaign-refinements/.
25 *Hao*, How Apple personalizes Siri without hovering up your data, abrufbar unter: https://www.technologyreview.com/2019/12/11/131629/apple-ai-personalizes-siri-federated-learning/; *Ippolito*, AI Differential Privacy and Federated Learning, abrufbar unter. https://towardsdatascience.com/ai-differential-privacy-and-federated-learning-523146d46b85; https://machinelearning.apple.com/research/learning-with-privacy-at-scale.
26 Dies sieht im Grundsatz auch die *Datenschutzkonferenz* so, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, S. 17.
27 FAZ v. 10.5.2021, S. 18.