# Bericht von Dr. Johnny Ryan – Verhaltensbasierte Werbung und persönliche Daten

Inhaltsverzeichnis

## *1. Hintergrund und Expertise*

Mein Name ist Johnny Ryan. Ich bin leitender politischer Referent bei Brave, einem auf Datenschutz spezialisierten Internetbrowser.

Ich bin sowohl in der Ad-Tech-Branche als auch im Verlagswesen tätig gewesen. Bevor ich zu Brave kam, war ich bei PageFair, einem Werbetechnologieunternehmen, beschäftigt. In dieser Funktion war ich in Arbeitsgruppen tätig, die Standards für die Werbebranche entwickelte. Davor arbeitete ich als Chief Innovation Officer bei der Zeitung Irish Times.

Zudem war ich in Wissenschaft und Politik tätig und bin Autor zweier Bücher: Bei dem ersten handelt es sich um eine Geschichte der Technologie, die bereits auf Lektürelisten in Harvard und Stanford stand. Das andere diente der Europäischen Kommission als am häufigsten zitierte Quelle in ihrer Folgenabschätzung, die sich gegen eine Web-Zensur in der gesamten Europäischen Union entschied. Ich bin Fellow der Royal Historical Society und Mitglied des Expertennetzwerks des Weltwirtschaftsforums für Medien, Unterhaltung und Information.

Ich habe an der University of Cambridge mit einer Arbeit promoviert, die die Verbreitung von militanten Memes im Netz untersuchte.

Meine Analysen über die Online-Medien- und Werbebranche sind in Medien wie The New York Times, The Economist, The Financial Times, Wired, Le Monde, NPR, Advertising Age, Fortune, Business Week, BBC, Sky News und vielen anderen erschienen.

## *2. Wie personenbezogene Daten für verhaltensbasierte Online-Werbung verwendet werden*

Jedes Mal, wenn eine verhaltensorientierte Werbeanzeige an eine Person gerichtet wird, die eine Website besucht, sendet das System, das die Werbeanzeige auswählt,[1] persönliche Daten an Hunderte oder Tausende von Unternehmen.

Zu diesen personenbezogenen Daten gehören die URL jeder Seite, die ein Benutzer besucht, seine IP-Adresse (aus der sich die geografische Position ableiten lässt), Details zu seinem Gerät und verschiedene eindeutige IDs, die zuvor über den Benutzer gespeichert wurden, um ein langfristiges Profil über ihn oder sie aufzubauen.

Bei diesem System handelt es sich um eine relativ junge Entwicklung der Online-Medien. Erst im Dezember 2010 hat sich ein Konsortium[2] von Unternehmen der Werbetechnik (im Folgenden AdTech) auf die Methoden von Tracking und Werbung geeinigt. Zuvor wurde Online-Werbung durch weitaus einfachere Netzwerke, die Werbeplätze auf Websites verkauften, oder durch sehr lukrative Direktverkaufsgeschäfte von Verlagen platziert.[3]

Wie im Folgenden ausgeführt, hat die Ad-Tech-Industrie trotz der Übergangsfrist bis zum Inkrafttreten der Datenschutz-Grundverordnung keine angemessenen Maßnahmen ergriffen, um geltendes Datenschutzrecht bei der Vielzahl von Unternehmen, die Daten erhalten, durchzusetzen.

---

1 Dieses System wird auch als Real Time Bidding bezeichnet.

2 Das Konsortium bestand aus DataXu, MediaMath, Turn, Admeld, PubMatic und The Rubicon Project. Siehe einen Hinweis zur Geschichte von OpenRTB in "OpenRTB API Specification Version 2.4, final draft", IAB Tech Lab, März 2016 (URL: https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API- Spezification-Version-2-4-FINAL.pdf ), S. 2-3.

3 Erst 2006 entstand die erste "Anzeigenbörse", die es den Werbenetzwerken ermöglicht, auf den Websites ihrer Kunden Flächen an potenzielle Käufer zu versteigern. Ein Pionier war Right Media, das von Yahoo! gekauft wurde.... "RMX Direct: alternative ad networks battle for your blog", Tech Crunch, 12. August 2006 (URL: https://techcrunch.com/2006/08/12/rmx-direct-alternative-ad-networks-battle-for-your-blog/?_ga=2.239524803.1716001118.15363).

## *3. Wie personenbezogene Daten verbreitet werden*

Ein großer Teil der Online-Medien- und Werbebranche verwendet ein System namens "RTB", was für "Real Time Bidding" steht. Es gibt zwei Versionen:

- "OpenRTB" wird von den bedeutendsten Unternehmen der Online-Medien- und Werbebranche eingesetzt.
- „Authorized Buyers“, Googles proprietäres RTB-System, das kürzlich von "DoubleClick Ad Exchange" (bekannt als "AdX") in "Authorized Buyers" umbenannt wurde.[4]

Google verwendet sowohl OpenRTB als auch Authorized Buyers.[5]

Die Fachspezifikationen von OpenRTB sind über das in New York ansässige IAB TechLab öffentlich zugänglich.[6] Die Fachspezifikationen von Authorized Buyers werden von Google öffentlich zur Verfügung gestellt.

Diese Spezifikationen zeigen, dass jedes Mal, wenn eine Person eine Seite auf einer Website lädt, die Real-Time-Bidding verwendet, persönliche Daten über sie an Dutzende - oder Hunderte - von Unternehmen übertragen werden. Beispielsweise können folgende personenbezogene Daten übermittelt werden:

- Welche Website die Nutzerin oder der Nutzer besucht
- Der Standort (OpenRTB enthält auch die vollständige IP-Adresse)
- Eine Beschreibung des verwendete Geräts
- Eindeutige Tracking-IDs oder ein "Cookie-Match", mit denen Werbetreibende versuchen können den Nutzer oder die Nutzerin bei Ihrem nächsten Besuch zu identifizieren, damit ein langfristiges Profil mit Offline-Daten aufgebaut oder gefestigt werden kann
- IP-Adresse (je nach Version des Systems RTB)
- Segment-ID des Datenvermittlers, falls vorhanden. Dies kann Dinge wie die Einkommensklasse, Alter und Geschlecht, Gewohnheiten, Social-Media-Einfluss, Ethnie, sexuelle Orientierung, Religion und politische Orientierung der Nutzerin oder des Nutzers umfassen (je nach Version des Systems RTB)

Eine vollständige Zusammenfassung der personenbezogenen Daten in Open RTB-Anfragen, die von allen RTB-Werbeunternehmen, einschließlich Google, genutzt werden, findet sich in Anhang 1.

Eine Zusammenfassung der personenbezogenen Daten in den Authorized-Buyers-Anfragen finden Sie unter Anhang 2.

Relevante Auszüge aus den OpenRTB "AdCOM"- Fachspezifikationen sind in Anhang 3 dargestellt, Auszüge aus Googles proprietärer RTB-Spezifikation in Anhang 4.

---

4 "Introducing Authorized Buyers", Authorized Buyers, Google (URL: https://support.google.com/adxbuyer/answer/9070822 , abgerufen am 24. August 2018).

5 "OpenRTB Integration", Authorized Buyers, Google (URL: https://developers.google.com/authorized-buyers/rtb/openrtb-guide , abgerufen am 24. August 2018).

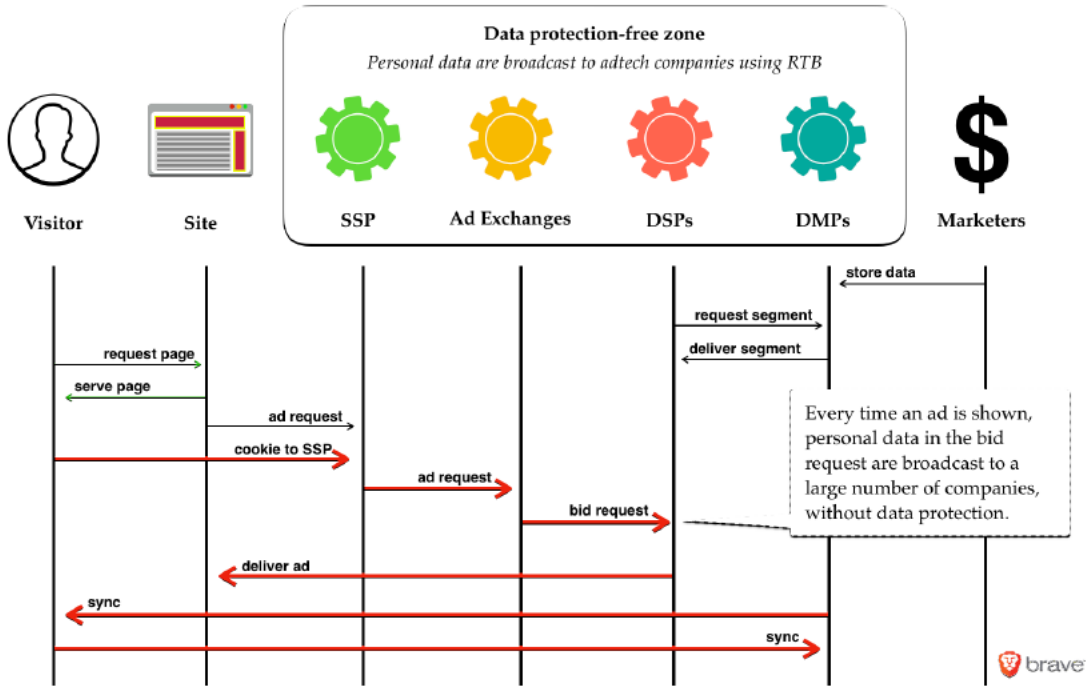
6 Das IAB (Interactive Advertising Bureau) ist die Standardisierungsorganisation und Interessenvertretung der globalen Werbetechnikbranche. Alle bedeutenden Ad-Tech-Unternehmen sind Mitglieder. Das IAB verfügt über lokale Franchiseunternehmen auf der ganzen Welt. Die Organisation, die Standards setzt, ist das IAB TechLab.

## Zur Arbeitsweise

Die Übermittlung von personenbezogenen Daten findet bei der Gebotsanfrage ("RTB bid request") statt. Diese Gebotsanfrage wird in der Regel weit verbreitet, da das Ziel darin besteht, Angebote von Unternehmen einzuholen, die eine Anzeige an die Person senden möchten, die gerade die Website geladen hat. Eine RTB-Gebotsanfrage wird durch Unternehmen, die als "Supply Side Platforms" (SSPs) bezeichnet werden, im Auftrag der Website verbreitet.

Das folgende Diagramm zeigt, wie personenbezogene Daten im Rahmen von Ausschreibungen an mehrere Demand Side Partner (DSP) übertragen werden, die dann entscheiden, ob sie Angebote abgeben. Der DSP handelt im Auftrag von Werbetreibenden und entscheidet auf Basis des Personenprofils, auf das der Werbetreibende abzielt, wann ein Angebot abgegeben wird.

Teilweise benutzen Data Management Plattformen, zu denen Cambridge Analytica gehört, die Daten, die sie so erhalten, um ihre bereits existierenden Personenprofile zu erweitern. Diese Synchronisierung wäre ohne die Gebotsanfragen nicht möglich.




Der wirtschaftliche Anreiz für viele Ad-Tech-Unternehmen besteht darin, so viele Daten wie möglich mit so vielen Partnern wie möglich zu teilen und sie an Partnerunternehmen, die Datenvermittlungen betreiben, weiterzugeben. Offenkundig ist die Weitergabe personenbezogener Daten an ein solches Umfeld hoch riskant.

Trotz dieses hohen Risikos hat RTB keine Mechanismen eingerichtet, die kontrollieren, was mit diesen personenbezogenen Daten passiert, sobald ein SSP oder eine Anzeigenbörse eine Gebotsanfrage sendet. Auch wenn der Anfrageverkehr sicher ist, gibt es keine technischen Maßnahmen, die den Empfänger einer Gebotsanfrage daran hindern, die Daten zu verkaufen oder durch Kombination mit anderen Daten ein Profil zu erstellen. Mit anderen Worten: Es gibt keinen Datenschutz.

Das "GDPR Transparency & Consent Framework" des IAB Europe besagt, dass ein Unternehmen, das personenbezogene Daten erhält, diese nur mit anderen Unternehmen teilen sollte, wenn "eine

gerechtfertigte Annahme dafür besteht, dass der Empfänger über eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten verfügt.[7] Mit anderen Worten: Die Branche verfolgt einen "trust everyone"-Ansatz zum Schutz der sehr intimen Daten, sobald sie einmal übertragen wurden.

Es gibt keine technischen Maßnahmen, um die Daten angemessen zu schützen. Das IAB Europe hat kürzlich angekündigt hat, dass es in Zusammenarbeit mit einer Organisation namens Media Trust ein Tool entwickelt, mit dem versucht werden soll, festzustellen, ob die "consent management platforms" (CMPs), die am IAB Europe teilnehmen, den Richtlinien des Frameworks entsprechen. Laut einer Pressemitteilung von IAB validiert das Tool, ob der Code eines CMPs mit den Anforderungen der technischen Spezifikationen und Protokolle, die im IAB Europe Transparency & Consent Framework detailliert beschrieben sind, entspricht.[8]

Dieses Tool, das sich derzeit in der Beta-Phase befindet, wird nicht ausreichen, um persönliche Daten zu schützen, die in Gebotsanfragen übertragen werden. Denn - auch wenn es möglich wäre, alle webbasierten Datenübertragungen zu kontrollieren[9] - gäbe es immer noch keine Möglichkeit herauszufinden, ob ein Unternehmen z.B. einen kontinuierlichen Server-zu-Server-Transfer von personenbezogene Daten an andere Unternehmen eingerichtet hat.

Sobald die personenbezogenen Daten in einer Ausschreibung an eine große Anzahl von Unternehmen weitergegeben werden, ist das Spiel vorbei. Mit anderen Worten, sobald DSPs personenbezogene Daten erhalten, können sie nach Belieben mit diesen personenbezogenen Daten mit Geschäftspartnern handeln.

Dies ist besonders gravierend, da es sich häufig um Daten besonderer Kategorien handelt. Die betreffenden personenbezogenen Daten zeigen, was eine Person online tut, und geben oftmals einen bestimmten Standort preis. Dies allein kann Aufschluss über die sexuelle Orientierung der Person, den Glauben, die politische Orientierung oder die ethnische Zugehörigkeit geben. Zusätzlich gibt eine Segment-ID an, in welche Personenkategorie ein Data Broker oder ein langfristiger Profiler eine Person einordnet.

Darüber hinaus ist sich die Branche der Mängel dieses Ansatzes bewusst, verfolgt ihn aber dennoch weiter.

RTB-Gebotsanfragen müssen nicht unbedingt personenbezogene Daten enthalten. Wenn alle Akteure der Branche sich damit einverstanden erklären und die Normen unter der Leitung des IAB verändert würden, könnten nur Anfragen, die keine personenbezogenen Daten enthalten, zwischen Unternehmen weitergeleitet werden, sodass die Relevanz einer Werbeanzeige an dem Kontext der Website ausgerichtet würde. Dies würde die beteiligten Unternehmen an der Erstellung von Personenprofilen hindern, was sich auf ihre Einnahmen auswirken würde. Die Industrie ist gerade dabei, eine neue RTB-Spezifikation zu entwickeln (OpenRTB 3.0), die weiterhin personenbezogene Daten sendet, ohne dass Schutzvorkehrungen bestünden. In Anhang 4 wird OpenRTB 3.0 genauer dargestellt.

Online-Werbung, die diesen Ansatz nutzt, wird weiterhin Details darüber, was Personen im Internet lesen oder ansehen, an eine große Anzahl von Unternehmen verbreiten. Die personenbezogenen

---

7 "IAB Europe Transparency & Consent Framework - Policies", IAB Europe, 25. April 2018 (URL: http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf ), S. 7.

8 "IAB Europe Press Release: IAB Europe CMP Validator Helps CMPs Align with Transparency & Consent Framework", IAB Europa, 12. September 2018 (URL:https://www.iabeurope.eu/all-news/press-releases/iab-europe-press-release-iab-europe-cmp-validator-helps-cmps-align-with-transparency-consent-framework/)

9 Siehe "Data Compliance", The Media Trust Website (URL: https://mediatrust.com/how-we-help/data-compliance)

Daten sind nicht geschützt. Die Verbreitung erfolgt dauernd, sie geschieht auf praktisch jeder Website, jedes einzelne Mal, wenn eine Person eine Seite aufruft.

Dies ist eine weit verbreitete beunruhigende Praxis. Aufgrund des Umfangs der Branche sind die Grundrechte praktisch jeder Person, die in Europa das Internet nutzt, beeinträchtigt.

## *4. Bedenken gegenüber diesen Praktiken (Mediale Berichterstattung, Untersuchung von Nichtregierungsorganisationen, aufsichtsbehördliche Betrachtung usw.)*

Mehrjährige Erhebungsdaten zeigen, dass in der Gesellschaft grundlegende und weitverbreitete Bedenken gegenüber diesen Praktiken herrschen. Eine Umfrage des britischen Information Commissioners, veröffentlicht im August 2018, berichtet, dass 53% der britischen Erwachsenen besorgt sind, über "Online-Aktivitäten verfolgt zu werden". [10]

Im Jahr 2017 wurde die GFK vom IAB Europe beauftragt, 11.000 Menschen in der gesamten EU über ihre Einstellung zu Online-Medien und Werbung zu befragen. Die GFK berichtete, dass es nur "20 % gut finden würden, wenn ihre Daten zu Werbezwecken an Dritte weitergegeben werden".[11] Dies steht in engem Zusammenhang mit der Umfrage, die die GFK 2014 in den Vereinigten Staaten durchführte und die ergab, dass "7 von 10 Baby Boomers (geboren nach 1969) und 8 von 10 Pre-Boomers (geboren vor 1969) Misstrauen gegenüber dem Umgang von Werbetreibenden mit ihren Daten haben".[12]

Im Jahr 2016 ergab eine Eurobarometer-Umfrage unter 26.526 Personen in der Europäischen Union Folgendes:

"Sechs von zehn (60%) Befragten haben bereits die Datenschutzeinstellungen für ihren Internetbrowser geändert und vier von zehn (40%) vermeiden bestimmte Websites, weil sie besorgt sind, dass ihre Online-Aktivitäten überwacht werden. Über ein Drittel (37%) verwendet Software, die sie davor schützt, Online-Werbung angezeigt zu bekommen und mehr als ein Viertel (27%) nutzt Software, die verhindert, dass ihre Online-Aktivitäten überwacht werden".[13]

Dies entspricht einer früheren Eurobarometer-Umfrage ähnlichen Umfangs aus dem Jahr 2011, in der festgestellt wurde, dass "70% der Europäer besorgt sind, dass ihre personenbezogenen Daten bei Unternehmen für einen anderen Zweck als den, für den sie gesammelt wurden, verwendet werden".[14]

Die gleichen Bedenken bestehen auch in den Vereinigten Staaten. Im Mai 2015 hat das Forschungszentrum Pew Research Centre berichtet:

"76% der Erwachsenen in den Vereinigten Staaten sagen, dass sie "weniger Vertrauen haben" oder "überhaupt kein Vertrauen haben ", dass die Aufzeichnungen über ihre Aktivitäten durch Online-Werbetreibende privat und sicher bleiben."[15]

Tatsächlich hatten die Befragten am wenigsten Vertrauen, dass die Online-Werbebranche die personenbezogenen Daten über sie vertraulich und sicher verarbeitet verglichen mit jeder anderen

[10] „Information rights strategic plan: trust and confidence", Harris Interactive for the Information Commissioner's Office, August 2018, S. 21.

[11] "Europe online: an experience driven by advertising. Summary results", IAB Europe, September 2017 (URL: http://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf), S. 7.

[12] "GFK survey on data privacy and trust: data highlights", GFK, Juli 2015, S. 29.

[13] "Eurobarometer: E-Privacy (Eurobarometer 443)", Europäische Kommission, Dezember 2016 (URL: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124), S. 5, 36-7.

[14] "Special Eurobarometer 359: attitudes on data protection and electronic identity in the European Union", Europäische Kommission, Juni 2011, S. 2.

[15] Mary Madden und Lee Rainie, "Americans' view about data collection and security", Pew Research Center, Mai 2015 (URL: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf), S. 7.

Kategorie von Datenverarbeitern, einschließlich Social Media Plattformen, Suchmaschinen und Kreditkartenunternehmen. 50% sagte, dass keine Informationen an "Online-Werber" weitergegeben werden sollten.[16]

In einer Reihe von Umfragen äußern große Mehrheiten ihre Besorgnis über Ad-Tech. Die britische Royal Statistical Society veröffentlichte Forschungsergebnisse über das Vertrauen in Daten und die Einstellung zu Datennutzung und Datenaustausch im Jahr 2014 und stellte fest:

"Die Öffentlichkeit zeigte nur sehr wenig Unterstützung für "Online-Händler, die zuletzt angesehene Seiten beobachten und zielgerichtete Anzeigen senden"; 71% der Befragten meinten, dass dies nicht geschehen sollte".[17]

Ähnliche Ergebnisse sind in der eigenen Forschung der Marketingbranche zu verzeichnen. RazorFish, eine Werbeagentur, führte eine Studie mit 1.500 Personen in Großbritannien, den USA, China und Brasilien im Jahr 2014 durch, die ergab, dass 77% der Befragten Werbung, mit der sie auf dem Handy angesprochen werden, als einen Angriff auf ihre Privatsphäre ansehen.[18]

Diese Bedenken manifestieren sich in der Art und Weise, wie sich Menschen heute online verhalten. Das enorme Wachstum von Adblocking-Tools (auf 615 Millionen aktive Geräte bis Anfang 2017)[19] über den gesamten Zeitraum hinweg zeigt die globale Sorge von Internetnutzenden, von der Werbebranche verfolgt zu werden. Ein Branchenkommentator nannte dies den "größten Boykott der Geschichte".[20]

Die Sorge um den Missbrauch personenbezogener Daten in der verhaltensorientierten Online-Werbung wird der Öffentlichkeit nicht kommuniziert. Selbst renommierte Werbetreibende, die Kampagnen online bezahlen, teilen die Sorge. Im Januar 2018 schrieb der CEO des Weltverbandes der Werbetreibenden, Stephan Loerke, einen Kommentar in AdAge, der die aktuellen Systeme als "Data free-for-all" ("Datenzugriff für alle"), attackierte, wobei "jede gezeigte Anzeige Daten beinhaltet, die von bis zu fünfzig Unternehmen berührt wurde, so die Programmexperten Labmatik".[21]

## *5. Kommunikation mit den betroffenen Unternehmen*

Am 16. Januar 2018 habe ich an den Vertreter der Arbeitsgruppe IAB Europe geschrieben (via IAB UK), um privat Feedback zu einem nicht-öffentlichen Entwurf der vom IAB geführten Industrie zur Reaktion auf die DS-GVO zu geben. Ich habe Folgendes hervorgehoben.

Erstens würden Angebotsanfragen personenbezogener Daten zu vielen Parteien gelangen, ohne dass irgendein Schutz bestünde. Dies würde gegen Artikel 5 DS-GVO verstoßen.

---

16 Mary Madden und Lee Rainie, "Americans' view about data collection and security", Pew Research Center, May 2015 (URL: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf), S. 25.

17 "The data trust deficit: trust in data and attitudes toward data use and data sharing", Royal Statistical Society, Juli 2014, S. 5.

18 Stephen Lepitak, "Three quarters of mobile users see targeted adverts as invasion of privacy, says Razorfish global research", The Drum, 30. Juni 2014 (URL: https://www.thedrum.com/news/2014/06/30/three-quarters-mobile-users-see-targeted-adverts-Invasion - Privatsphäre - sagt -razorfish).

19 "The state of the blocked web: 2017 global adblock report", PageFair, Januar 2017 (https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf).

20 Doc Searls, "Beyond ad blocking - the biggest boycott in human history", Doc Searls Weblog, 28 September 2015 (https://blogs.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/).

21 Stephan Loerke, "GDPR data-privacy rules signal a welcome revolution", AdAge, 25. Januar 2018 (URL: http://adage.com/article/cmo-strategy/gdpr-signals-a-revolution/312074/).

Zweitens mangele es aufgrund der Zusammenführung einer Vielzahl von Zwecken und inadäquater Information an einer informierten Einwilligung, was die Einwilligung unwirksam mache.

Obwohl mir für meinen Beitrag gedankt wurde, erhielt ich keine substanziierte Antwort.

Am 21. Februar 2018 habe ich in einem Videoanruf mit dem Koordinator der IAB TechLab-Arbeitsgruppe, die verantwortlich für die Entwicklung der neuen OpenRTB-Fachspezifikation ist, meine Besorgnis über die Verbreitung von persönlichen Daten zum Ausdruck gebracht.

Aber als das IAB im März sein DS-GVO-Framework veröffentlichte, erfuhr ich, dass keine dieser Bedenken berücksichtigt wurde. Am 20. März 2018 habe ich meine Original-Einschätzung in einem offenen Brief veröffentlicht.

Dieser ist online unter https://pagefair.com/blog/2018/iab-europa-konsens-probleme/ zu finden.

Am 4. September 2018 habe ich im Namen von Brave einen ausführlichen Brief an das IAB und an das IAB TechLab geschrieben, um problematische Datenschutzfehler in OpenRTB 3 aufzuzeigen. Ich habe im Detail die akute Gefahr der Übermittlung der personenbezogenen Daten eines Website-Besuchers in Angebotsanfragen dargelegt. Der Brief ist verfügbar unter

https://brave.com/iab-rtb-problems/feedback-on-the-beta-OpenRTB-3.0-Spezifikation-.pdf.

Am 5. September 2018 antwortete das IAB mit einer vierzeiligen E-Mail, die den Antrag ablehnte.

# APPENDICES

## Appendix 1. What personal data are shared in OpenRTB bid requests?

This summary list is incomplete. Other fields may contain personal data.[22]

"Site"[23]

- The specific URL that a visitor is loading, which shows what they are reading or watching.

"Device"[24]

- Operating system and version.
- Browser software and version.
- IP address.
- Device manufacturer, model, and version.
- Height, width, and ratio of screen.
- Whether JavaScript is supported.
- The version of Flash supported by the browser.
- Language settings.
- Carrier / ISP.
- Type of connection, if mobile.
- Network connection type.
- Hardware device ID (hashed).
- MAC address of the device (hashed).

"User"[25]

- An Ad Exchange's unique personal identifier for the visitor to the website. (This may rotate, but the specification says that it "must be stable long enough to serve reasonably as the basis for frequency capping and retargeting."[26])
- Advertiser's "buyeruid", a unique personal identifier for the data subject.
- The website visitor's year of birth, if known.
- The website visitor's gender, if known.
- The website visitor's interests.
- Additional data about the website visitor, if available from a data broker.[27] (These may include the "segment"[28] category previously decided by the data broker, based on the broker's previous profiling of this particular person.)

---

[22] For example, thirty eight of the data fields in the specification contain the phrase "optional vendor specific extensions".

[23] "Object: site" in "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--site-).

[24] "Object: device" in ibid.

[25] "Object: device" in ibid.

[26] ibid.

[27] "Object: data" in ibid.

[28] "Object: segment" in ibid.

"Geo"[29]

- Location latitude and longitude.
- Zip/postal code.

[29] "Object: geo" in ibid.

## Appendix 2. What personal data are shared in Google's proprietary bid requests?

"Publisher"[30]

- The specific URL that a visitor is loading, which shows what they are reading or watching. Note that sometimes publishers using Google's system prevent their URL from being shared.[31]

"Device"

- Operating system and version.
- Browser software and version (some data may be partially redacted).[32]
- Device manufacturer, model, and version.
- Height, width, and ratio of screen.
- Language settings.
- Carrier.
- Type of connection, if mobile.
- Hardware device IDs[33] (in "some circumstances", Google may impose "special constraints" on this. These constraints are not defined)[34]

"User"

- The Google ID of the website visitor
  (May be subject to some form of undefined "special constraints" in "some circumstances".)[35]
- Google's "Cookie Match Service" results, which enables a recipient to determine if the website visitor is a person they already have a profile of, and to combine their existing data with new data in the bid request.[36]

---

[30] All items in this appendix are drawn from "Authorized Buyers Real-Time Bidding Proto", Google, 5 September 2018 (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide).

[31] "Set your mobile app inventory to Anonymous or Branded in Ad Exchange", Google Ad Manager Help (URL: https://support.google.com/admanager/answer/6334919?hl=en)

[32] "Certain data may be redacted or replaced", see "user_agent" in "Authorized Buyers Real-Time Bidding Proto", Google, 5 September 2018 (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide).

[33] Some fields (such as advertising_id) are sent encrypted, but recipients can decrypt using keys that Google gives them when they set up their accounts, or are sent using standard encrypted SSL web connections. See "Decrypt Advertising ID", Authorized Buyers, Google (URL: https://developers.google.com/authorized-buyers/rtb/response-guide/decrypt-advertising-id).

[34] "In some circumstances there are special constraints on what can be done with user data for an ad request". Google vaguely states that in such a case, "user-related data will not be sent unfettered". User ID, Android or Apple device advertising ID, and "cookie match" data can be affected. See "User Data Treatments", Authorized Buyers, Google (URL: https://developers.google.com/authorized-buyers/rtb/user_data_treatments).

[35] ibid.

[36] "Cookie Matching", Google, 5 September 2018 (URL: https://developers.google.com/authorized-buyers/rtb/cookie-guide?hl=en).

(May be subject to some form of undefined "special constraints" in "some circumstances".)[37]

- The website visitor's interests.
- Whether the website visitor is present on a particular "user list" of targeted people (which may be a category previously decided by an advertiser, or the data broker they acquired the data from, based on the broker's previous profiling of this particular person).

"Location"

- Location latitude and longitude.
- Zip/postal code, or postal code prefix if a full post code is unavailable.
- Whether the user is present within a small "hyper local" area.

[37] see note 36.

## Appendix 3. Selected data tables from OpenRTB bid request specification documents

The following tables are copied from AdCOM specification v1, which is part of the OpenRTB 3.0 specification.[38] This defines what data can be included in a bid request. Only selected tables relevant to website bid requests are included here. URLs of the specific part of the specification from where the tables are taken are presented above each table.

Publisher

**Object: Site**

*Derived from:* DistributionChannel

This object is used to define an ad supported website, in contrast to a non-browser application, for example. As a derived class, a "Site" object inherits all "DistributionChannel" attributes and adds those defined below.

| Attribute | Type | Definition |
|---|---|---|
| domain | string | Domain of the site (e.g., "mysite.foo.com"). |
| cat | string array | Array of content categories describing the site using IDs from the taxonomy indicated in "cattax". |
| sectcat | string array | Array of content categories describing the current section of the site using IDs from the taxonomy indicated in "cattax". |
| pagecat | string array | Array of content categories describing the current page or view of the site using IDs from the taxonomy indicated in "cattax". |
| cattax | integer | The taxonomy in use for the "cat", "sectcat" and "pagecat" attributes. Refer to List: Category Taxonomies. |
| privpolicy | integer | Indicates if the site has a privacy policy, where 0 = no, 1 = yes. |
| keywords | string | Comma separated list of keywords about the site. |
| page | string | URL of the page within the site. |
| ref | string | Referrer URL that caused navigation to the current page. |
| search | string | Search string that caused navigation to the current page. |
| mobile | integer | Indicates if the site has been programmed to optimize layout when viewed on mobile devices, where 0 = no, 1 = yes. |
| amp | integer | Indicates if the page is built with AMP HTML, where 0 = no, 1 = yes. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--site-

38 "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md).

### Object: Publisher

This object describes the publisher of the media in which ads will be displayed.

| Attribute | Type | Definition |
|---|---|---|
| id | string, recommended | Vendor-specific unique publisher identifier, as used in ads.txt files. |
| name | string | Displayable name of the publisher. |
| domain | string | Highest level domain of the publisher (e.g., "publisher.com"). |
| cat | string array | Array of content categories that describe the publisher using IDs from the taxonomy indicated in "cattax". |
| cattax | integer | The taxonomy in use for the "cat" attribute. Refer to List: Category Taxonomies. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--publisher-

User

### Object: User

This object contains information known or derived about the human user of the device (i.e., the audience for advertising). The user ID is a vendor-specific artifact and may be subject to rotation or other privacy policies. However, this user ID must be stable long enough to serve reasonably as the basis for frequency capping and retargeting.

| Attribute | Type | Definition |
|---|---|---|
| id | string; recommended | Vendor-specific ID for the user. At least one of "id" or "buyeruid" is strongly recommended. |
| buyeruid | string; recommended | Buyer-specific ID for the user as mapped by an exchange for the buyer. At least one of "id" or "buyeruid" is strongly recommended. |
| yob | integer | Year of birth as a 4-digit integer. |
| gender | string | Gender, where "M" = male, "F" = female, "O" = known to be other (i.e., omitted is unknown). |
| keywords | string | Comma separated list of keywords, interests, or intent. |
| consent | string | GDPR consent string if applicable, complying with the comply with the IAB standard Consent String Format in the Transparency and Consent Framework technical specifications. |
| geo | object | Location of the user's home base (i.e., not necessarily their current location). Refer to Object: Geo. |
| data | object array | Additional user data. Each "Data" object represents a different data source. Refer to Object: Data. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--user-

### Object: Data

The data and segment objects together allow additional data about the related object (e.g., user, content) to be specified. This data may be from multiple sources whether from the exchange itself or third parties as specified by the "id" attribute. When in use, vendor-specific IDs should be communicated *a priori* among the parties.

| Attribute | Type | Definition |
|---|---|---|
| id | string | Vendor-specific ID for the data provider. |
| name | string | Vendor-specific displayable name for the data provider. |
| segment | object array | Array of "Segment" objects that contain the actual data values. Refer to Object: Segment. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--data-

### Object: Segment

Segment objects are essentially key-value pairs that convey specific units of data. The parent "Data" object is a collection of such values from a given data provider. When in use, vendor-specific IDs should be communicated *a priori* among the parties.

| Attribute | Type | Definition |
|---|---|---|
| id | string | ID of the data segment specific to the data provider. |
| name | string | Displayable name of the data segment specific to the data provider. |
| value | string | String representation of the data segment value. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--segment-

## Device

### Object: Device

This object provides information pertaining to the device through which the user is interacting. Device information includes its hardware, platform, location, and carrier data. The device can refer to a mobile handset, a desktop computer, set top box, or other digital device.

| Attribute | Type | Definition |
|---|---|---|
| type | integer | The general type of device. Refer to List: Device Types. |
| ua | string | Browser user agent string. |
| ifa | string | ID sanctioned for advertiser use in the clear (i.e., not hashed). |
| dnt | integer | Standard "Do Not Track" flag as set in the header by the browser, where 0 = tracking is unrestricted, 1 = do not track. |
| lmt | integer | "Limit Ad Tracking" signal commercially endorsed (e.g., iOS, Android), where 0 = tracking is unrestricted, 1 = tracking must be limited per commercial guidelines. |
| make | string | Device make (e.g., "Apple"). |
| model | string | Device model (e.g., "iPhone"). |
| os | integer | Device operating system. Refer to List: Operating Systems. |
| osv | string | Device operating system version (e.g., "3.1.2"). |
| hwv | string | Hardware version of the device (e.g., "5S" for iPhone 5S). |
| h | integer | Physical height of the screen in pixels. |
| w | integer | Physical width of the screen in pixels. |
| ppi | integer | Screen size as pixels per linear inch. |
| pxratio | float | The ratio of physical pixels to device independent pixels. |
| js | integer | Support for JavaScript, where 0 = no, 1 = yes. |
| lang | string | Browser language using ISO-639-1-alpha-2. |
| ip | string | IPv4 address closest to device. |
| ipv6 | string | IP address closest to device as IPv6. |
| xff | string | The value of the x-forwarded-for header. |
| iptr | integer | Indicator of truncation of any of the IP attributes (i.e., "ip", "ipv6", "xff"), where 0 = no, 1 = yes (e.g., from 1.2.3.4 to 1.2.3.0).<br>Refer to tools.ietf.org/html/rfc6235#section-4.1.1 for more information on IP truncation. |
| carrier | string | Carrier or ISP (e.g., "VERIZON") using exchange curated string names which should be published to bidders a priori. |
| mccmnc | string | Mobile carrier as the concatenated MCC-MNC code (e.g., "310-005" identifies Verizon Wireless CDMA in the USA). Refer to en.wikipedia.org/wiki/Mobile_country_code for further information and references. Note that the dash between the MCC and MNC parts is required to remove parsing ambiguity. |
| mccmncsim | string | MCC and MNC of the SIM card using the same format as "mccmnc". When both values are available, a difference between them reveals that a user is roaming. |
| contype | integer | Network connection type. Refer to List: Connection Types. |
| geofetch | integer | Indicates if the geolocation API will be available to JavaScript code running in display ad, |

| | | |
|---|---|---|
| geofetch | integer | Indicates if the geolocation API will be available to JavaScript code running in display ad, where 0 = no, 1 = yes. |
| geo | object | Location of the device (i.e., typically the user's current location). Refer to Object: Geo. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--device-

## Location

### Object: Geo

This object encapsulates various methods for specifying a geographic location. When subordinate to a "Device" object, it indicates the location of the device which can also be interpreted as the user's current location. When subordinate to a "User" object, it indicates the location of the user's home base (i.e., not necessarily their current location).

The "lat" and "lon" attributes should only be passed if they conform to the accuracy depicted in the "type" attribute. For example, the centroid of a large region (e.g., postal code) should not be passed.

| Attribute | Type | Definition |
|---|---|---|
| type | integer | Source of location data; recommended when passing lat/lon. Refer to List: Location Types. |
| lat | float | Latitude from -90.0 to +90.0, where negative is south. |
| lon | float | Longitude from -180.0 to +180.0, where negative is west. |
| accur | integer | Estimated location accuracy in meters; recommended when lat/lon are specified and derived from a device's location services (i.e., type = 1). Note that this is the accuracy as reported from the device. Consult OS specific documentation (e.g., Android, iOS) for exact interpretation. |
| lastfix | integer | Number of seconds since this geolocation fix was established. Note that devices may cache location data across multiple fetches. Ideally, this value should be from the time the actual fix was taken. |
| ipserv | integer | Service or provider used to determine geolocation from IP address if applicable (i.e., "type" = 2). Refer to List: IP Location Services. |
| country | string | Country code using ISO-3166-1-alpha-2.<br>Note that alpha-3 codes may be encountered and vendors are encouraged to be tolerant of them. |
| region | string | Region code using ISO-3166-2; 2-letter state code if USA. |
| metro | string | Regional marketing areas such as Nielsen's DMA codes or other similar taxonomy to be agreed among vendors prior to use.<br>Note that DMA is a trademarked asset of The Nielsen Company. Vendors are encouraged to ensure their use of DMAs is properly licensed. |
| city | string | City using United Nations Code for Trade & Transport Locations "UN/LOCODE" with the space between country and city suppressed (e.g., Boston MA, USA = "USBOS"). Refer to UN/LOCODE Code List. |
| zip | string | ZIP or postal code. |
| utcoffset | integer | Local time as the number +/- of minutes from UTC. |
| ext | object | Optional vendor-specific extensions. |

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--geo-

## Appendix 4. Selected data tables from Google ("Authorised Buyer") RTB bid request specification documents

The following tables are copied from Google's RTB documentation.[39] This defines what data can be included in a bid request. Only selected tables relevant to website bid requests are included here. URLs of the specific part of the specification from where the tables are taken are presented above each table.

[39] "Authorized Buyers Real-Time Bidding Proto", Google, 5 September 2018 (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide)

User

| | | | |
|---|---|---|---|
| **google_user_id** | optional | string | The Google ID for the user as described in the documentation for the cookie matching service. This field is the unpadded web-safe base64 encoded version of a binary cookie ID. See the Base 64 Encoding with URL and Filename Safe Alphabet section in RFC 3548 for encoding details This field is the same as the Google ID returned by the cookie matching service. Not set if there is one or more **user_data_treatment** value, see **constrained_usage_google_user_id** instead. |
| **constrained_usage_google_user_id** | optional | string | Only set if there is one or more **user_data_treatment** value. If **constrained_usage_google_user_id** is set, then **google_user_id** is not set. You must be whitelisted for all **user_data_treatments** in this request in order to receive this field. |
| **cookie_version** | optional | uint32 | The version number of the **google_user_id**. We may sometimes change the mapping from cookie to **google_user_id**. In this case the version will be incremented. |
| **cookie_age_seconds** | optional | int32 | The time in seconds since the **google_user_id** was created. This number may be quantized. |
| **hosted_match_data** | optional | bytes | Match data stored for this **google_user_id** through the cookie matching service. If a match exists, then this field holds the decoded data that was passed in the **google_hm** parameter.<br><br>Not set if there is one or more **user_data_treatment** value, see **constrained_usage_hosted_match_data** instead. |
| **constrained_usage_hosted_match_data** | optional | bytes | Only set if there is one or more **user_data_treatment** value. If **constrained_usage_hosted_match_data** is set, then **hosted_match_data** is not set. You must be whitelisted for all **user_data_treatments** in this request in order to receive this field. |
| **user_agent** | optional | string | A string that identifies the browser and type of device that sent the request. Certain data may be redacted or replaced. |
| **publisher_country** | optional | string | The billing address country of the publisher. This may be different from the detected country of the user in **geo_criteria_id** or the hosting country of the website. For a complete list of country codes, see the country codes list in the AdWords API documentation. |
| **geo_criteria_id** | optional | int32 | Location of the end user. Uses a subset of the |

| | | | |
|---|---|---|---|
| | | | API documentation. |
| **geo_criteria_id** | optional | int32 | Location of the end user. Uses a subset of the codes used in the AdWords API. See the geo-table.csv table in the technical documentation for list of IDs. The **geo_criteria_id** field replaces the deprecated country, region, city, and metro fields. |
| **postal_code**<br>**postal_code_prefix** | optional | string | Detected postal code of the appropriate type for the country of the end user (e.g., zip code if the country is "US"). The **postal_code_prefix** field is set when accuracy is too low to imply a full code otherwise the **postal_code** field is set. |
| **encrypted_hyperlocal_set** | optional | bytes | Hyperlocal targeting signal when available, encrypted as described in the Decrypt Hyperlocal Target Signals guide. |
| **hyperlocal_set** | optional | HyperlocalSet | Unencrypted version of **encrypted_hyperlocal_set**. This field is only set when using an SSL connection. |
| **timezone_offset** | optional | int32 | The offset of the user's time from GMT in minutes. For example, GMT+10 is **timezone_offset = 600**. |
| **user_vertical** | repeated | int32 | List of detected user verticals. Currently unused. |
| **user_list** | repeated | UserList | |

### UserList object

This field is not populated by default. We recommend that bidders instead store and look up list IDs using either `google_user_id` or `hosted_match_data` as keys.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **id** | optional | int64 | The user list ID. |
| **age_seconds** | optional | int32 | The time in seconds since the user was added to the list. |

| | | | |
|---|---|---|---|
| **advertising_id** | optional | bytes | Unencrypted version of **encrypted_advertising_** This field is only set when using an SSL connection. T field is a 16 byte UUID. |
| **hashed_idfa** | optional | bytes | Unencrypted version of **encrypted_hashed_idfa**. This field is only set when using an SSL connection. T field is a 16 byte MD5. |
| **constrained_usage_ encrypted_advertising_id** | optional | bytes | Only set if the BidRequest contains one or more **user_data_treatment** value. If **constrained_usage_encrypted_advertising** or **constrained_usage_encrypted_hashed_id** is set, then the corresponding non-constrained field is set. You must be whitelisted for all **user_data_treatments** in this request in order to receive these fields. |
| **constrained_usage_advertising_id** | optional | bytes | Unencrypted version of **constrained_usage_encrypted_advertising** This field is only set when using an SSL connection. T field is a 16 byte UUID. |
| **constrained_usage_ encrypted_hashed_idfa** | optional | bytes | |
| **constrained_usage_hashed_idfa** | optional | bytes | Unencrypted version of **constrained_usage_encrypted_hashed_idfa**. This field is only set when using an SSL connection. T field is a 16 byte MD5. |
| **app_name** | optional | string | App names for Android apps are from the Google Pla store. App names for iOS apps are provided by App Annie. |
| **app_rating** | optional | float | Average user rating for the app. The range of user rati is between 1.0 and 5.0. Currently only available for ap in Google Play store. |

## Mobile object

Information for ad queries coming from mobile devices. A mobile device is either a smartphone or a tablet. This is present for ad queries both from mobile devices browsing the web and from mobile apps.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **is_app** | optional | bool | If true, then this request is from a mobile application. always be true when **app_id** is set. May also be true anonymous inventory, in which case **anonymous_id** be set. |
| **app_id** | optional | string | The identifier of the mobile app when this ad query comes from a mobile app. If the app was downloaded from the Apple iTunes app store, then this is the app-store ID, e.g., 343200656. For Android devices, this is fully qualified package name, e.g., com.rovio.angrybir For Windows devices it's the App ID, e.g., f15abcde-f6 47i0-j3k8-37l93817mn3o. |
| **is_interstitial_request** | optional | bool | If true, then this is a mobile full screen ad request. |
| **app_category_ids** | repeated | int32 | This field contains the IDs of categories to which the current mobile app belongs. This field will be empty if **is_app** is false. The mapping between mobile apps a categories is defined by the Google Play Store for Android apps, or the Apple iTunes Store for iOS apps. look up category name from category ID, refer to the mobile app categories table. |
| **is_mobile_web_optimized** | optional | bool | For a mobile web request, this field indicates whether page is optimized for mobile browsers on high-end mobile phones.<br>default=false |
| **encrypted_advertising_id** | optional | bytes | This field is used for advertising identifiers for:<br>1) iOS devices (This is called Identifier for Advertising IDFA, as described in this Help Center article.)<br>2) Android devices.<br>3) Roku devices.<br>4) Microsoft Xbox devices.<br>5) Amazon devices.<br><br>When the **encrypted_advertising_id** is an IDFA, plaintext after decrypting the ciphertext is the IDFA (1 byte UUID) returned by iOS's **[ASIdentifierManag advertisingIdentifier]**. For **encrypted_hashed_idfa**, the plaintext is the 16 by MD5 hash of the IDFA. Only one of the two fields will b available, depending on the version of the SDK makin the request. Later SDKs provide unhashed values. Th are not set if there is one or more **user_data_treatment** value in the BidRequest, se **constrained_usage_encrypted_advertising** and **constrained_usage_encrypted_hashed_i** instead. |
| **encrypted_hashed_idfa** | optional | bytes | See also the description for **encrypted_advertising_id**. |
| **advertising_id** | optional | bytes | Unencrypted version of **encrypted_advertising_** This field is only set when using an SSL connection. T |

| | | | |
|---|---|---|---|
| **advertising_id** | optional | bytes | Unencrypted version of **encrypted_advertising_** This field is only set when using an SSL connection. T field is a 16 byte UUID. |
| **hashed_idfa** | optional | bytes | Unencrypted version of **encrypted_hashed_idfa**. This field is only set when using an SSL connection. T field is a 16 byte MD5. |
| **constrained_usage_ encrypted_advertising_id** | optional | bytes | Only set if the BidRequest contains one or more **user_data_treatment** value. If **constrained_usage_encrypted_advertising** or **constrained_usage_encrypted_hashed_id** is set, then the corresponding non-constrained field is set. You must be whitelisted for all **user_data_treatments** in this request in order to receive these fields. |
| **constrained_usage_advertising_id** | optional | bytes | Unencrypted version of **constrained_usage_encrypted_advertising** This field is only set when using an SSL connection. T field is a 16 byte UUID. |
| **constrained_usage_ encrypted_hashed_idfa** | optional | bytes | |
| **constrained_usage_hashed_idfa** | optional | bytes | Unencrypted version of **constrained_usage_encrypted_hashed_idfa** This field is only set when using an SSL connection. T field is a 16 byte MD5. |
| **app_name** | optional | string | App names for Android apps are from the Google Pla store. App names for iOS apps are provided by App Annie. |
| **app_rating** | optional | float | Average user rating for the app. The range of user rati is between 1.0 and 5.0. Currently only available for ap in Google Play store. |

Publisher

This section lists information that we know about the web page or mobile application where the impression originates.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **publisher_id** | optional | string | The publisher ID as defined by the publisher code suffix of the web property code. For instance, "pub-123" is the publisher code of web property code "ca-pub-123" (ca- is the product specific prefix of the web property). |
| **seller_network_id** | optional | int32 | The seller network ID. See seller-network-ids.txt file in the technical documentation for a list of IDs. This is only set if the site is not anonymous and the publisher allows site targeting. |
| **partner_id** | optional | fixed64 | ID for the partner that provides this inventory. This is only set when **seller_network_id** is also set and further partner information beyond the **seller_network_id** is also available. The value of the **partner_id** is not meaningful beyond providing a stable identifier. |
| **url** | optional | string | The URL of the page with parameters removed. This is only set if the site is not anonymous and the publisher allows site targeting. You can use **anonymous_id** for targeting if the inventory is anonymous. Otherwise, use **detected_vertical**. Only one of **url** or **anonymous_id** is ever set in the same request. This always starts with a protocol (either http or https). |
| **anonymous_id** | optional | string | An id for the domain of the page. This is set when the inventory is anonymous. Only one of **url** or **anonymous_id** is ever set in the same request. |
| **detected_language** | repeated | string | Detected user languages, based on the language of the web page, the browser settings, and other signals. The order is arbitrary. The codes are 2 or 5 characters and are documented in the language codes table. |
| **detected_vertical** | repeated | Vertical | Unordered list of detected content verticals. See the publisher-verticals.txt file in the technical documentation for a list of IDs. |
| **detected_content_label** | repeated | int32 | List of detected content labels. See the content-labels.txt file in the technical documentation for a list of IDs. |
| **device** | optional | Device | |

| | | | |
|---|---|---|---|
| **device** | optional | Device | |
| **key_value** | repeated | KeyValue | |
| **mobile** | optional | Mobile | |
| **video** | optional | Video | |
| **publisher_settings_list_id** | optional | fixed64 | The publisher settings list ID that applies to this page. See the RTB Publisher Settings guide for details. |
| **publisher_type** | optional | PublisherType | Publisher type of the inventory where the ad will be shown. For an Authorized Buyers publisher, its inventory can be either owned and operated (O&O), represented by the publisher, or of unknown status. AdSense and AdMob inventory is represented by Google.<br><br>**enum PublisherType**<br>**UNKNOWN_PUBLISHER_TYPE = 0;**<br>**ADX_PUBLISHER_OWNED_AND_OPERATED = 1;**<br>**ADX_PUBLISHER_REPRESENTED = 2;**<br>**GOOGLE_REPRESENTED = 3;**<br>**default = UNKNOWN_PUBLISHER_TYPE** |
| **adslot** | repeated | AdSlot | |
| **bid_response_feedback** | repeated | BidResponseFeedback | |

### Vertical object

One or more detected verticals for the page as determined by Google.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **id** | required | int32 | The vertical ID. See the publisher-verticals.txt file in the technical documentation for a list of IDs. |
| **weight** | required | float | Weight for this vertical, in the (0.0, 1.0] range. More relevant verticals have higher weights. |

## Location

### Hyperlocal object

A hyperlocal targeting location when available.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **`corners`** | repeated | Point | The mobile device can be at any point inside the geofence polygon defined by a list of corners. Currently, the polygon is always a parallelogram with 4 corners. |

### Point object

A location on the Earth's surface.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **`latitude`** | optional | float | Latitude of the location. |
| **`longitude`** | optional | float | Longitude of the location. |

### HyperlocalSet object

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **`hyperlocal`** | repeated | Hyperlocal | This field currently contains at most one hyperlocal polygon. |
| **`center_point`** | optional | Hyperlocal.Point | The approximate geometric center of the geofence area. It is calculated exclusively based on the geometric shape of the geofence area and in no way indicates the mobile device's actual location within the geofence area. If multiple hyperlocal polygons are specified above then **`center_point`** is the geometric center of all hyperlocal polygons. |
| **`encrypted_hyperlocal_set`** | optional | bytes | Hyperlocal targeting signal when available, encrypted as described in this guide |

## Device

## Device object

Information about the device.

| Attribute | Required/Optional | Type | Implementation details |
|---|---|---|---|
| **DeviceType** | | enum | **UNKNOWN_DEVICE = 0;**<br>**HIGHEND_PHONE = 1;**<br>**TABLET = 2;**<br>**PERSONAL_COMPUTER = 3;** - Desktop or laptop devices.<br>**CONNECTED_TV = 4;** - Both connected TVs (smart TVs) and connected devices (such as Roku and Apple TV).<br>**GAME_CONSOLE = 5;** |
| **device_type** | optional | DeviceType | default = **UNKNOWN_DEVICE** |
| **platform** | optional | string | The platform of the device. Examples: Android, iPhone, Palm |
| **brand** | optional | string | The brand of the device, e.g., Nokia, Samsung. |
| **model** | optional | string | The model of the device, e.g., N70, Galaxy. |
| **os_version** | optional | OsVersion | The OS version; e.g., 2 for Android 2.1, or 3.3 for iOS 3.3.1. |
| **carrier_id** | optional | int64 | Unique identifier for the mobile carrier if the device is connected to the internet via a carrier (as opposed to via WiFi). To look up carrier name and country from carrier ID, refer to this mobile carriers table. |
| **screen_width** | optional | int32 | The width of the device screen in pixels. |
| **screen_height** | optional | int32 | The height of the device screen in pixels. |
| **screen_pixel_ratio_millis** | optional | int32 | Used for high-density devices (e.g., iOS retina displays). A non-default value indicates that the nominal screen size (with pixels as the unit) does not describe the actual number of pixels in the screen. For example, nominal width and height may be 320x640 for a screen that actually has 640x1080 pixels, in which case **screen_width=320**, **screen_height=640**, and **screen_pixel_ratio_millis=2000**, since each axis has twice as many pixels as its dimensions would indicate.<br><br>default = 0 |
| **screen_orientation** | optional | ScreenOrientation | The screen orientation of the device when the ad request is sent.<br><br>enum **ScreenOrientation**<br>**UNKNOWN_ORIENTATION = 0;**<br>**PORTRAIT = 1;**<br>**LANDSCAPE = 2;**<br>**default = UNKNOWN_ORIENTATION** |
| **hardware_version** | optional | string | Apple iOS device model, e.g., "iphone 5s", "iphone 6+", "ipad 4". |

### OSVersion object

Contains the OS version of the platform. For instance, for Android 2, major=2, minor=0. For iPhone 3.3.1, major=3 and minor=3.

| Attribute | Required/Optional | Type |
|---|---|---|
| **major**<br>**minor**<br>**micro** | optional | int32 |