Ağustos 2023

ÜÇÜNCÜ PARTİ ÇEREZ SONRASI DÖNEM IAB AVRUPA KILAVUZU

www.iabtr.org

iab.TR

ÜÇÜNCÜ PARTİ ÇEREZ SONRASI DÖNEM IAB AVRUPA KILAVUZU

Bu kılavuz, IAB Avrupa Programatik Komitesi üyesi uzmanlar tarafından Mayıs 2020'de hazırlanmış, Şubat 2021 ve Mart 2022'de güncellenmiş, İnteraktif Reklamcılık Derneği (IAB) tarafından Türkçe 'ye çevrilmiştir.

Kılavuz, günümüz dijital reklamcılığında çerezlerin kullanımına ilişkin arka plan bilgisi ve geliştirilmekte olan alternatif çözümlere genel bir bakış sunmaktadır. Çözümler geliştikçe, üçüncü parti çerezlerin yerine başvurulabilecek alternatifler hakkındaki en son bilgilerle birlikte düzenli olarak güncellenecektir.

IAB Europe Programatik Komitesi'nde ve bu kılavuzun ilk versiyonunu hazırlayanlar arasında yer alan IAB Reklam Teknolojileri ve Standartlar Yürütme Kurulu üyesi **Gökberk Ertunç'a** (OMG, Data Analitik ve Programatik Yöneticisi) katılım ve destekleri için; çalışmanın değerlendirilmesi ve Türkçe 'ye uyarlanması konusundaki destekleri için ise IAB Reklam Teknolojileri ve Standartlar Yürütme Kurulu üyelerine teşekkür ederiz.

Detaylı bilgi ve IAB çalışmalarına katkıda bulunmak için IAB profesyonel kadro ile iletişime geçebilirsiniz.

Jale Karaveli, İnteraktif Reklamcılık Derneği (IAB) Genel Koordinatör Yardımcısı
jale.karaveli@iabtr.org

Yasemin Koçak, İnteraktif Reklamcılık Derneği (IAB) Üye İlişkileri ve İçerik Yöneticisi
yasemin.kocak@iabtr.org

İçindekiler

GİRİŞ

Mayıs 2020'de IAB Europe, markaları, ajansları, yayıncıları ve teknoloji aracılarını merakla beklenen üçüncü parti çerez sonrası reklamcılık ekosistemine hazırlamak için ilk "Üçüncü Parti Çerez Dönemi Sonrası Kılavuzu'nu yayınladı. IAB Europe Programatik Ticaret Komitesi (PTC) uzmanları tarafından geliştirilen Kılavuz, dijital reklam çerezlerinin mevcut kullanımına, bunların devre dışı bırakılmasına katkıda bulunan faktörlere ve şu anda mevcut olan alternatif çözümlere genel bir bakış sundu.

Çözümler geliştikçe, PTC, üçüncü parti çerezlere yönelik pazar alternatifleri hakkında en son bilgileri ve rehberliği sağlamak için Kılavuzu güncel tutmaya çalıştı. İlk güncelleme Şubat 2021'de yayınlanmıştır ve bu son güncellemede aşağıdaki soruların yanıtlarına yer verilmektedir:

- Üçüncü parti çerezlerin devre dışı bırakılması dijital reklam ve platformlar dahil olmak üzere sektörün genelini nasıl etkileyecek?
- Üçüncü parti çerezlerinin olmaması, dijital reklam kampanyalarının yürütülmesini nasıl etkileyecek?
- Halihazırda üçüncü parti çerez kullanımının yerini alacak hangi çözümler bulunmaktadır?
- Hangi sektörel çözümler kim tarafından geliştiriliyor?
- Farklı çözümlere nasıl katkıda bulunabilirim?

Kılavuzun amacı budur. Sektöre nelerin geliştirilmekte olduğunu göstermek ve test, iş birliği ve öğrenmeye katılımı teşvik etmek.

Bu nedenle, paydaşların üçüncü parti çerez reklamcılığı sonrası döneme yönelmelerine ve hazırlanmalarına yardımcı olmak için, kılavuzun bu güncellenmiş baskısında ek kilit sorular da ele alınmıştır:

- İşletmem için hangi alternatif çözümler uygun olabilir?
- Şirketim sektörde bir tanımlama bilgisi geliştirme sürecine nasıl dahil olabilir?
- Test etmek ve etkili bir şekilde çalışmak için Kimlik (ID) çözümlerini nasıl belirleyebiliriz?

Kılavuz, sektördeki değişiklikleri ve gelişmeleri yansıtacak şekilde düzenli olarak güncellenmeye devam edecektir.

BÖLÜM 1- ARKA PLAN

Ağustos 2019'da Chrome, gizliliği korumak ve gizli takibi önlemek için yeni dijital reklam araçları geliştirerek "web'de gizliliği temelden geliştirmek için bir dizi açık standart geliştirmek" amacıyla yeni bir girişimi (Privacy Sandbox) duyurdu. Ocak 2020'de ise Chrome, önümüzdeki iki yıl içinde Chrome'da üçüncü parti çerezleri için desteği aşamalı olarak kaldırmayı planladığını duyurdu. Haziran 2021'de Chrome, zaman çizelgesinde bir güncelleme yaptığını duyurarak privacysandbox.com adresinde herkese açık bir zaman çizelgesi hazırladı. Yeni zaman çizelgesine göre Chrome'un üçüncü parti çerezlere yönelik desteği 2024 yılının 3. çeyreğinde kalkıyor. Üçüncü parti tanımlama bilgilerine yönelik desteğin aşamalı olarak kaldırılacağı duyurusu, yayıncılar arası reklamcılığın işleyiş şeklini değiştirecek.

Bazı sektör yorumcuları ve fikir önderleri, çerezsiz bir geleceğe dair iç karartıcı bir tablo çizmek için büyük çaba sarf etseler de bunun tüm çerezler için geçerli olmadığı konusunda net olunmalıdır. Birinci parti çerezleri, bir kullanıcının doğrudan ziyaret ettiği etki alanı (web sitesi) tarafından saklanır. Üçüncü parti çerezleri ise bir kullanıcının doğrudan ziyaret ettiği alan dışındaki etki alanları tarafından oluşturulur, bu nedenle üçüncü parti olarak anılırlar. Bu üçüncü parti çerezler öncelikle siteler arası takip (cross-site tracking) ve yeniden hedefleme (re-targeting) için kullanılsa da, frekans sınırlama, reklam öğesi sıralama ve optimizasyon ile bazı reklam sunma özelliklerini geliştirmek için de kullanılabilirler.

Eşleşme oranı sorunları göz önüne alındığında, sektördeki pek çok kişi üçüncü parti çerezlerin tükenmesinin dijital medyanın doğal bir evrimi olduğunu ve bu durumun uzun süredir beklendiğini söylemişlerdir. Üçüncü parti çerezlerin ortadan kaldırılması şüphesiz dijital reklamcılık tedarik zincirinin birçok aşamasını etkilemektedir, ancak bunun sektörün sonu olacağını veya üçüncü parti kullanıcı kitlelerini tamamen ortadan kaldıracağını öne sürmek yanıltıcıdır.

Bu nedenle, bir hedef kitleye ulaşma amaçlı çözümlerin veya alternatif yolların oluşturulmasını sağlamak için, bir kampanyanın nasıl sunulacağı ve gerçekleşeceği konusundaki değişiklikleri anlamak önemlidir.

Öncelikle, web (masaüstü ve mobil özellikli web siteleri) ve uygulama içi birbirinden ayrılmalıdır. Çerezler salt web teknolojisidir ve mobil işletim sistemi tarafından sağlanan uygulama içi mobil reklamlar (örn. IDFA, AAID veya MAID'ler) halihazırda tanımlama için kullanılmaktadır. Reklamcılık açısından bakıldığında, şu anda üçüncü parti çerezler gibi siteler arası tanımlayıcılar tarafından desteklenen ve aşağıda özetlenen bir dizi kullanım durumu bulunmaktadır. Siteler arası tanımlayıcılar olmadan bu kullanım alanları bugün olduğu gibi çalışmayacaktır ve gelecekte bunları desteklemek için gizliliği koruyan yeni teknolojiler gerekecektir.

- Yayıncılar arası tanımlayıcılara bağlı olarak frekans limiti.
- Pazarlamacıların birinci parti verilerini bir yayıncıya sendikasyon. Kitle genişletme için birinci parti yayıncı verileri.
- Kitle tabanlı dinamik kreatif optimizasyon (DCO)
- DMP'ler (Veri Yönetim Platformları), CDP'ler (Müşteri Data Platformları) ve cloud sistemleri tanımlayıcı (ID) bağlantıları.
- View-through veya multi-touch ilişkilendirme.

Günümüzde çoğu kampanyada bu özellikler ve teknolojilerden en az biri uygulanmaktadır, bu da neredeyse tüm kampanyalarda yeni yaklaşımlar bulunması gerektiği anlamına gelir. Bu bilgileri akılda tutarak, depolama ve erişim ve hedefleme verilerini birbirinden ayırmak esastır.

Depolama ve Erişim

İnternet tarayıcıları iki farklı depolama türünü kullanır: Çerezler ve web depolama (Document Object Model veya DOM depolama olarak da adlandırılır). Web depolaması, oturum depolaması ve lokal depolama (LSO) olarak gerçekleşir ve her ikisi de tarayıcı istemci sisteminde verileri çerezlere benzer şekilde saklamanıza olanak verir. Basit bir ifadeyle, web depolama, çerezlerin daha da geliştirilmesidir ve depolama için çok daha fazla kapasite ve daha iyi geliştirici API'ler sağlar ve aynı zamanda çerezlere göre farklılıkları da vardır. Çerezler istemci ve sunucu tarafından okunabiliyorken, web depolaması salt istemci teknolojisidir, yani çerezler her zaman bir sayfanın HTTP(s) isteği ile gönderilirken, yerel depolamanın javascript tarafından açıkça okunması/yazılması gerekir.

Bir çerez, bir domain ismi (=key), bir değer (bu değer bir veri olabilir, örneğin: Reklam Kimliği veya başka kimlikler) ve atanan nitelikten (attribute) (ör. alan adı, yol, geçerlilik tarihi, boyut, http only, güvenli ve samesite) oluşur. Nitelikler temel olarak veri erişim iznini ve kullanım süresini tanımlar.

Bir çerez birinci veya üçüncü parti çerezse, okunduğu ve yazıldığı içeriğe bağlıdır. Erişim yerindeki anlam, erişime izin verilip verilmediğini tanımlar. Çerezin kendisi, verileri tutabilen bir depolama biçimidir, ancak kendi başına bir tanımlayıcı (identifier) değildir.

Yayıncı Örneği

Mail.com'u çalıştırdığınızı düşünün, aynı alanda okunan ve yazılan tüm çerezler birinci partidir, ancak web sitesine diğer alanlardan (ör. ssp.eu veya adserver.eu) yerleştirilen tüm (müşteriye yönelik reklamlar hariç) komut dosyaları üçüncü parti olarak kabul edilir ve bu nedenle oradan okunan veya yazılan çerezler de bu çerçevede değerlendirilir.

Reklamveren Örneği

Bir reklamveren kendi www.advertiser.eu alanına birinci parti olarak yeniden hedefleme çerezi yazsa bile, bu bilgiye daha sonra kişiselleştirilmiş bir ürün reklamı sunmak için, yayıncının web sitesinde örn. mail.com'da reklam yayını sırasında erişilemez, çünkü mail.com açısından bu üçüncü parti bir çerezdir.

Tarayıcılarda üçüncü parti çerezlerinin yaygın olarak kullanımdan kaldırılması ve oturum açma tabanlı tanımlayıcıların yükselişiyle birlikte reklamcılık bağlamında web veya uygulama içi bağımsız alternatif sunucu tarafı depolama çözümleri geliştirilmektedir. Bu alternatif çözümler hakkında daha fazla bilgi 5. bölümde ayrıntılı olarak açıklanmaktadır.

Kampanya Verisi

Çapraz yayıncı oturumlarını ilişkilendirecek bir tanımlayıcının mevcut olması durumunda, kullanıcı merkezli veriler kampanyaların KPI'ları için oldukça faydalı olabilir.

Kampanya verileri, tanımlayıcının kendisiyle aynı yerde depolanmak zorunda değildir, genel olarak sunucu tarafında (örneğin bir veri platformunda) depolanır.

Neredeyse tüm kampanyalar için adreslenebilir bir kullanıcıyla (yani kalıcı bir tanımlayıcıya bağlı bir kullanıcıyla) ilgili standart veri kullanım kaynağı "frekans limiti"dir.

Reklamverenler veya ajanslar, belirli bir dönemde belirli bir kullanıcıya sunulacak reklam sayısını sınırlandırmak için frekans limitini kullanırlar.

Bu frekans limitinin bir kampanya, reklam öğesi veya envanter düzeyinde ayarlanmış olması fark etmemektedir; hedef, kullanıcı başına medya harcamasını kontrol etmektir. Üçüncü parti çerezlerinin kaldırılması, satın alan tarafın bir kampanyanın bu yönünü kontrol etme imkanını önemli ölçüde etkilemektedir.

Performans Pazarlaması, yoğunlukla ürün seviyesi, ürün kategorisi veya alışveriş sepeti verilerini adreslenebilir bir kullanıcıyla ilişkilendiren (yeniden hedefleme/plan) veri göstergeleri üzerine kuruludur.

Dijital Marka Pazarlama kampanyaları, adreslenebilir bir kullanıcıyla ilgili, sosyodemografik (ör. yaş, cinsiyet, gelir, hane halkı sayısı, aile durumu), coğrafi (IP, posta kodu, enlem / boylam), teknik (cihaz, işletim sistemi, tarayıcı, ISS, bağlantı, ekran boyutu), ilgi alanı verilerini kullanırlar.

Paydaşların Gelişimi

Dijital reklamcılık ekosistemine dahil olan her paydaş, üçüncü parti çerezlerinin ortadan kalkmasından bir şekilde etkilenecektir.

Ajanslar, bir yandan reklamverenler için teknoloji planları oluştururken bir yandan da planlama ve satın alma işleminin izleyici aktivasyonuyla sürmesini sağlamak için çoğunlukla kavramsal iş yüküyle ilgileneceklerdir. Reklamverenlerin kendi müşterilerini daha iyi anlamaları önemli ve birinci parti verileri bunun anahtarı olacaktır.

Yayıncıların, kitle verilerini toplama ve genişletme stratejilerini yeniden düzenlemeleri gerekecektir. Yayıncılar, ajanslar ve reklamcılar arasındaki iletişim çok daha önem kazanacaktır.

DSP'lerin ve SSP'lerin, teknolojilerinin hedeflenen dijital reklamcılık sunmaya devam etmesini sağlamaları gerekecektir. DSP'ler bu zorluğun üstesinden gelmek için kimlik (ID) pazarları yaratmakta veya bunlara katılmaktadırlar (daha fazla bilgi 5. bölümde). SSP'ler satın alma tarafıyla yakın ilişkiler kurmaya başlamışlardır. Medya satın alma yolu optimizasyonuna ek olarak, ölçüm ve hedeflemeye ilişkin genişletilmiş kimlik (ID) paylaşım fırsatları sunmaktadırlar.

BÖLÜM 2- ÜÇÜNCÜ PARTİ ÇEREZLERİN DEVRE DIŞI BIRAKILMASINDA ETKEN OLAN 3 FAKTÖR

Son iki yılda, dijital reklamcılıkta üçüncü parti çerezlerin devre dışı bırakılması kararında etken olan temel gelişmeler açısından, bakılması gereken üç temel alan vardır:

1. Veri toplama ve kullanıma ilişkin yasal ortam

2. Tarayıcı denetimi (Browser gatekeeping)

3. Reklam engelleme (Ad-blocking)

2.1 Veri toplama ve kullanıma İlişkin Yasal Ortam

Kişilerin temel veri gizliliği hakkı, ayrıca verilerinin nasıl kullanıldığını ve paylaşıldığını bilme hakkı vardır. Kişiler verilerinin reklam için kullanılıp kullanılamayacağını belirleme hakkına sahiptirler.

Dünya çapında çevrimiçi gizliliği düzenleyen kapsayıcı tek yasa yoktur. Bunun yerine, çeşitli yargı alanlarında bölgesel, federal veya eyalet yasalarından oluşan karma düzen geçerlidir.

20. yüzyılın ikinci yarısında, Avrupa'daki birkaç ülke, kişisel bilgilerin kullanımını kontrol etmeyi amaçlayan eski yasalar ve düzenlemeler üzerinde çalışmaya başlamıştır. 1995 yılında, Avrupa Birliği (AB) Veri Koruma Direktifi (Direktif 95/46/EC) onaylanmıştır. Aşağıdaki bölüm, halihazırda çerezleri, rızayı ve internette takibi etkileyen mevcut yasalara odaklanmaktadır; ancak hukuki çerçevenin bu konuda sürekli gelişmekte olduğunun altı çizilmelidir.

AB eGizlilik Direktifi (EU ePrivacy Directive) ve Genel Veri Koruma Yönetmeliği (GDPR)

AB'nin eGizlilik Direktifi, öncelikle elektronik iletişim sektöründe, yani telekomünikasyon sağlayıcıları tarafından kişisel verilerin işlenmesini düzenleyen AB aracıdır. eGizlilik Direktifi (ePD), çerezlerle ilgili kuralları nedeniyle dijital reklamcılık sektörü için çok önemlidir.

eGizlilik Direktifi, üye devletlerin, web sitesi operatörlerinin ilgili kullanıcıyı çerezlerin kullanımı hakkında bilgilendirmesini ve (çoğu) çerezi kullanmak için onayını almasını gerektiren kurallar oluşturmasını şart koşmaktadır. 2017'de kuralların daha da uyumlu olmasını ve AB vatandaşlarına doğrudan uygulanabilirliğini sağlamak üzere Direktifin yerini alacak yeni bir eGizlilik Yönetmeliği için bir teklif yayınlanmıştır.

Olağan yasama prosedürünü takip eden Avrupa Parlamentosu, eGizlilik Tüzüğü'ne ilişkin raporunu Ekim 2017'de kabul etti. 10 Şubat 2021'de AB Konseyi, Portekiz'in dönem başkanlığı sırasında AP ile müzakerelerin başlangıcını işaret eden eGizlilik tüzüğünün kendi versiyonunu imzaladı. Anlaşma, güncellenmiş bir yönetmeliğin yürürlüğe girmesi ve 2022'de üçleme yapılması yolunda önemli bir kilometre taşı oluşturdu.

Oysa mevcut haliyle önerilen Tüzük, tarayıcıları ve diğer yazılım sağlayıcılarını çerezler ve diğerleri yoluyla veri toplanmasını etkin bir şekilde önleme seçeneği sunmaya ve kullanıcıları kurulum sırasında gizlilik tercihleri konusunda seçim yapmaya zorlamaya zorlayacak metni artık içermemektedir. Bu hükmün (Madde 10) yokluğu, uygulamada kaldırılan Madde 10 hükmünü eski haline getiren Konsey metnindeki benzer dille hala gizlenebilir.

Teklif aynı zamanda Avrupa Parlamentosu'nun bir hizmete erişim için rızayı bir koşul olarak dahil etmesi için bir fırsat olmuştur. Avrupa Konseyi, *'gazetecilik amaçları da dahil olmak üzere ifade ve bilgi edinme özgürlüğüne uygun olarak sağlanan hizmetler'* için hakları tanıyarak tam tersi bir tutum benimsemiştir. Avrupa Parlamentosu'nun tutumu, çevrimiçi medya işletmelerinin sürdürülebilirliğinin devamı için sözde koşulluluğun öneminin altını çizmektedir.

Dijital Hizmetler Yasası (Digital Services Act - DSA)

AB'nin Dijital Hizmetler Yasası, tek pazarı güçlendirmek ve vatandaşları ve haklarını korumak için dönüm noktası niteliğinde bir mevzuat olarak vaat edildi. Ancak Avrupa Komisyonu'nun Aralık 2020'de ilk kez teklif etmesinden bu yana, mevzuat tartışıldı, tartışılıyor ve bazı politika yapıcılar kapsamını büyük ölçüde genişletmeyi ve çevrim içi çalışma şeklini değiştirmeyi planlamakta.

Ocak 2022'de Avrupa Parlamentosu (AP), yazılım gizlilik ayarının yapılması durumunda, yayıncıların kullanıcı ile bağımsız olarak, diyalog kurma, onay isteme hakkını ortadan kaldıracak rıza ve hizmetlere erişim için daha fazla yükümlülük de dahil olmak üzere Komisyon teklifinde çeşitli değişiklikler içeren hükümleri kabul etti.

Kabul edilen metin, reşit olmayanlara yönelik hedefli reklamların ve özel kategorilerdeki kişisel verilerin kullanımının yasaklanmasını da içeriyor. Bu hükümlerden bazıları endişe yaratmakta ve reklam teknolojisi ekosisteminin bugünkü haliyle uygulanması ve işleyişine ilişkin temel soruları gündeme getirmektedir.

Konsey'in DSA teklifine ilişkin kabul ettiği pozisyon Avrupa Komisyonu'nun metnine daha yakın olmakla birlikte, arama motorlarını da içerecek şekilde kapsamını değiştirmekte, küçüklere yönelik korumayı arttırmakta ve pazar yerleri, arama motorları ve çok büyük çevrimiçi platformlara yükümlülükler getirmektedir.

Avrupa Parlamentosu'nun metninin kabul edilmesinin ardından, Fransa Dönem Başkanlığı sırasında geçici bir anlaşmaya varmak amacıyla bir uzlaşma metnine ulaşmak için üçlü müzakereler başladı. Asıl soru şu: Kurumlar arası müzakerelerin ardından nihai metin nasıl olacak?

Dijital Piyasalar Yasası (Digital Markets Act - DMA)

Dijital Piyasalar Yasası, Avrupa Komisyonu tarafından Aralık 2020'de DSA ile aynı zamanda önerilmişti. DMA'nın amacı, adil ve rekabetçi bir çevrim içi platform ortamı ile dijital pazarlarda etkin rekabeti teşvik ederek iç pazarın iyi işlemesini sağlamaktır.

Aralık 2021'de Avrupa Parlamentosu, İç Pazar ve Tüketicinin Korunması'nın (IMCO) DMA raporuna ilişkin genel kurul oylamasını onaylayarak DMA'ya ilişkin tutumunu benimsedi.

AP tarafından onaylanan metin, web tarayıcıları, sesli asistanlar ve CTV'ler gibi daha önemli dijital hizmetleri düzenlemeye dahil ederek DMA kapsamını genişletti. Metin ayrıca "dark patterns" olarak adlandırılan uygulamaların yasaklanmasını da içeriyor.

Kabul edilen mevcut metin, bu düzenlemenin hangi büyüklük ve türdeki işletmeleri kapsadığı konusunda kapsamı daraltmaktadır. Metin, dev teknoloji şirketleri olmayan şirketlerin büyük çoğunluğunu kapsam dışında bırakacaktır.

Konsey, Aralık 2020'de Avrupa Komisyonu tarafından önerilen orijinal metne benzer bir metinle ve kullanıcıların abonelikten çıkmalarına olanak tanıyacak temel platform hizmetlerine ilave yükümlülükler getirerek Kasım 2021'de pozisyonunu kabul etti. Uzlaşma metnine ulaşma süreci Ocak 2022'de, Fransa Dönem Başkanlığı altında geçici bir anlaşmaya varılmasına yönelik DSA ile aynı amacı taşıyan üçlü müzakerelerle başladı.

Devam eden düzenleyici kurum soruşturmaları (CMA, ICO, DG COMP)

Sektör, CMA, ICO ve DG COMP tarafından yürütülen soruşturmalarda bazı yeni gelişmeler bekleyebilir. Bu soruşturmaların sonucu, Chrome tarayıcısında üçüncü parti çerezlerinin kullanımdan kaldırılmasının uygulama aşamasını veya zaman çizelgesini etkileyebilir. İngiltere Rekabet ve Piyasalar Kurumu neredeyse bir yıldır Google'ın yeni önerilerini araştırıyor.

Mayıs ayında, şirketin Privacy Sandbox'ın daha da geliştirilmesinde takip edeceğine söz verdiği ilk taahhütleri yayınladı. Yayının ardından, ilgili tarafların yorumlarını ve endişelerini iletebilecekleri bir ay süren bir danışma süreci yaşandı. CMA, 40'tan fazla tarafla görüşerek taahhütlerin belirli alanlarda güçlendirilmesini talep etti. CMA taahhütleri Şubat ayında kabul edilmiştir.

Taahhütler şunları içermektedir:

- CMA'nın rolünün ve devam eden CMA sürecinin Google'ın önemli kamuoyu duyurularında belirtilmesini sağlamak;
- Personeline müşterilere taahhütlerle çelişen iddialarda bulunmamaları talimatını vermek;
- Google'ın üçüncü taraf görüşlerini nasıl dikkate aldığına dair CMA'ya düzenli olarak rapor vermek;
- Gizlilik Bütçesi teklifinin uygulanmasının ertelenmesi ve IP adreslerine (Gnatcatcher) erişimi azaltmaya yönelik önlemlerin getirilmesi konusunda taahhütler sunmak da dahil olmak üzere, Google'ın tam Gizlilik Sandbox değişikliklerinden önce işlevselliği veya bilgileri kaldırmasına ilişkin endişeleri ele almak;
- Google'ın kullanabileceği verilere ilişkin dahili sınırların netleştirilmesi;
- Alternatif teknolojiler geliştiren üçüncü taraflara daha fazla kesinlik sağlanması;
- CMA onaylı bir takip kayyumu atanması da dahil olmak üzere raporlama ve uyum hükümlerinin iyileştirilmesi;
- Google'ın değiştirilmiş taahhütlerini kabul etmeye yönelik herhangi bir karar tarihinden itibaren 6 yıllık daha uzun bir süre sağlanması.

Bu taahhütlerin tamamı raporda yer almaktadır. CMA nihai karara daha varmadı, güncel raporları ile birlikte süreci takip ediyor.

CMA'nın raporundan bir gün önce, Birleşik Krallık Bilgi Komiseri, veri koruma yasalarına uymaları için yeni çevrimiçi reklam yöntemleri tasarlayan şirketlere uyarı niteliğinde bir Görüş yayınladı. CMA raporu yalnızca Google tarafından geliştirilen Privacy Sandbox'a odaklanırken, bu görüş çok daha geniş kapsamlı ve tüm üçüncü parti çerez alternatiflerine dokunmaktadır. ICO, "vitrin süslemesinden" kaçınmak ve insanlara kişisel verileri üzerinde gerçekten kontrol sağlamak için henüz gelişimin ilk aşamalarındayken ortaya çıkan teklifleri etkilemek istemektedir. Komiser, mevcut durumu iyileştirme ve statükoyu koruyan alternatifleri kabul etmeme isteğini açıkça vurgulamıştır. Görüşün sonunda komiser, sektöre yönelik bir dizi tavsiyede bulunmuştur:

- Tasarım seçimlerini göstermek ve açıklamak
- Faydalar konusunda adil ve şeffaf olmak
- Veri toplama ve daha fazla işlemeyi en aza indirmek
- Kullanıcıları korumak ve onlara anlamlı bir kontrol sağlamak

- Gereklilik ve orantılılık- faydalar gizlilik haklarına risk oluşturacak şekilde orantısız değildir.
- Yasallık, risk değerlendirmeleri ve bilgi hakları- çözüm uygun yasal dayanağın gerekliliklerini karşılar.
- Özel kategori verileri- çözüm özel kategori verilerinin işlenme potansiyelini ele alır.

Kaliforniya Tüketici Gizliliği Yasası (CCPA) ve Gizlilik Hakları Yasası (CPRA)

CCPA, Kaliforniya'da bir eyalet yasası olarak sunulmuş ve 1 Ocak 2020 tarihinde yürürlüğe girmiştir. CCPA, GDPR gibi kullanıcıların kişisel bilgilerinin toplanmasını ve kullanılmasını kabul etmelerini gerektirmese de belirli gizlilik bildirimlerinin ve devre dışı bırakma araçlarının uygulanmasını gerektirmektedir. Özellikle, CCPA kullanıcılara herhangi bir gizlilik bilgisi üzerinde sahiplik sağlar ve Kaliforniya kullanıcılarının kişisel olarak tanımlanabilir bilgilerini (PII) işleyen işletmelerin kullanıcıların aşağıdakileri yapmasını gerektirir:

- Hangi PII'nin toplandığını bilmek;
- PII'lerinin ifşa edilip edilmediğini ve kime ifşa edildiğini bilmek;
- Satışından vazgeçmek;
- Toplanan herhangi bir PII'ye erişmek; ve
- Toplanan PII'nin silinmesini talep etmek.

Kasım 2020'de kabul edilen CPRA, tüketicilere tanınan hakları artırarak, işletmeler için ek gereklilikler getirerek ve yeni uygulama mekanizmaları oluşturarak CCPA'yı revize etmekte ve genişletmektedir. CPRA Ocak 2023'te yürürlüğe girdi.

Kaliforniya, Amerika Birleşik Devletleri'nde bu nitelikte kapsamlı bir gizlilik yasasını kabul eden ilk eyalettir. Bununla birlikte, şu anda çeşitli inceleme ve mevzuat aşamalarında olan bir dizi başka eyalet yasa tasarısı da bulunmaktadır.

Kanada Tüketici Gizliliğini Koruma Yasası (CPPA)

CPPA, işletmelerin bu tür verileri nasıl topladığı ve işlediği üzerinde daha fazla kontrol sağlayarak kullanıcıların kişisel bilgilerine yönelik korumaları artırmak amacıyla Kasım 2020'de yürürlüğe girmiştir. CPPA, Kanada'da 2000 yılında yürürlüğe giren PIPEDA'nın (Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası) ilk büyük revizyonudur. CPPA kapsamında işletmelerin:

- Tüketicilere, kişisel verilerinin kullanımını tam olarak anlayabilmeleri ve anlamlı bir şekilde onay verebilmeleri için sade bir dille bilgi sağlamaları;
- Kullanıcılara kişisel verilerini işletmeler arasında aktarma olanağı sağlamaları;
- Kullanıcılara onaylarını geri çekme ve verilerini sildirme olanağı sağlamaları;
- Yapay zekaya dayanan ve otomatik karar verme süreçlerinden yararlanan sistemlere şeffaflık sağlamaları ve
- Kullanıcıların kişisel veri bilgilerini sildirme olanağı sağlamaları gerekmektedir.

Brezilya Genel Veri Koruma Kanunu (LGPD)

LGPD Eylül 2020'de yürürlüğe girmiştir ve Brezilya'nın bugüne kadarki ilk kapsamlı gizlilik ve veri koruma kanunudur.

LGPD, AB'nin GDPR'sini temel almaktadır ve bölgesel (yani, Brezilya'da ikamet eden kullanıcıların kişisel verilerini işleyen herhangi bir kuruluş için geçerlidir) ve maddi kapsamı açısından çok benzerdir.

Yasa kapsamında, kuruluşlar kişisel verileri işlemek için yasal bir dayanak oluşturmalıdır ve kullanıcılara erişim, düzeltme, veri taşınabilirliği vb. haklar da dahil olmak üzere GDPR kapsamındakilere çok benzer haklar tanınmaktadır. LGPD ayrıca yönetişim ve hesap verebilirlikle ilgili kurallar içermekte ve kuruluşların veri koruma görevlileri atamasını, işleme faaliyetlerinin kayıtlarını tutmasını ve ayrıntılı gizlilik bildirimleri uygulamasını gerektirmektedir.

O halde tüm bu yasalar bugün rıza ve takip için ne anlama geliyor?

1. Kullanıcılar, kişisel verilerinin/bilgilerinin dijital reklamcılık ekosisteminde nasıl kullanıldığını kontrol etmek için her zamankinden daha fazla hakka sahipler ve bu hakların giderek daha fazla farkına varıyorlar.

2. Dünya genelinde, gizlilik ve veri koruma yasal çerçevesi hızla gelişmektedir ve şirketlerin, verileri reklama ilgili amaçlarla kullanırken yasalara uymak ve kullanıcı beklentilerini karşılamak için ellerinden gelenin en iyisini yapmaları gerekmektedir.

3. Şirketlerin, web'deki kitleleri takip etmek ve hedefleyebilmek için hem teknoloji hem de politika açısından önemli iyileştirmeleri dikkate alması gerekmektedir.

4. Şeffaflık, rıza ve kişisel veri işleme yükümlülüklerine uyma ihtiyacı, üçüncü parti çerezlerinin kullanımdan kaldırılmasıyla sona ermez.

2.2 İnternet Tarayıcılarının "Bekçiliği"

Gizlilik ve bireylerin internet üzerinden takibi konusunda artan farkındalık sonucunda, yukarıda açıklandığı gibi, kişinin gizliliğini korumak için Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) ve Kaliforniya Tüketici Gizliliği Yasası (CCPA) gibi yeni düzenlemeler yürürlüğe girmiştir. Şirketler, bu yasalara uymanın yanı sıra, diğer tarafların, bireylerin kişisel verilerine/bilgilerine erişme ve bunları kullanma yöntemlerini de değiştirmektedir.

Chrome, Firefox, Edge ve Safari gibi tarayıcılar tarafından üçüncü parti çerezlerin ve birinci parti çerez geçici çözümlerinin kullanımını engellemek için yapılan değişiklikler (Chrome'da değişiklikler yapılmaya devam ediyor) yayıncılar, reklamcılar ve reklam teknolojisi şirketleri gibi diğer tarafların kişisel bilgileri/verileri toplama ve kullanma şeklini değiştirmekte, dolayısıyla pazar üzerinde bir etkiye sahip olmaktadır.

Aşağıdaki genel bakış, üçüncü parti çerez döneminin sonu olarak adlandırabileceğimiz konuyu özetlemelidir.

Safari (Apple)

Tüm tarayıcılar arasında Safari, bu tür gizlilik girişimlerinde en uzun geçmişe sahiptir. Apple'ın WebKit web tarayıcı motoru için hedefi "tüm gizli izlemeyi ve tüm siteler arası takibi önlemek için elinden gelenin en iyisini yapmaktır". Şirket, son 2 yıldır "Akıllı İzleme Önleme" (Intelligent Tracking Prevention - ITP) işlevini adım adım tarayıcılarına dahil etmektedir. Kötü aktörler, ITP'nin en son değişikliklerini aşmak için taktiklerini değiştirdikçe, Apple onların siteler arası takip becerilerini giderek azaltmaktadır.

Haziran 2017'de kullanıma sunulan ITP 1.0 ile tarayıcı içi makine öğrenimi kullanılarak üçüncü parti takip çerezlerinin çoğu engellenmiştir. O dönemde, birçok üçüncü parti takip şirketi Safari'nin üçüncü parti çerezleri üzerindeki kısıtlamalarına geçici bir çözüm olarak yeniden yönlendirmeleri kullanıyordu. Örneğin, bir kullanıcı bir haber sitesini ziyaret ediyor, takip çerezi yerleştirebileceği web sitesine yönlendiriliyor ve ardından web sitesine geri yönlendiriliyordu. Yönlendirme anlık olduğundan, kullanıcı bunun gerçekleştiğinin farkında değildi. Apple'ın makine öğrenimi, kullanıcının takip web sitesiyle etkileşimine dayalı olarak bu davranışı tespit edebiliyordu.

Sonuç olarak, kullanıcı son 30 gün içinde takip ettiği web sitesiyle etkileşime girmemişse, üçüncü parti çerezler otomatik olarak silinir ve sitedeki tüm yeni üçüncü parti çerezler engellenir. Takip eden web sitesini ziyaret ederek birinci parti çerezinin oluşturulmasına neden olduysa, bu çerez yalnızca 24 saat boyunca üçüncü parti bağlamında kullanılabilir. 24 saat sonra, çerez yalnızca birinci parti bağlamında kullanılabilir. Takip edilen web sitesine tekrar ziyaret yapılmadan geçen 30 günün ardından, çerez silinir.

ITP işlevselliği aşağıdaki şekilde güncellenmiştir:

- Mart 2018: Yasadışı takipçiler tarafından kullanılan ve siteler arası kalıcı kimlik oluşturmak için kullanılan sisteme izinsiz erişim geçişi önlenerek HTTP Strict Transport Security (HSTS) kötüye kullanımına karşı koruma eklendi.
- Haziran 2018: Birinci parti çerezlerin üçüncü parti bağlamında kullanılabileceği 24 saatlik zaman aralığı ortadan kaldırıldı.
- Şubat 2019: Tüm üçüncü parti takip çerezler engellendi ve birinci parti çerezlerin yaşam döngüsü 7 günle sınırlandı.
- Nisan 2019: İstemci tarafı birinci parti çerezler için maksimum süre sonu, sitedeki gezinti bir "takip web sitesi" aracılığıyla olduğunda, 24 saate düşürüldü.
- Eylül 2019: İstemci tarafı birinci parti çerezlerin 24 saat sonra geçerliliğini yitirmesi, böylece tüm "komut dosyası tarafından (script) yazılabilir" web sitesi verilerinin (özellikle LocalStorage) 7 gün sonra geçerliliğinin sona erdirilmesi sağlandı.

- Haziran 2020: Webkit yeni, isteğe bağlı bir teknoloji olan App-Bound Domains'i duyurdu. App-Bound Domains özelliği, bir uygulamanın uygulama içi tarama sırasında kullanıcıları takip etmek için güçlü API'leri kullanabileceği etki alanlarını sınırlandırarak kullanıcı gizliliğini korumak için adımlar attı. Sonuç olarak, uygulama içi tarayıcılarda alanlar arası kullanıcı takip olasılığını sınırlandırmakta.
- Kasım 2020: Webkit, CNAME gizleme savunma özelliğini macOS Big Sur, Catalina ve Mojave, iOS 14 ve iPadOS 14'teki Safari 14'te ITP'ye yayınlayacağını duyurdu. Üçüncü parti CNAME ile gizlenmiş bir HTTP yanıtı tarafından oluşturulan tüm çerezler 7 gün içinde sona erecek şekilde ayarlanmakta. Bu, etki alanlarının üçüncü parti çerezlerini birinci parti çerezleri olarak kullanma becerisini sınırlamakta.
- Haziran 2021: Apple, iOS 15, iPadOS 15, macOS Monterey ve watchOS 8 ile gizlilik konusundaki liderliğini ilerletti. Mail uygulamasında Mail Gizlilik Koruması, gönderenlerin kullanıcı hakkında bilgi toplamak için görünmez pikseller kullanmasını engellemekte. Yeni özellik, kullanıcıların gönderenlerin bir e-postayı ne zaman açtıklarını bilmelerini engellemelerine yardımcı oluyor ve IP adreslerini maskeliyor, böylece diğer çevrim içi etkinliklerle ilişkilendirilemiyor veya konumlarını belirlemek için kullanılamıyor. Akıllı Takip Önleme, kullanıcının IP adresini de takipçilerden gizleyerek daha da güçleniyor. Bu, kullanıcının IP adresini, web sitelerindeki etkinliklerini birbirine bağlamak ve onlar hakkında bir profil oluşturmak için benzersiz bir tanımlayıcı olarak kullanamayacakları anlamına gelmekte.

ITP 2.3 ile sonuçlanan bu güncellemeler, Safari'de hedeflenmiş reklamları ortadan kaldırmış ve sadece Yayıncılar için gelir düşüşüne yol açmakla kalmamış, aynı zamanda bu cihazları birçok reklam kampanyasından da çıkarmıştır.
Not: ITP, uygulama mağazasındaki tüm uygulamalar için geçerlidir. ITP, Apple arama reklamları sistemi (uygulama mağazasındaki uygulamaları tanıtmak için oluşturulmuştur) için de geçerlidir. Reklam Takibini Sınırlama ve Kişiselleştirilmiş Reklamlar hakkında daha fazla bilgiyi burada bulabilirsiniz.

Mozilla Firefox- Gelişmiş İzleme Koruması (ETP)

Firefox, kendisini güçlü gizlilik korumaları sağlayacak şekilde konumlandırmak üzere önemli bir hamle yapmıştır. Mozilla'nın İzlenmeyi Önleme Politikası, engellemeyi amaçladığı kullanımlarla ilgili olarak hedeflerini sıralamaktadır, halihazırda bunlardan yalnızca bazıları çalışmaktadır. Apple gibi, onların da hedefleri gizli veya siteler arası takip imkanını ortadan kaldırmaktır.

Mozilla'nın çerez sınırlaması sürümü "Gelişmiş İzleme Koruması" (ETP) olarak adlandırılmaktadır. Mozilla ilk olarak, Ekim 2018'de v63 ile disconnect.me URL listesine dayalı olarak, üçüncü parti çerezlerini engellemek üzere beta sürümlerinde kullanıma sunulan öntanımlı bir ETP etkinleştirmesininin duyurusunu yapmıştır.

Öntanımlı etkinleştirme, ETP'nin kendisi devre dışı bırakılmış modda olduğu halde, Ocak 2019'daki v65'e kadar aktif olmamıştır.

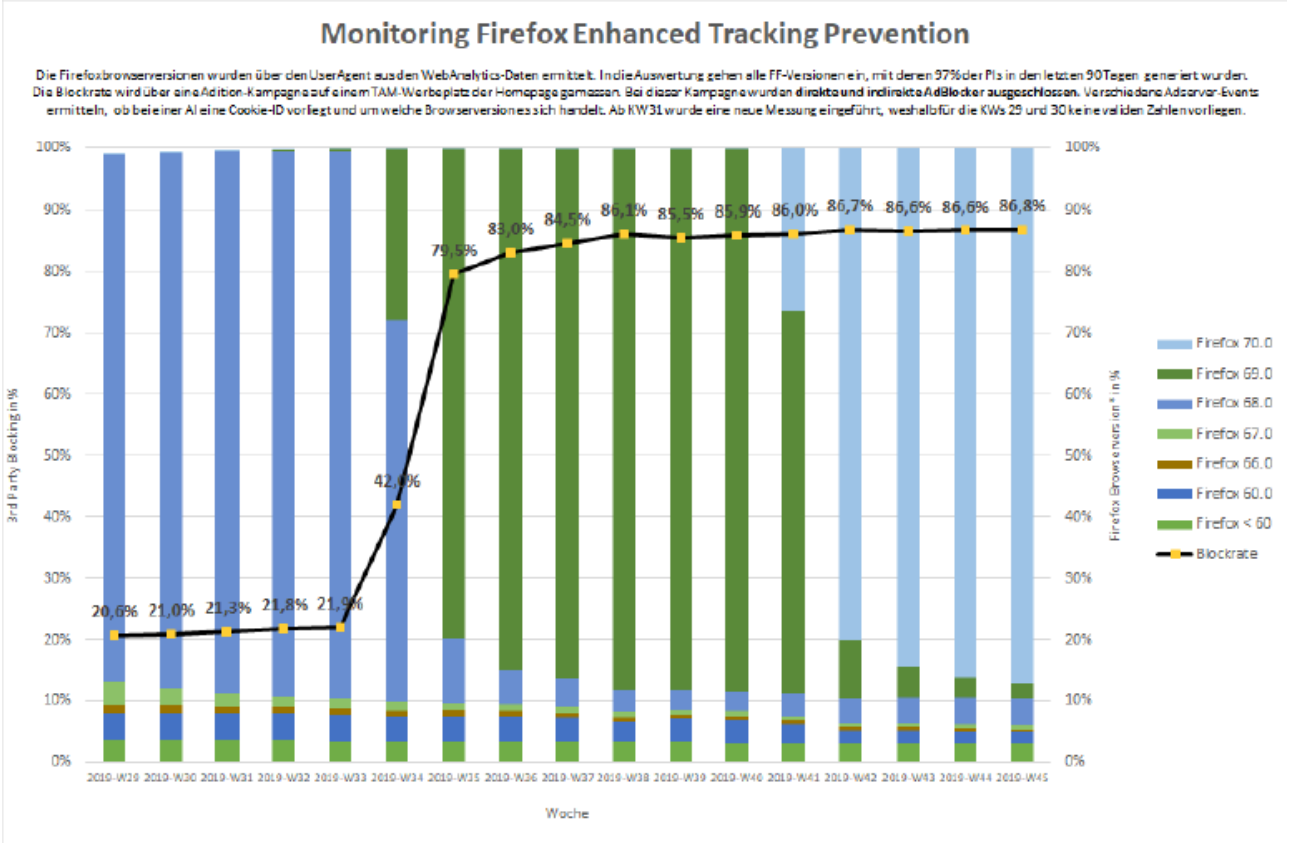
Mozilla, bu özelliği şu şekilde tanımlamaktadır: Basitleştirilmiş içerik engelleme ayarları, kullanıcılara online takipçileri denetlemek için standart, sıkı ve özelleştirilmiş seçenekler sunmaktadır. Site bilgi panelindeki yeniden tasarlanmış içerik engelleme bölümü (adres çubuğundaki küçük "i" simgesi genişletilerek görüntülenir), Firefox'un ziyaret ettiğiniz her web sitesinde neyi algıladığını ve engellediğini göstermektedir.

Haziran 2019'da Mozilla, tüm "yeni" kurulumlar için varsayılan olarak ETP özelliğini etkinleştirerek v67.0.1'i takip edip Firefox'taki üçüncü parti çerez engelleme oranını sonraki aylar için yaklaşık % 20'ye yükseltmiştir.

Sonuç olarak, Mozilla Eylül 2019'un başında, tüm "mevcut" kurulumlar için varsayılan olarak ETP özelliğini v69 sürümünde etkinleştirmiştir. Bu durum, birkaç hafta içinde kullanıcıların %80'ine kadarında üçüncü parti çerezlerinin engellenmesini sağlamıştır.

Bu çözüm, gizli gezinti veya tüm gezintiler sırasında sıkı koruma modundayken izleme yaptığı bilinen web sitelerini içeren kara listeyi kullanmaktadır. ETP, izlemeler için yalnızca çerezleri engellemekle kalmaz, aynı zamanda bu sitelere yapılan gerçek çağrıları da engeller. Kullanıcılar, ikinci listeyi kullanan ve yalnızca gizli gezinti için değil tüm gezinti için çağrı engellemeyi etkinleştiren sıkı moda kolayca geçebilirler. Ancak sıkı mod, birçok web sitesini (örneğin, kullanıcı tarafından görülebilen işlevselliği yüklemek için Adobe Launch veya Dinamik Etiket Yönetimi ürünlerini kullanan siteler) kapatır. Gizli modda, kullanıcılar daha az kısıtlayıcı olan listeyi kullanmayı seçebilir, ancak her zaman etkinleştirebilirler veya 3P izleme çerezlerini engellemeyi seçebilir, ancak aramalara izin verebilirler. Mozilla'nın finansmanının ezici çoğunluğunun çerezlere dayanmayan arama reklamlarından elde edildiğini belirtmek önemlidir.

2019'da Mozilla Firefox için ölçülen üçüncü parti çerez engelleme oranı



ETP'nin işlevselliği daha sonra aşağıdaki şekilde güncellenmiştir:

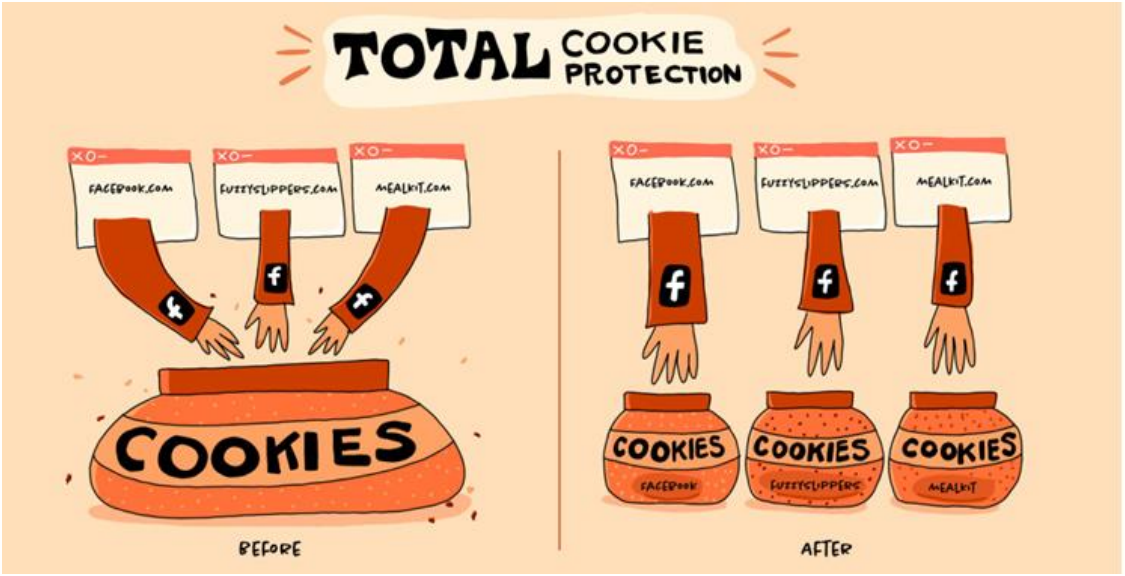
Ocak 2020: Firefox 72 üçüncü taraf parmak izi kaynaklarını engeller. Firefox 72, parmak izine katıldığı bilinen şirketlere yönelik tüm üçüncü taraf isteklerini engelleyerek kullanıcıları parmak izine karşı korur. Bu, söz konusu tarafların JavaScript kullanarak bir kullanıcının cihazının özelliklerini incelemesini engeller. Ayrıca, kullanıcının IP adresi veya kullanıcı aracısı başlığı gibi ağ istekleri yoluyla ortaya çıkan bilgileri almalarını da engeller.

Ağustos 2020: Firefox 79, yönlendirme takibine karşı korumalar içerir. Geliştirilmiş Takip Koruması 2.0 ile Firefox, sıçrama takip olarak da bilinen yeniden yönlendirme takip adı verilen yeni bir gelişmiş takip tekniğini engelleyecektir. ETP 2.0, kullanıcının düzenli olarak etkileşimde bulunduğu siteler hariç olmak üzere, takip sitelerindeki çerezleri ve site verilerini her 24 saatte bir temizler.

Ocak 2021: Firefox 85, Supercookies kullanımını sınırlar. Supercookies, kullanıcı tanımlayıcılarını saklamak için sıradan çerezlerin yerine kullanılabilir, ancak silinmesi ve engellenmesi çok daha zordur. Yıllar geçtikçe, kullanıcıların tanımlayıcılarını Flash depolama, ETag'ler ve HSTS bayrakları da dahil olmak üzere tarayıcının giderek daha belirsiz kısımlarında süper çerezler olarak depoladıkları tespit edildi.

Şubat 2021: Firefox 86, Toplam Çerez Korumasını Sundu. Toplam Çerez Koruması, kullanıcının ziyaret ettiği her web sitesi için ayrı bir "cookie jar" tutarak çalışmaktadır.

Bir web sitesi veya bir web sitesine gömülü üçüncü parti içeriği, kullanıcının tarayıcısına bir çerez bıraktığında, bu çerez, başka herhangi bir web sitesiyle paylaşılmasına izin verilmeyecek şekilde o web sitesine atanan cookie jar ile sınırlandırılmaktadır. Toplam Çerez Koruması, popüler üçüncü parti, oturum açma sağlayıcıları tarafından kullanılanlar gibi takip dışı amaçlar için gerekli olduklarında siteler arası çerezler için sınırlı bir istisna yapmaktadır. Yalnızca Toplam Çerez Koruması kullanıcının bir sağlayıcı kullanmak istediğini tespit ettiğinde, o sağlayıcıya özellikle ziyaret ettiği site için siteler arası çerez kullanma izni verecektir. Bu tür anlık istisnalar, kullanıcının tarama deneyimini etkilemeden güçlü bir gizlilik koruması sağlar. Ocak ayında duyurulan Supercookie Korumaları ile birlikte Toplam Çerez Koruması, Firefox'taki web siteleri arasında çerezlerin ve diğer site verilerinin kapsamlı bir şekilde bölümlenmesini sağlamıştır. Bu özellikler birlikte, web sitelerinin bir kullanıcının tarayıcısını "etiketlemesini" önleyerek en yaygın siteler arası takip tekniğini ortadan kalkmıştır.



Şekil 4: Toplam Çerez Koruması. Kaynak:

https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/

Mart 2021: Firefox 87 varsayılan olarak HTTP Yönlendiricilerini kırpar. Firefox, sitelerin yanlışlıkla hassas kullanıcı verilerini sızdırmasını önlemek için varsayılan olarak yönlendiren başlıklarından yol ve sorgu dizesi bilgilerini kırpmıştır. HTTP Yönlendirici başlığı genellikle özel kullanıcı verileri içerir: Bir kullanıcının yönlendiren web sitesinde hangi makaleleri okuduğunu ortaya çıkarabilir veya bir kullanıcının bir web sitesindeki hesabına ilişkin bilgileri içerebilir.

Mart 2021: Firefox 87, SmartBlock adlı yeni bir gizlilik özelliğini tanıttı. SmartBlock, takip korumaları tarafından bozulan web sayfalarını akıllıca düzeltmiştir.

Nisan 2021: Firefox 88, window.name gizlilik ihlallerini azalttı.

İzleme şirketleri, window.name özelliğini web siteleri arasında veri taşımak ve siteler arası takibi mümkün kılmak için bir iletişim kanalına dönüştürdü. Firefox, kullanıcı web siteleri arasında gezindiğinde window.name özelliğini temizlemeye başladı.

Haziran 2021: Firefox 89, özel taramada varsayılan olarak siteler arası çerez takibini engelledi. Firefox 86'dan bu yana, ETP Sıkı Modu etkin olan kullanıcılar için Toplam Çerez Koruması mevcuttu. Firefox 89 ile aynı koruma Özel Tarama pencerelerine de genişletildi.

Temmuz 2021: Firefox 90, Özel Tarama için SmartBlock 2.0'ı sundu. SmartBlock 2.0, kullanıcının web sitelerinde oturum açmak için üçüncü parti Facebook giriş düğmelerini kullanmaya devam edebilmesini sağlarken, siteler arası takibe karşı da koruma sağladı.

Ağustos 2021: Firefox 91 Geliştirilmiş Çerez Temizleme özelliğini sundu. Firefox Strict Mode'un yeni sürümü, kullanıcıların bir web sitesi veya web sitesine gömülü herhangi bir izleyici tarafından bilgisayarlarında depolanan tüm çerezleri ve süper çerezleri kolayca silmelerini sağladı.

Ekim 2021: Firefox 93, geliştirilmiş bir SmartBlock ve yeni Yönlendiren İzleme Korumaları içeriyor. Sürüm 93'ün yayınlanmasıyla birlikte Firefox, siteler arası istekler için 'no-referrer-when-downgrade', 'origin-when-cross-origin' ve 'unsafe-url' gibi daha az kısıtlayıcı yönlendirici ilkelerini göz ardı etmeye başladı. Firefox, web sitesinin ayarlarından bağımsız olarak siteler arası istekler için HTTP yönlendiricisini her zaman kırpmaya başladı. Aynı site istekleri için, web siteleri hala tam yönlendirici URL'sini gönderebilir. Bu, web sitelerinin takip şirketleriyle iş birliği yaparak takibin engellenmesini atlamayı imkansız hale getirdi.

Ekim 2021: ISRG'den Tim Geoghegan, Cloudflare'den Christopher Patton ve Christopher Wood ve Mozilla'dan Eric Rescorla (Firefox CTO'su), gizliliği koruyan ölçüm için bir protokol öneren bir Gizlilik Koruma Ölçümü taslağı yayınladı. Taslak öneri, büyük bir istemci grubunun, girdileri kendileri öğrenmeden bir istemcinin girdileri üzerinden toplu istatistikleri hesaplayan küçük bir sunucu grubuna bağlı olduğu konseptine dayanmaktadır. Taslakta yazarlar, akış ve buna dahil olan rollerin yanı sıra riskleri ve bunlara yönelik potansiyel hafifletmeleri önermekte ve tartışmaktadır. Bu makale, Mozilla'dan önemli bir temsilcinin (Firefox'un CTO'su) dahil olduğu ve şirketin hangi yönü takip etmek istediğini gösteren ilk büyük teklif olması nedeniyle özel bir öneme sahiptir.

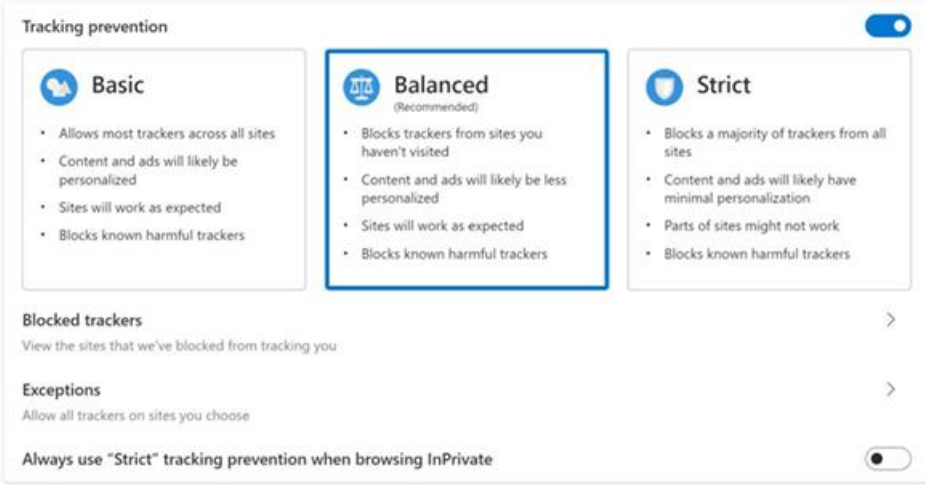
Ocak 2022: Meta ve Mozilla arasında işbirliği - Ben Savage (Meta), Erik Taubeneck (Meta) ve Martin Thomson (Mozilla), reklam ilişkilendirmesi için mevcut çözümlerin ötesine geçen ve tarayıcı satıcıları arasında potansiyel birlikte çalışabilirlik sunan bir IPA önerisi yayınladı. Bu teklif, Gizlilik Koruma Ölçümü gibi diğer tekliflerden önemli parçalar almayı amaçlamaktadır.

Edge (Microsoft)

Microsoft, Haziran 2019'da post edilen bir blog yazısında "Microsoft Tracking Prevention" (MTP)'nin kullanıma sunulduğunu duyurmuştur. İşlevsel anlamda Firefox'un Gelişmiş

İzleme Önleme işlevine çok benzemekte ve disconnect.me'deki açık kaynak kodunu paylaşabilmektedir. MTP temel, dengeli (önerilen) ve sıkı olarak üç ayrı koruma seviyesi sunmaktadır. Dengeli varsayılan seviyedir. Firefox'tan farklı olarak, MTP'nin özelleştirilmiş bir modu yoktur ve InPrivate modunda farklı davranmamaktadır. ETP gibi, üçüncü parti çerezler bilinen izleme sitelerinden ve sıkı modda bu sitelere yapılan çağrılar engellenir.

MTP'nin lansmanı, 15 Ocak 2020'de piyasaya sürülen Microsoft'un Edge Sürüm 80 ile yapılmıştır. Microsoft'a göre, üç takip önleme modu (özellikle Sıkı mod), "parmak izi alınmasına" (fingerprinting) yol açan kişiselleştirme türüne karşı korunmaya yardımcı olacaktır. Edge, reklamları doğrudan engellememekte, ancak reklam engelleme uzantıları indirilebilmektedir. Tarayıcı artık Chromium'u temel aldığından, birçok Chrome uzantısı (ve ayrıca Microsoft Store'daki uzantılar), ciddi bir avantaj olan Edge'in bu en son sürümüyle çalışacaktır.



Şekil 5: Microsoft İzleme Önleme (MTP).

Ocak 2021 MTP güncelleştirmeleri: Microsoft Edge 88 ile kullanıcılar konum, kamera ve mikrofon erişimini hangi sitelerle paylaşacaklarını denetleyebilir. Kullanıcılar site izinlerini gözden geçirebilir, düzenleyebilir ve sıfırlayabilir, ayrıca yakın zamanda hangi izinlerin değiştiğini görebilir. Yalnızca üçüncü parti çerezlerini silme seçeneği sunuldu.

Chrome (Google)

Chrome, Mayıs 2019'da gizlilik ve güvenliğin bazı yönlerini iyileştirmek için çerez etiketlemesinde bir değişiklik yaptığını duyurdu. Şubat 2020'de Chrome, üçüncü parti çerezlerinin "SameSite=None" ve "Secure" ile etiketlenmesini gerektiren yeni bir güvenlik özelliğini kullanıma sunmaya başladı. SameSite=None özelliği mevcut olduğunda, siteler arası çerezlere yalnızca HTTPS bağlantıları üzerinden erişilebilmesi için ek bir Secure özelliği kullanılmalıdır.

Ağustos 2019'da Chrome, insanların gizliliğini korumak ve gizli takibi önlemek için yeni dijital reklam araçları geliştirerek "web'de gizliliği temelden geliştirmek için bir dizi açık standart geliştirmek" amacıyla yeni bir girişim (Privacy Sandbox) duyurdu. Ocak 2020'de Chrome, önümüzdeki iki yıl içinde Chrome'da üçüncü parti çerezleri için desteği aşamalı olarak kaldırmayı planladığını duyurdu.

Haziran 2021'de Chrome, zaman çizelgesinde bir güncelleme yaptığını duyurdu ve privacysandbox.com adresinde üçüncü parti çerezlerinin ne zaman kaldırılacağına ve gizliliği koruyan alternatiflerle değiştirileceğine dair herkese açık bir zaman çizelgesi hazırladı. Privacy Sandbox, Chrome'un dijital reklamcılık endüstrisi için önerdiği alternatif bir yolu temsil etmektedir. Chrome, ekosistem tarafından görüntülenebilecek ve benimsenebilecek, aşağıdaki kullanım durumlarını ele alan çeşitli API'ler önermiştir: Web'de spam ve dolandırıcılıkla mücadele; alakalı içerik ve reklamların gösterilmesi; dijital reklamların ölçülmesi; siteler arası gizlilik sınırlarının güçlendirilmesi; ve parmak izi ve ağ düzeyinde takip gibi gizli takip tekniklerini ele alan API'ler. API'ler hakkında daha fazla bilgi privacysandbox.com ve developers.chrome.com adreslerinde bulunabilir.

Chrome, Mart 2021'den Temmuz 2021'e kadar, benzer tarama düzenlerine sahip büyük insan gruplarını kümeleyerek insanlara alakalı içerik ve reklamlarla ulaşmanın bir yolu olan Federated Learning of Cohorts API'nin (FLoC) ilk sürümü için bir kaynak denemesi gerçekleştirdi. Chrome, daha ileri ekosistem testlerine geçmeden önce FLoC'nin ilk kaynak denemesinden gelen geri bildirimleri değerlendiriyor.

FLEDGE önerisi (First "Locally-Executed Decision over Groups" Experiment) yeniden pazarlama kullanım durumları için bir öneridir. 27 Ocak 2022 tarihinde Chrome, yeniden pazarlama ve reklamveren tanımlı kitleleri desteklemek için Gizlilik Korumalı Alanı önerisi olan FLEDGE için önerilen bir test planı yayınladı. Bu ilk deneme önerisi, karmaşıklığı azaltmak ve geliştiricilerin zaman içinde eklenen ek özellikler ve gereksinimlerle birlikte temel özellikleri test etmeye başlamasını sağlamak için tasarlanmıştır. Attribution Raporlama API'si, siteler arası tanımlayıcıları kullanmadan kullanıcı eyleminin (reklam tıklaması veya görüntüleme gibi) ne zaman bir dönüşüme yol açtığını ölçmek için bir yol sunar.

Chrome, privacysandbox.com/timeline adresinde ve kaynak deneme sayfasında belirtildiği üzere 2021 yılında Privacy Sandbox API'leri için bir dizi kaynak denemesini kullanıma sunmuştur. Buna ek olarak, Privacy Sandbox'taki aylık blog Progress, en son gelişmelerden haberdar olmak için bir yol sunmaktadır.

2.3 Reklam Engelleme (Ad Blocking)

Bir tarayıcıda reklam engelleme, bir web sitesinde veya web sayfasında görüntülenen online reklamları ortadan kaldıran bir özelliktir. En yaygın reklam engelleme araçları tarayıcı uzantılarıdır. Yıllar içinde tarayıcılar, reklam engelleme uzantılarının temel özelliklerini tarayıcı sürümlerine dahil etmeye başlamıştır.

Bunun en iyi örneği, Eylül 2019'un başında Firefox Sürüm 69'un kullanıma sunulmasıyla birlikte ön tanımlı olarak etkinleştirilen Mozilla Firefox "Gelişmiş İzleme Koruması"dır (ETP)

Son yıllarda, reklam engelleme de giderek artan bir şekilde uygulama ekosistemine dahil edilmekte, ancak dünya çapında hala tarayıcılara kıyasla yeterince ilgi çekmemektedir.

Bugün, reklam engellemenin ve izleme komut dosyası engellemenin bu araçların iki temel özelliği olduğu görülmektedir. Genel anlamda, disconnect.me (Firefox ETP tarafından kullanılır) veya easylist.to (Adblock Plus tarayıcı uzantısı tarafından kullanılır) gibi genel olarak yönetilen harici URL kara listelerini baz almaktadırlar.

Ancak, reklamı ve takibi filtrelemek için kullanılan AI odaklı yaklaşımlar da bulunmaktadır.

Bu araçlar ya ad tag dağıtımını ya da takip ve profil oluşturma amacıyla kullanıldığı bilinen komut dosyası alanlarının yüklenmesini engeller. Takip veya reklam engelleme araçlarının hemen hemen tamamı her iki özelliği de barındırdığından, iki yöntem de an itibariyle net değildir.

Ortalama reklam engelleme oranı pazara göre değişir. ve reklam engelleme ve izleme komut dosyası araçlarını kullanmanın en yaygın nedenleri şunlardır:

- Gizlilikle ilgili endişeler (kişisel veri sızıntısı)
- Güvenlik amaçlı (ör. kötü amaçlı yazılım)
- Web sitelerinin daha hızlı yükleniyor olması
- İçerikte daha az dikkat dağıtıcılık
- Bant genişliğinden tasarruf (özellikle mobil cihazlarda)
- Pil tasarrufu

"Doğrudan" reklam engelleyicilerin yanı sıra, bir tarayıcı veya tarayıcının uzantısı özelliği olarak, daha az bilinen bir faktör, virüs tarayıcı uygulamaları tarafından sunulan dolaylı reklam engelleyicilerdir. Kullanıcıların bunu devre dışı bırakması veya etkilemesi adına kolay bir seçenek olmaksızın, trafik filtrelemesi veya uzantı yükleme özelliği sunarlar.

BÖLÜM 3- SAHİPLİ PLATFORMLARIN PAYDAŞLARIN KULLANIMI ÜZERİNDEKİ ETKİSİ

Dijital reklamcılık sektörü daha önce, veri gizliliği çözümlerindeki ve düzenlemelerdeki sallantılı değişikliklerin, sahipli platformlara yanlışlıkla daha fazla hakimiyet imkânı sağladığını gözlemlemiştir.

Sahipli, özel bir platform, normal gerçek zamanlı açık artırma (openRTB protokolüne dayanan) ekosisteminin dışında yer alan herhangi bir satın alma noktasıdır ve bu ekosistemin dışındaki medya, veri veya satın alma fırsatlarının kullanımına imkân verir.

Geçmişte birçok büyük yayıncı, envanterlerinin daha seçkin alt kümelerini (ör. Ana sayfa başlığını) doğrudan/özel olarak satardı. Programatik, yayıncıların geniş ölçekte satış yapmalarına ve envanterlerinin geri kalanından (doğrudan satışını daha zor buldukları bölümlerden) gelir artışı elde etmelerine yardımcı olmanın bir yolu olarak başlamıştır. Sahipli platformlar artık büyük yayıncılardan (veya yayıncı gruplarından), veri şirketlerinden, talep platformlarından ve hatta ajanslardan çıkmaya başlamaktadır. Üçüncü parti çerezlerin olmadığı bir ekosistemde, sahipli platformlar, önemli miktarda birinci parti verilerine dayalı hedefleme sunabileceklerdir.

3.1 Sahipli Platformlar ve Reklamverenler

Reklamverenler için ölçek ve rekabetçi fiyatlandırmayı, yayıncılar için optimize edilmiş talebi ve tüketiciler için artan içerik seçeneklerini desteklemek için açık internete yatırım yapmak giderek daha önemli hale geliyor. Bu nedenle, reklamverenlerin tüketicilere ulaşmak için sadece sahipli platformlara bağımlı hale gelmemeleri önemlidir. Bu durum hem erişimi hem kontrolü ve şeffaflığı etkileyebilir.

Erişim: Tüketiciler içeriğe hem sahipli platformlardan hem de açık internet üzerinden ekranlar ve platformlar arasında eriştiğinde, izleyicilerin ilgisi giderek dağılmaktadır. Reklamverenler bütçelerinin çoğunu bu platformlara yatırıyorlarsa, kitleleriyle geniş ölçekte bağlantı kurma fırsatlarını kaçırma riskiyle karşı karşıya kalırlar.

Kontrol ve şeffaflık: Sahipli platformlar, log seviyesindeki verilerin paylaşımını engelleyerek, satın alıcıların platformlar tarafından sağlananların dışındaki verileri doğrulama imkanını kısıtlar. Log seviyesindeki verilerin olmaması, bu platformlar tarafından sağlanan sonuçların doğrulanmasını zorlaştırır. Ayrıca, satın alıcıların sonuçları birden çok platformdan karşılaştırma ve ilişkilendirme imkanını engelleyerek bu tür analizlerin değerini düşürür ve rekabeti tıkar.

3.2 Sahipli Platformlar ve Yayıncılar

Üçüncü parti çerezlerinin kaybı, daha az sayıda alıcının belirli reklam alanlarına verdikleri tekliflerin değerini anlaması nedeniyle yayıncılar üzerinde artan bir baskı oluşturacak ve bu da toplam geliri etkileyecektir.

Yayıncılar terimini kullandığımızda, kendi içeriğini oluşturan herhangi bir siteden bahsettiğimizi belirtmek önemlidir. Bu, YouTube, Twitter, Instagram, Facebook gibi içeriği kendileri için oluşturması için tüketicisine bağımlı olan ve kendi oturum açmış kullanıcı çözümlerine sahip oldukları için üçüncü parti çerezlerine de güvenmeyen platformlardan farklıdır.

Çok sayıda reklamverenin, bu siteler arası tanımlayıcının yokluğunda frekans sınırlama ve kitle hedefleme gibi kullanım durumlarını uyarlaması gerekecektir, ancak gelecekte bunları desteklemek için gizliliği koruyan teknolojileri (doğrudan veya reklam teknolojisi sağlayıcıları aracılığıyla) kullanabilmelidir.

Birçok yayıncı hâlâ, yayıncıların birinci taraf verilerini premium yayıncılardan oluşan bir ağda kullandığı kitle genişletmeye güvenmektedir. Ancak, üçüncü parti çerezlere yönelik destek aşamalı olarak kaldırıldığında, yayıncıların bunun ve üçüncü parti bağlamında ayarlanan çerezlere dayanan diğer kullanım durumlarının gizliliğini koruyan alternatif teknolojiler kullanılarak nasıl sunulabileceğini düşünmeleri gerekecektir.

Yayıncıların, tüketicileri için harika bir kullanıcı deneyimi yaratmaları, reklamverenler için bir veri çözümü sunmaları ve sürdürülebilirlik ve şeffaflık sağlamak için sahipli platformlara bağımlılıklarını en aza indirmelerini sağlayacak bir denge bulmaları çok önemlidir. Yine de bu, kullanıcı için şeffaflık ve kontrol hissi korunarak gerçekleştirilmelidir.

3.3 Sahipli Platformlar ve Tüketiciler

Açık bir internet seçeneği olmayan tüketiciler, premium içeriği kullanmak için giderek daha fazla ödeme yapmak zorunda kalacaklar veya sahipli platformlar aracılığıyla erişim sağlayacaklardır. Haberlere sadece sahipli bir platformdan bakılabilecek bir dünya hiç de hoş olmayacaktır. Aslında, interneti bu kadar değerli kılan, çeşitli kaynaklardan ücretsiz kaliteli içeriğe erişimdir. Tüketiciler çok seçenek ve herkese açık güvenilir haber sitelerine erişim imkânı istemektedirler. Reklamlarla finanse edilen "ücretsiz" içeriğe erişebilme veya içerik için ödeme yapma seçeneğine sahip olmak istiyorlar - içerik tüketimine hibrit bir yaklaşım.

Özetle, reklamverenler ve yayıncıların, üçüncü parti çerezlerini çoğaltmaya veya bu çerezler için bir "geçici çözüm" bulmaya çalışmak yerine, doğrudan tüketiciye temas noktalarından elde edilen birinci parti verilerinden maksimum değer elde etmeleri ve faaliyetlerini sahipli platformların ötesinde çeşitlendirmeleri çok önemlidir.

Bunu yaparken, müşterilerine içerik kullandıkları her yerde başarılı bir şekilde ulaşma konusundaki mevcut güçlerinin farkına varacak ve reklamın bir sonraki evriminde internette envanterlerinden gelir elde edeceklerdir.

BÖLÜM 4- REKLAM DOĞRULAMA (AD VERİFİCATİON) VE ÖLÇÜMLEME ÜZERİNDEKİ ETKİSİ

Sektör olarak online reklam formatlarının 1994 yılında oluşturulmasından bu yana, teknolojiler ve reklamcılık imkanları sürekli değişmektedir. Çerezlerin ortadan kalkması sektördeki son önemli değişiklik olsa da reklam doğrulama ve ölçümleme konuları kesinlikle çerezlerin olmadığı bir dünyaya adapte olabilir, hatta olmaya başlamıştır.

4.1 Reklam Doğrulama

Birçok reklam doğrulamasının sahtekarlığı tespit etmek, marka güvenliği sağlamak veya görüntülenebilirliği ölçmek için çerezlere ihtiyacı yoktur. Bu nedenle, doğrulama çözümleri eskisi gibi devam edebilecektir. Tavsiyemiz, güvenilir doğrulama sağlayıcılarınıza danışmanız ve çözümlerinin üçüncü parti çerezlerine bağlı olup olmadığını onaylamalarını istemenizdir. Bu durum, ürün gruplarının gelecekte kullanıma uygun olup olmadığını anlamanızı sağlayacaktır.

4.2 Ölçümleme

Ölçümleme uygulamalarındaki temel değişiklik, artık online reklamlara maruz kalma durumunu belirlemek için üçüncü parti çerezlerine güvenememizdir. Bununla birlikte, üçüncü parti çerezlerinin 2022 yılı içerisinde tamamen ortadan kalkmayacağını, bu nedenle bazı durumlarda çerez verilerinin ve diğer kaynakların bir karışımının mümkün olabileceğini unutmamak gerekir.

Bu yeni dünyada, dijital reklamcılık yatırımlarının etkisini anlamak için aşağıdakileri de içeren çeşitli ölçüm yaklaşımları olacaktır:

1. Reklama maruz kalma verisini ve etkileşim verilerini eşleştirmek üzere, yayıncılar, network'ler ve ölçüm şirketleri ile ortaklıklar kurulabilir. Bu entegrasyonlar, ileride yayıncılar arası ve cihazlar arası ölçümlemelere imkân verebilir.

2. Reklama maruz kalma takibinin mümkün olmadığı yerlerde, maruz kalma olasılığını modellemek için görme fırsatı (OTS) veya spesifik medya kullanımı soruları hala kullanılabilir. Bazı durumlar ve bazı pazarlar için bu, kampanyanın etkisini ayrı tutmak için en uygun yöntem olabilir. Olasılıksal maruz kalma (probabilistic exposure) yaklaşımları, pasif maruz kalma yaklaşımlarıyla giderek daha fazla harmanlanacaktır. Ayrıca, olasılıksal tahminlerin doğruluğunu daha da arılaştırmak ve iyileştirmek için pasif yaklaşımlara karşı doğrulamalar kullanılacaktır.

3. Kontrollü olarak reklam gösterimine maruz kalmayı içeren (online veya yüz yüze) araştırmalar, içeriğin etkinliğini birden çok ve farklı medya bağlamında karşılaştırmak için giderek daha fazla kullanılmaktadır.

   Bu yaklaşım aynı zamanda çerezlerle ölçülmesi her zaman zor olan içeriği ölçmek için de kullanılmaktadır (ör. Influencer içeriği veya sponsorluklar).

4. Telco onaylı geçici tanımlayıcılarla çalışmak, kitle etkileşimini ölçmek ve eylem sonuçlarını belirlemek için reklam sürecini genişletebilir.

5. Gelişmiş analitik, toplam yatırım getirisini anlamak amacıyla çeşitli veri kümelerine

(anket, satış ve medya harcaması/dağıtım verileri gibi) dayalı olarak kampanya etkisini modellemek için şu anda kullanılmaktadır ve kullanılmaya devam edilebilir. Aynı şekilde, kitle katılımını ve kampanyaların gerçek etkisini anlamanın en etkili yollarından biri olan dikkat sinyallerini ölçme konusunda da henüz kullanılmamış bir fırsat bulunmaktadır.

6. Reklamverenler, etkiyi ortadan kaldırmak için A/B testi gibi daha deneysel tasarımlar kullanabilir (örneğin, basit ölçümlemeyi sağlamak için görünmeyen bir kısmı olan medya planları tasarlamak).

7. Kullanıcılarının platformlarındaki maruziyetini belirleyebilen ve canlı ortamlarında anketler ("polling") sunabilen yayıncılarla tek site analizi için çalışma imkânı yine devam edecektir.

8. Amaca yönelik olarak oluşturulmuş pasif maruz kalma takip panelleri ile daha özelleştirilmiş yaklaşımlar geliştirilebilir (örneğin, mobil ölçüm kullanılarak), ancak yönetim maliyetleri düşürülünceye kadar kapasite düşük kalacaktır.

En uygun yaklaşımın ne olduğu, bir reklamverenin ölçümlemek istediği aktiviteye, ölçümleme pazarındaki farklı yaklaşımların uygulanabilirliğine, pazarlarında ve markalarında mevcut olan veri kümeleri ve ortaklıklara ve ölçüm için mevcut yatırım düzeyine bağlı olacaktır.

Önümüzdeki yıllarda sektör değişmeye devam ettikçe, başka yöntemler geliştirmek de mümkün olabilecektir.

4.3 Attribution

Ölçümün değişme şekli, reklamverenlerin ilişkilendirmeyi nasıl yürüteceğini de etkileyecektir. Bazı teklifler hiçbir tanımlayıcı içermeyecek, bazıları bir, bazıları ise birden fazla tanımlayıcı içerecektir. Bir reklamveren, her bir kullanıcının bir kampanyaya maruz kalma sıklığını nasıl tekilleştirebilir ve ilişkilendirebilir?

Modelleme kesinlikle bunun bir parçası olacak, ancak şu anda kullanılanlar yukarıda açıklanan ortamı sürdürecek kadar esnek değildir. Reklamverenlerin, kampanyalarının kullanıcıları nasıl etkilediğine dair anlamlı bir sonuç elde etmek için yeni modelleri veya bunların bir kombinasyonunu test etmeleri ve denemeleri gerekecektir.

E-postalara dayanan belirli tanımlayıcılar diğerlerinden daha güvenilir olmalı ve "hayalet" kullanıcılara ulaşan ve böylece ilişkilendirme ölçeği sağlayan telekomünikasyon tarafından doğrulanmış geçici etkinleştirme kimlikleri gibi diğer kimliklerle tamamlanabilir.

Veri parçalanmasının artması, ilişkilendirmeyi daha da zorlaştıracak ve sektör içinde veya yayıncılarla bir anlaşmaya varılmadığı takdirde, reklamverenler kampanyalarının etkisini anlamlandırmak için şu anda olduğundan daha fazla mücadele edeceklerdir.

Ölçümleme, açık web'in hayatta kalması için çok önemli bir noktadır. Bir kanal olarak programatik, daha ölçülebilir ve harcamaların daha hesap verebilir hale gelmesi için evrim geçirdi. Üçüncü parti çerezlerin ortadan kalkmasıyla birlikte, kişisel bilgilerin analizi üzerine kurulu ilişkilendirme ve ölçüm modelleri artık işe yaramayacaktır.

Ancak, ölçüme giden birçok yol var. İlişkilendirme ölçümünün kullanım alanı üçüncü taraf çerezler olmadan gerçekleştirilebilir; çeşitli araçlar ve teknikler artık mevcuttur veya geliştirilmektedir. Örneğin, adtech ve yayıncılardan oluşan konsorsiyumlar, karma e-postalara dayalı yeni tanımlayıcılar oluşturmaktadır ve Chrome, pazarlamacıların tanımlayıcı bilgiler tarayıcıdan hiç çıkmadan kullanıcılarla etkileşime girmesinin bir yolunu yeniden tanımlayan "Gizlilik Sandbox girişimi "ni önermiştir.

BÖLÜM 5- MEVCUT ALTERNATİF ÇÖZÜMLERE GENEL BAKIŞ

Reklamverenler, hedef kitlesiyle bağlantı kurmak için her zaman bir araca ihtiyaç duyacaklardır. İlgili ortamlarda hem mevcut hem de potansiyel müşterilere ulaşmaları ve etkili içerikle onların ilgilerini çekmeleri gerekecektir. Dijital reklamcılık sektörü bu temel gerçeğe dayanmaktadır ve dijital pazarlama bütçesinin çoğunluğunu oluşturduğundan, değişmesi pek olası değildir. Üçüncü parti çerezler, 25 yılı aşkın bir süredir dijital reklamcılığın büyümesini desteklemede önemli bir rol oynamıştır. Ancak, üçüncü parti çerezlere olan güvenin hızlı bir şekilde sona ermesi ve değiştirilmesiyle birlikte bu durum değişecektir. Şu anda, üçüncü parti çerezler için baskın alternatif birinci parti kimlik tabanlı çözümlerdir. Bununla birlikte, birinci parti kimliklerine ek olarak, üçüncü parti çerezlerin dijital reklamcılıkta siteler arası takip, yeniden hedefleme ve reklam sunumu için baskın araç olmaktan çıktığı bir dijital ortamın geliştirilmesinde temel araçlar olarak hizmet eden çok çeşitli farklı eşzamanlı teknolojiler bulunmaktadır.

Aşağıdaki bölüm, dijital reklamcılıkta üçüncü parti çerezlerin kullanımına ilişkin bazı alternatif yaklaşımları özetlemektedir:

- Kimlik (ID) çözümleri (Identity Solutions)
- Hedefleme konusunda karar vermek için diğer reklam verilerinin kullanılması
- Bağlamsal Zekâ (Contextual Intelligence)

Kimliğin rolünü ve bugün kullanılan farklı tanımlayıcıları özetleyerek başlayalım.

5.1 Kimlik (ID)

Açık web'de tanımlayıcılarla ilgili zorluklar sektör için çok fazladır ve markaların kitlelere anlamlı bir şekilde ulaşma ve yayıncıların içerik üretimini finanse etme becerilerini etkilemektedir.

Markalar için tanımlayıcılar, kampanyaların hem verimliliğini hem de etkinliğini etkileyerek daha iyi frekans kontrolü, daha fazla erişim ve daha ilgili mesajlar sağlar. Bu sadece pazarlama etkinliğini artırmakla kalmaz; mevcut ve potansiyel müşterilerle daha iyi bir ilişki de yaratır: daha ilgili mesajlar ve rahatsız edici aşırı reklam gönderimi olmaz.

Yayıncılar, reklam envanterlerinin değerini en üst düzeye çıkarmak için tanımlayıcılara ihtiyaç duymaktadır. Yayıncıların çalışanlarına, kreatiflerine, fotoğrafçılarına, yazılım mühendislerine ve içerik ve dijital hizmetlerin üretimi ve sunumunda yer alan diğer kişilere düzgün bir şekilde fon sağlayamadığı bir ekosistemden insanlar ve toplumun geneli zarar görecektir. Frekans sınırlaması ve ilgili reklamları sağlama becerisindeki herhangi bir kayıp da web üzerindeki genel kullanıcı deneyimini azaltır ve daha fazla parçalanmayı ve ödeme duvarları gibi erişim engellerini teşvik eder.

Neyse ki, üçüncü parti çerezler uzun zamandır bu faydaları kolaylaştırmak için en çok kullanılan araç olsa da gizlilik ve ilgi düzeyi arasında bir denge kuran yeni teknolojiler hızla ortaya çıkmakta ve reklamverenlere web kullanıcılarının gizliliğinden veya etkileşimlerini kontrol etme becerilerinden ödün vermeden ilgili kitlelere ulaşma fırsatı sunmaktadır.

Reklam Tanımlayıcıları nelerdir?

Çeşitli formatlarda olabilen reklam tanımlayıcıları, frekans limiti veya kişiselleştirilmiş ve optimize edilmiş reklamcılık için bir kullanıcıyı adreslemenin ön koşuludur. Reklam tanımlayıcıları, tanımlayıcının türüne bağlı olarak cihaz veya kullanıcı düzeyinde olabilir. Tanımlayıcılar aşağıdaki özelliklere sahip olabilir:

- **Persistent, Yarı Persistent veya Transient:** (Kalıcı, Yarı Kalıcı veya Geçici)
  - Kalıcı tanımlayıcılar, etkin bir şekilde etkileşim kurmak, frekans sınırlaması yapmak ve etkileşimi ölçmek, dönüşümleri nitelendirmek ve medya harcamalarını optimize etmek için yeterli süre boyunca tarama oturumlarında bulunur.
  - Yarı kalıcı tanımlayıcılar genellikle tutarlı müşteri tanıma için kalıcı bir tanımlayıcıya bağlanabilen veya bağlanamayan birinci parti çerezlerdir:
  - Kapalı bir ekosistemde aktivasyon amacıyla kullanılan geçici tanımlayıcılar, yukarıdaki kullanım durumlarına karşı teslimat için yarı kalıcı tanımlayıcılara bağlanabilir, örneğin telekomünikasyon şirketi tarafından doğrulanmış geçici kimlikler.
- **People-Based vs Technographic Identifier (**Kişi Bazlı veya Teknografik Tanımlayıcılar)
  - **Teknografik Tanımlayıcılar** tarayıcı uygulamaları (çerezler), akıllı telefonlar (Mobil Reklam Kimlikleri), CTV'ler veya diğer web özellikli cihaz tanımlayıcılarını içerir.
  - **Kişi bazlı tanımlayıcılar**, masaüstü, mobil ve CTV dahil olmak üzere birden fazla web özellikli cihazı aynı kişiyle ilişkilendirir.
- **Deterministic vs Probabilistic / Inferred (**Deterministik veya Olasılıksal)
  - Belirleyici bilgiler, e-postalar veya oturum açma gibi bilgileri sağlayan kişi tarafından açıkça beyan edilir.

    - Olasılıklı / çıkarılan bilgiler, bir cihazı bir tanımlayıcı ile ilişkilendirmek için birden fazla veri noktası istatistiksel yöntem kullanır. IP adresi, işletim sistemi, coğrafi konum vb. gibi yaygın olarak bilinen kriterleri kullanırlar.
- **Directly-Identifiable vs Pseudonymous** (Doğrudan Tanımlanabilir veya Sahte Anonim)
    - Doğrudan tanımlanabilir bilgiler, farklı, gerçek bir kişiyi (ev adresi, telefon numarası veya e-posta gibi) kesin olarak belirlemek için kullanılabilir.
    - Takma adlı bilgi, bu tanımlayıcıyı bir bireyin kimliğinden ayrı tutmak için tanımlayıcıyı kullanan kuruluş içinde uygun teknik ve operasyonel süreçler olduğu anlamına gelir.
- **Dinamik:** her işlem için dinamik olarak oluşturulan ve PII içermeyen tek kullanımlık benzersiz bir tanımlayıcılardır.

Dijital reklamcılıkta kullanıcı adreslenebilirliğinin tek bir kişiyi isim, adres veya telefon numarası ile tanımlamayı amaçlamadığını, bunun yerine medya satın alırken veya reklam yayınlarken etkileşim kurmak ve optimize etmek için bir takma ad oluşturmayı amaçladığını belirtmek önemlidir.

Tanımlayıcılar üç başlık altında gruplanabilir:

- **Pseudonymous Universally Unique Identifier (UUID)**
    - 3. parti çerezler
    - Mobil Ad ID (MAID)
        - IDFA – iOS
        - AAID/GAID – Android
- **Pseudonymous, people-based deterministic identifier**
    - Kullanıcı kimlik doğrulamasına dayalı (şifrelenmiş e-posta), yayıncı 1. Parti kimlikleri/saklama veya telco doğrulama
    - Common IDs, Stable IDs, Universal IDs'lerin yanı sıra genellikle birinci parti kimlikleri olarak adlandırılır.
- **Pseudonymous probabilistic / inferred identifier**
    - İstatistiksel modelleme yöntemlerine dayanır
    - Düzgün çalışmak/eğitmek için yeterli veri ölçeği gerektirir - kullanıcı/kişi başına daha fazla veri temas noktası potansiyel doğruluğu ve alaka düzeyini artırır

The Pseudonymous (UUID)

Bu tanımlayıcı sınıfı en kolay birinci parti çerezi ile gösterilebilir. Tanımlayıcı, bir kimlik doğrulama olayına veya PII'ye bağlı olmadığında takma addır. Bu tanımlayıcıların çoğu, yayıncı veya yayıncı sistemleri tarafından sayfaya yazılan benzersiz tanımlayıcılar olarak site başına mevcuttur ve genellikle HTML5 kapsamında bir yayıncı birinci parti çerezi ve/veya tarayıcı yerel depolama alanında saklanır.

Yayıncılar devre dışı bırakma, kalıcılık süresi ve diğer tüm kontrol mekanizmalarını etkinleştirir. Bir kullanıcı tarayıcı önbelleğini veya çerezlerini temizlerse bu kimlikler de kaldırılır.

Pseudonymous Deterministic Authenticated Identifier

Bu tür bir tanımlayıcı, kimliğin oluşturulmasının temeli olarak bir kimlik ispatlama olayını (genellikle bir web sitesindeki bir forma girilen bir e-posta adresi) veya bir doğrulama olayını (genellikle bir telekomünikasyon ağı doğrulama talebiyle bağlantılı) kullanır, dolayısıyla "ispatlanmıştır" veya "'doğrulanmıştır"". Bu tür bir tanımlayıcı için cihaz ilişkilendirmeleri, genellikle "şifreleme(hashing)" ve "salting" gibi ikili bir işlemle anonim hale getirilmiş kişisel olarak tanımlanabilir bilgilere (PII) dayanmaktadır.

Hashing, bir e-postayı veya MSISDN'i (Mobil İstasyon Entegre Hizmetler Dijital Ağı - yani bir cep telefonu numarası) tersine çevrilemeyen rastgele bir karakter dizisine dönüştürmek anlamına gelir. Salting, bu dizeye ek karakterler eklemektir. Daha sonra bu kimlikler için platform düzeyinde kodlama da dahil olmak üzere ek şifrelemeler ve kodlamalar da uygulanabilir. Bu kimlikler birden fazla site ve cihazda kullanıcı kimlik ispatlamasına veya doğrulamaya dayandığından, bağlantı deterministiktir ve ortaya çıkan tanımlayıcı doğrudan girdi değeriyle ilişkili olmadığından, bunlar da takma ad olarak kabul edilir. Çok daha önemlisi, bu cihazlar kullanıcı düzeyindedir ve tipik olarak masaüstü ve mobil cihazlara ve giderek artan bir şekilde CTV'ye çok kanallı erişim genişletmesi ve frekans sınırlaması sunar.

Üçüncü parti çerezlerin kullanımdan kaldırılmasıyla birlikte, ister e-posta ister telefon numarasına dayalı olsun, bu tür tanımlayıcılar çoklu cihaz, web ve uygulama ortamlarında üçüncü parti çerezlerinin ve MAID'lerin kaybını çözmeye potansiyel olarak yardımcı olabilir. Mevcut kimlik çözümlerinin kapsamlı bir listesi için 47. sayfadaki listeye bakabilirsiniz.

Pseudonymous Probabilistic Identifier

Fraud tespiti gibi bazı kullanım durumları, algoritmalar aracılığıyla oluşturulan sahte tanımlayıcılara dayanır. Bu algoritmalar, web siteleri arasında bir kullanıcının benzersizliğini çıkarmak için HTTP Protokolü aracılığıyla paylaşılan IP adresleri ve cihazın kullanıcı aracısı dizesi gibi pasif tanımlama sinyallerini kullanır. Bu süreç, markaların açık web üzerindeki envanter ve kitlelere erişmesini ve dolandırıcılık nedeniyle boşa harcanan bütçe miktarını ölçüp azaltmasını sağlar.

Bu genellikle istatistiksel bir tanımlayıcı oluşturmak olarak adlandırılır. Bu tanımlama yöntemi için GDPR kapsamında yasal bir dayanak ve algoritmalar kullanıcının cihazından aktif olarak alınan verileri (mevcut yazı tipleri ve ekran boyutu gibi) kullandığında ePrivacy direktifi kapsamında kullanıcı onayı gereklidir. Ayrıca bu yöntem, tüm büyük tarayıcılar dahil olmak üzere birçok kişi tarafından parmak izi olarak kabul edilmekte ve reklam amacıyla kullanılması açıkça yasaklanmaktadır.

5.2 Kimlik Çözümleri

5.2.1 CRM Verisi

Birçok reklamveren ve ajans, en iyi bildiklerine -CRM dünyasına- ve "bilinen" tüketiciye geri dönmüştür. Zorlukları olsa da CRM ve e-posta bu yeni gizlilik bilincine sahip ortamda yeniden doğuş yaşamış, programatik ve dijital ortamda giderek daha önemli bir duruma gelmiştir.

Sahipli platformlar yıllarca, bir markanın CRM dosyasını kalıcı cihazlar arası tanımlayıcılarıyla doğru bir şekilde eşleştirme becerilerine dayanarak, açık web'de bulunmayan şekilde kuruma özel, kişiselleştirilmiş reklam kampanyaları için fırsatlar yaratmıştır.

Bildiğimiz gibi, bu onlara eşsiz bir avantaj ve sahipli platformların dijital reklamcılık pazarındaki aslan payını kapmalarını sağlamıştır ancak tüketicilerin zamanının çoğu (yüzde 56'dan fazlası) bu platformların dışındaki dijital medyada geçmektedir.

Bölüm 2'de ayrıntılı olarak açıklandığı gibi, tarayıcılar üçüncü parti çerezleri engelliyor ve açık web, birinci parti ve kişi tabanlı tanımlayıcılarla premium envanterin bir araya getirildiği bir ortama geçmeye başlamıştır Bu tanımlayıcılar, markaların medyayı CRM dosyaları doğrultusunda etkinleştirmesine ve daha önce sahipli platformlara özel olan pazarlama tekniklerini taklit etmesine imkan sağlayabilir.

Bu durum, markaların erişimini premium ortamlar ve omnichannel reklam formatları genelinde genişletebilecek büyük bir paradigma değişiminden başka bir şey değildir.

Neden CRM ve e-Postalarla Çalışmalı?

Birçok reklamveren, yıllar içinde CRM veritabanlarını oluşturmuş ve geliştirmiş ve bunu kampanyaları pazarlama otomasyonu yoluyla sürdürme, upsell ve geliştirme amacıyla desteklemek için kullanmıştır. Bununla birlikte, dijital, sosyal ve aramaya ilişkin faaliyetlerini desteklemek için bu tür veri kümelerini kullanmak, arama ve sosyal medya söz konusu olduğunda nispeten yakın zamana kadar medya planının temel dayanağı haline gelmemiştir ve dijital ekranda ender görülmemektedir (Amerika Birleşik Devletleri dışında). CRM'nin son birkaç yılda popüleritesindeki artış kesinlikle anlaşılabilir, bu arada gelişen dijital reklamcılıkta tüketici verilerinin ve kimliğinin kaynağı olarak önemi neredeyse kaçınılmazdır ve faydaları şu şekilde sıralanabilir:

1. e-Posta adresi nispeten kalıcıdır. Çerezin yarı ömrünün 7-30 gün arası olabileceği durumlarda, çoğu kişi aynı e-posta adresini birkaç yıl veya en az birkaç ay kullanır. Bu da verilerin zaman içinde kayıpsız olarak depolanabileceği ve biriktirilebileceği anlamına gelir.

2. Bir tanımlayıcı olarak e-posta adresi, etki alanına ve dolayısıyla platforma özel olan üçüncü

parti çerezden farklı olarak, platformdan bağımsızdır. Bu durum, onu kimlik senkronizasyonu ve eşleştirme tablolarına bağlı kalmadan, tüketici yolculuğuyla bağlantı kurmada, medya etkinliğini ilişkilendirmede ve hedef segmentasyonunu aktivasyon platformlarına tarafsız olarak dağıtmada önemli bir bileşen haline getirir.

3. GDPR'nin yürürlüğe girmesinden bu yana, reklamverenler, ajanslar ve reklam teknolojisi tedarik zincirindeki diğer kurumlar çoğunlukla, rıza alınmış veri setlerini temizlemektedirler.

Web sitesi formu gönderimleri ve benzer doğrulanmış kullanıcı eylemi yoluyla elde edilen, genellikle içeriğin olumlu onaylanmasıyla ilgili olarak daha yüksek bir beklentinin karşılanmasını gerektiren CRM, rıza verilen, kullanımı onaylanan pazarlama verileri için altın standart haline gelmiştir.

Operasyonel olarak, CRM verileriyle çalışmanın da zorlukları vardır. Birçok kurumsal CRM, Müşteri Veri Platformu ve pazarlama otomasyonu platformu, Facebook, Instagram ve Google Ads gibi belirli platformlarda e-posta adreslerinin doğrudan entegrasyonunu ve etkinleştirilmesini uzun süredir desteklese de, e-postanın dijital ve programatik ekranda kullanılması, e-posta adreslerini dijital tanımlayıcılara, tarihsel olarak üçüncü parti çerezlerine ve/veya mobil reklam kimliklerine (AID ve IDFA) eşleyebilen ve aktarabilen "onboarding" çözümlere aracılık etmiştir ve bunu yapmaya devam etmektedir.

Onboarding çözümler, telekomünikasyon şirketleri, dijital yayıncılar, e-ticaret platformları ve e-posta hizmet sağlayıcıları da içeren ortaklarla sürdürdükleri ilişkiler aracılığıyla e-posta adreslerini dijital tanımlayıcılara bağlayarak kendi kimlik grafiklerini geliştirir. Satın alıcılar, bir kimlik grafiği sağlayıcısını kullanarak, bir kimlik çerçevesi aracılığıyla programatik ekosistem genelinde etkinleştirilen online kişi tabanlı tanımlayıcılarla online hedef kitlelerini eşleştirebilir. Daha sonra tekil bir "deal ID" kullanarak bu kitleler üzerinde işlem yapabilirler. Bu kitlenin içindeki tüketiciler premium ve uygun bir yayıncıyı ziyaret ettiğinde ve daha da önemlisi, verilerini paylaşmaya rıza gösterdiğinde, satın alıcılar bu kullanıcılar için gerçek zamanlı olarak (kendi seçtikleri DSP aracılığıyla) teklif verebilir.

Sonuç olarak markalar, kullanıcılara daha alakalı reklamlar sunarak katılımı, yayıncılar da gelir akışlarını artırabilirler ve tüketicilere, gerçekten almak istedikleri reklamlara erişim imkânı sunulur (bu tür reklamları almak için "opt-in" yaptıkları takdirde).

Toplu olarak, bu çabalar, bağımsız ve premium satın alıcıların ve satıcıların sahipli platformlarla geniş ölçekte rekabet etmesini sağlayarak sektörün oyun alanını eşitleyebilir.

Data Clean Room

Üçüncü parti çerezinin kullanımdan kaldırılması ve daha güvenli bir ortama geçişle birlikte, Facebook ve Google gibi platformlardan bilgi toplanan ve ölçüm, ilişkilendirme ve hedefleme için reklamcılardan alınan birinci parti verileriyle bir araya getirilen, temelde güvenli alanlar olan Data Clean Room'ların yükselişine şahit olunmuştur.

Kimlik düzeyinde hiçbir veri paylaşılmaz ve gizlilik endişelerini azaltmak için analiz genellikle bir yığın düzeyinde yapılır.

Reklamveren verileri çeşitli kimlikler kullanılarak paylaşılabilse de odak noktası CRM ve e-postadır ve ilk işlerin çoğu bu tanımlayıcı sınıfı etrafında yoğunlaşmıştır.

Data Clean Room'lar Facebook ve Google'dan bağımsız olarak çalışabilir. Bazı onboarding sağlayıcıları bunları tekliflerinin bir uzantısı olarak sunar ve yalnızca birinci parti verileri üzerinde istatistiksel modelleme ve/veya zenginleştirilmiş birinci parti verileri (birinci parti verileri + ID sağlayıcı üçüncü parti grafiği) üzerinde istatistiksel modelleme çalıştırmak için kullanılabilir.

Sınırlamalar

CRM ve e-posta ile çalışmada bazı aksaklıklar bulunmaktadır ve bu mükemmel bir ekosistem değildir.

- **Veri Temizliği:** Tipik olarak e-posta adreslerinin ve CRM verilerinin, veri setinin boyutuna ve karmaşıklığına bağlı olarak ek veri bilimleri/mühendisliği kaynakları gerektirebilecek onboarding çözümüne dağıtılmadan önce temizlenmesi, normalleştirilmesi, hashing edilmesi ve bazen önceden segmentlere ayrılması gerekecektir.
- **Eşleşme Oranları:** Hashing uygulanmış CRM, yeni katılımcıya gönderildiğinde, medya platformu uç noktasına aktarılmadan önce ön tanımlı bir kimlikle eşleşecektir. ABD'de eşleşme oranları %80-90'a kadar ulaşabilmektedir. Bununla birlikte, Avrupa'da ortalama eşleşme oranları %40-60 arasında değişmektedir ancak verilerin türüne, yaşına ve bütünlüğüne bağlı olarak bu oran daha düşük olabilir.
- **Teknoloji Ücretleri:** Avrupa'daki çoğu onboarding çözümü, hizmetlerini yalnızca sabit, yinelenen maliyetler ve minimum sözleşme süreleriyle SaaS tabanlı bir lisans ücreti altında sunarak, onboarding çözümüne yatırımı nispeten büyük ölçekli bir satın alma kararı haline getirmektedir.

- **İlişkilendirme/Attribution Ölçümü:** Birçok pazarlamacı, web sitesi içeriklerine erişmek için e-posta talep etmez. Buna göre, görüntüleme ve çoklu dokunma ilişkilendirmesini etkili bir şekilde ölçmek için oturum açmış takma adlı yayıncılar arası tanımlayıcılar da gereklidir.

Genel olarak, tüketiciler için şeffaflık kilit önem taşıyacaktır. Denklemin hem reklamveren hem de yayıncı tarafındaki kullanıcılar, e-postalarının siteler arası "adreslenebilirlik" için kullanıldığı konusunda her zaman bilgilendirilmelidir.

5.2.2 Birinci Parti Telko Operatör Verileri

Telekom operatörleri, sundukları hizmetler nedeniyle, cep telefonunun ortaya çıkışından bu yana müşterileriyle güvenilir, faturalandırmaya dayalı bir ilişkiye sahip olmuştur. Mobil cihazlar söz konusu olduğunda, bu bire bir ilişkidir.

Mart 2014'ten bu yana operatörler, GSMA'nın Mobile Connect güvenli evrensel hizmeti aracılığıyla üçüncü taraf işletmelerin kullanıcıları tanımlaması ve kimliklerini doğrulaması için güvenli ve emniyetli bir yol sağlamıştır. Bankacılık, finansal hizmetler, ödemeler ve e-ticaret gibi sektörler bu hizmeti kimlik doğrulama, yetkilendirme ve güvenli kimlik doğrulamasını hızlı, küresel ve uygun maliyetli bir şekilde sağladığı için kullanmaktadır.

Son yıllarda, kimliğe yönelik bu güvenli yaklaşım programatik dijital reklamcılığı da kapsayacak şekilde genişletilmiştir.

Mobil operatörler çeşitli kimlik çözümleri sunmaktadır:

- **Tek Oturum Açma (SSO)**- birden fazla kimlik bilgisini kaydetmek ve hatırlamak yerine, birden fazla web sitesinde kullanılmak üzere tek bir kimlik bilgisi seti için bir araç.
- **Mobil Dijital İmza-** kriptografik işlemleri yürütmek için SIM içindeki güvenli ortam kullanılarak oluşturulan bir dijital kimlik. Bazı ülkeler, mobil dijital imza metodolojilerini, kanunen elle atılan imza ile aynı kabul edilecek kadar güvenli olarak kabul etmektedir.
- **Kimlik Attribute Aracılığı**- birinci parti müşteri verilerinin belirli attribute'lerinin operatör güvenlik duvarının arkasında eşleştirilmesi.
- **Yayıncı veya Marka Kitle Doğrulaması**- yeni anonimleştirilmiş web'in zorluklarını ele almak için doğru, gerçek zamanlı çapraz etki alanı ve çapraz cihaz, gizlilik uyumlu kullanıcı profili oluşturmak için onaylanmış birinci parti yayıncı çerezlerinin doğrulanması.
- **İzleyici Etkinleştirme**- reklam teknolojisi ekosistemine herhangi bir PII verisi girmeden reklam etkinliğini artırmak için yayıncıların veya markaların kendi mülklerinde ve açık web'de onaylı birinci parti kitle verilerini eşleştirmenin işlemsel ve anonim bir yöntemi.

Dijital reklamcılıkta telekomünikasyon zekasının bu uygulaması, yayıncılar ve markalar için doğrulanmış kitlelerin sürekli olarak oluşturulmasına ve reklamverenler için belirleyici kitle hedeflemesine olanak tanır.

Bir telekomünikasyon ağının gerçek zamanlı yapısı, reklam talebi başına bireysel düzeyde kitle işlemleri için bir Telko Doğrulanmış Kullanıcı Kimliği ve bir Dinamik Kimlik kullanılmasına olanak tanır. Dinamik Kimlik, teklif talebinde dağıtılır ve teklif öncesi kitle yanıtı için takas edilir. Bu, reklamcılık ekosistemi için bir çözüm paketi oluşturur:

- Telko tarafından doğrulanmış bir kullanıcı kimliği
- Kitle aktivasyonu için dinamik bir kimlik
- Reklamveren odaklı birinci parti veri aktivasyonu
- Yayıncı analizi ve profil oluşturma

Yayıncılar için, telekomünikasyon tarafından doğrulanmış bir kimliğin kullanılması, giderek artan sayıda 'hayalet' kullanıcı olarak adlandırılan, yayıncı sitelerine ve uygulamalarına giriş yapmadan ve doğrulanmadan göz atan tüketicilerin ele alınmasına yardımcı olabilir.

Bu anonim web kitlesi oldukça büyüktür, ancak bir yayıncı telekomünikasyon istihbaratını kullanarak kullanıcı tabanını anlayabilir ve kullanılan cihazdan bağımsız olarak bir kullanıcıyı sitesine veya uygulamasına geri döndüğünde tanıyabilir. Bu hem kimliği doğrulanmış hem de doğrulanmamış site ziyaretlerinde tek tip kitle kimliklerinin oluşturulmasını sağlar.

Bu profiller yayıncı bazında oluşturulur ve tek tip bir kimlik (UUID) değildir. Yayıncılar bu profilleri site analizlerini çalıştırmak ve kendi kullanıcı profillerini güçlendirmek için kullanır. Bu sayede kendi birinci parti kitle verilerini güvenli bir şekilde etkinleştirebilirler.

Dinamik Kimlik ayrıca bir yayıncının envanterini telekomünikasyon şirketi tarafından türetilmiş başka kitle özellikleriyle zenginleştirmesine olanak tanıyarak reklamların alaka düzeyini ve bu reklam gösterimlerinin değerini artırır.

Telekomünikasyon şirketi tarafından doğrulanmış kitle verilerinden yararlanmak, reklamverenlerin birinci parti veri sahibi düzeyinde toplanan ve onaylanan doğrulanmış verileri kullanarak gerçek kitlelere gerçek zamanlı ve geniş ölçekte ulaşmasına olanak tanır. Bu da verilerin ve kullanılan sürecin ilgili tüm veri gizliliği düzenlemeleriyle uyumlu olmasını sağlar.

Dinamik bir tanımlayıcı sağlamak için telko istihbaratını kullanmak, bir reklamverenin belirli kitleleri hedeflemesine, tercih ettikleri DSP ile bu kitlelere karşı harekete geçmesine ve frekans sınırlama, ölçüm ve ilişkilendirme işlemlerini gizlilikle uyumlu bir şekilde gerçekleştirmesine olanak tanır.

5.3 Kimlik (ID) Ortamına Genel Bakış

Yayıncılar, gerçek bir iş birliği ruhu içinde, envanter ve kitle segmentlerini paylaşarak sahip oldukları varlıklar üzerinde işlem yapılmasını kolaylaştırmak için ortak ve paylaşımlı

uygulamalar geliştirmek üzere birlikte çalışmaktadırlar. The Ozone Project ve Pangea Alliance EMEA da bunlardan ikisidir. Kimlik sorunlarını çözmek ve kendi pazarlarına daha fazla uyum sağlamak için birden fazla mülkte standartlar oluşturma çalışmalarına katılmaktadırlar. Bunlar genellikle Kimlik Konsorsiyumları (ID Consortiums) veya Paylaşımlı Kimlik Çözümleri (Shared ID solutions) olarak adlandırılır. Üçüncü parti çerezlerin aksine, birinci parti çerezlere dayalıdırlar, bu nedenle, üçüncü parti çerezler hedeflemesine çekici bir alternatif oluşturmaktadırlar.

Genelde, bir yayıncının sitesindeki üçüncü parti çerezlerin sayısı ortalama olarak çok fazladır ve reklamları bireylere hedeflemek için bu tekil çerezlerin tümünün eşleştirilmesi gerekir. Paylaşımlı kimlik, yayıncıların tek bir paylaşımlı kimlik (kullanıcı başına) üzerinden işlem yapmasına olanak sağlamak için birden çok web sitesindeki kullanıcı kimliğini birleştirir.

Paylaşılan kimlikler şifrelenmeli ve kullanmak için güvenli API'ler veya barındırılan uygulamalar gerektirmelidir.

Paylaşılan kimlikler üzerinde işlem yapan farklı kuruluşlar, yalnızca işleme dahil olan tüm tarafların izinli olması durumunda korunan verileri paylaşabilmeli veya örtüştürebilmelidir; bu da yayıncıların, platformların ve pazarlamacıların kişi tabanlı bir tanımlayıcı üzerinde etik ve güvenli bir şekilde programlı olarak işlem yapmasına olanak tanır.

Ayrıca, paylaşılan kimlikler tarafsız ve birlikte çalışabilir olmalı, güvenilir ve doğrulanmış, gizlilik bilincine sahip bir şekilde olmalıdır. Teknoloji uyumlu olmalı ve güvenilir, açık ve tarafsız bir ekosistemi desteklemelidir.

Konsorsiyum Örneği- IAB Tech Lab Rearc

Üçüncü parti çerezler ve diğer tanımlayıcılarda yapılması muhtemel değişiklikler göz önüne alındığında, IAB Tech Lab tamamen Project Rearc'ye odaklanmıştır. Project Rearc, dijital tedarik zincirindeki paydaşların, tüketici gizliliği ve kişiselleştirmeyi dengelerken temel sektörel kullanımları desteklemek için dijital pazarlamanın üzerinde yeniden düşünülmesi ve yeniden tasarlaması için küresel bir eylem çağrısıdır.

IAB Tech Lab, üye olan ve olmayan paydaşları eğitmek ve bu makalede ele alınan “çözüm” alanlarının birçoğu için teknik standart ve kılavuzları içeren adreslenebilir reklamcılık ve ölçümü "varsayılan olarak gizlilik" esasıyla kullanan yeni teknik standartların ve kılavuzların geliştirilmesi sürecine küresel girdiyi sağlamak üzere, iş birliğine dayalı bir süreç yönetmektedir.

Çoklu Kimlik Çözümleri ve Kimlik Konsorsiyumları ile Çalışma

Elbette, çok sayıda kimlikle ve kimlik konsorsiyumu ile nasıl çalışılacağı sorusu söz konusudur. Prebid.org inovasyonu teşvik etmek için çözümler ve açık kaynaklı ürünler sağlamak amacıyla reklam teknolojisi topluluğu ile birlikte çalışan reklam teknolojisi sektör liderlerinden oluşan bir organizasyondur. Prebid açık kaynak header bidding yazılım paketinin temel bir parçası olarak bir Kullanıcı Kimliği Modülüne sahiptir. Sitelerine Prebid kurulumu yapan yayıncılar için Kullanıcı Kimliği Modülü, bu yazılım yığınının opsiyonel bir parçasıdır. Kullanıcı Kimliği Modülü, teklif akışı içinde standartlaştırılmış veya "evrensel" kimlikler oluşturmak, depolamak ve iletmek üzere kullanılır. Modül, standartlaştırılmış kimlik tedarikçilerine açıktır, böylece yayıncıların seçmeli olarak kullanmaları için, kendi alt modüllerini sunabilirler. Prebid Kullanıcı Kimliği Modülü'nde şu anda mevcut olan evrensel kimlik alt modülleri şunlardır:

- BritePool (BPID)
- Criteo ID for Exchanges
- Fabrick ID
- Halo ID
- ID5 Universal ID
- IDx
- IntentIQ ID
- LiveIntent ID (NonID)
- LiveRamp RampID (önceden IdentityLink olarak bilinen)
- Lotame Panorama ID
- Merkle ID
- netID
- Novatiq Hyper ID (önceden Snowflake ID)
- Parrable ID
- PubCommon ID (SharedID)
- Pub Provided ID
- Quantcast ID
- Tapad ID
- Unified ID (The Trade Desk)
- Verizon Media ConnectID
- Zeotap ID+ solution

En güncel Ön Teklif listesine buradan erişebilirsiniz.

Tutarlı Yayıncılar Arası Tanımlayıcı Üretimi

Yayıncıların Prebid kurulumlarında etkinleştirdikleri yukarıdaki kimliklerden herhangi biri için Kullanıcı Kimliği Modülü, yayıncının takdirine bağlı olarak ilgili kimlikleri üretecek ve ardından bu değerleri birinci parti çerezinde saklayacaktır. Prebid daha sonra bu kimlikleri teklif akışı içinde kullanılabilir hale getirebilir.

Tutarlı Yayıncılar Arası Tanımlayıcı Aktarımı (veya Yeniden Oluşturma)

Aynı tanımlayıcının aynı tarayıcıyla ilişkilendirilmesini sağlamak, gizlilik tercihlerini hatırlamanın yanı sıra pazarlamacı kullanım durumlarını ele almak için de önemlidir. Bu nedenle, takma ad tanımlayıcısını oluşturmaya ek olarak, bu çözümlerin ortak tanımlayıcıyı çeşitli yayıncılar arasında taşıması (veya yeniden oluşturması) gerekir. Ortak yayıncılar arası tanımlayıcıyı yeniden oluşturmaya yönelik bir yaklaşım, yukarıda açıklandığı gibi kullanıcı e-postalarına dayanmaktadır.

Depolama

Yukarıda listelenen evrensel kimliklerin çoğu veya tamamı normalde sayfaya üçüncü parti çerezler olarak yazılsa da, Prebid'in sayfaya etki alanı düzeyinde erişime sahip olması, yayıncının etki alanı içinde birinci parti çerezi ayarlayabileceği anlamına gelir. Bu birinci parti depolama (veya "zarf") yöntemi tamamen yayıncının kontrolündedir ve daha sonra bu standartlaştırılmış kimliklerin teklif akışı içinde üçüncü parti çerezlerine güvenmeden katılımcı DSP'lere iletilmesini sağlar.

Bireysel şirketler de bu çözümü geliştirmektedir. Çoklu kimlik desteği Prebid ve OpenRTB'de yerleşik olarak bulunmaktadır. Yayıncılar bu standartlar aracılığıyla yukarıda belirtilen kimlik modüllerinden istedikleri kadarını yerel olarak destekleyebilir.

Birden Fazla Kimlikle Çalışmanın Kullanım Alanları

Markaların ve yayıncıların birden fazla kimlikle çalışmayı tercih edebileceği çeşitli kullanım alanları vardır. Öne çıkan iki tanesi şunlardır:

a) Küresel operasyonlar: Tedarik genelinde evrensel kimlik ölçeği küresel bölgelere göre değişebilir, bazı kimlikler bazı ülkelerde diğerlerine kıyasla daha güçlü bir ayak izine sahip olabilir. Küresel markalar ve yayıncılar, tercih edilen kimlikleri ülke bazında seçmeyi düşünebilirler.

b) Kimliği doğrulanmış ve doğrulanmamış trafik: Site ziyaretçilerinin büyük bir kısmının kimliğinin doğrulanmayacağını varsayabiliriz. Dolayısıyla, en büyük ölçekli kimliği doğrulanmış kimlik bile, hedeflemede e-posta adreslerinin kullanılmasına katkıda bulunan ve izin veren kullanıcılara ulaşamayacaktır.

Çıkarımsal kimlikler ve Telko tarafından doğrulanmış kimlikler, kimlik doğrulaması yapılmamış kullanıcılara rıza ile ulaşabilir. Yayıncıların ve markaların hem kimliği doğrulanmış hem de doğrulanmamış kitleler için kimlik çözümlerini göz önünde bulundurmaları gerekecektir.

5.4 Kimlik Sağlayıcıları Nasıl Değerlendirilmeli

Yeni kimliklerin akınına ve bir tanımlayıcının cihazları ve siteleri kullanıcılarla nasıl ilişkilendirdiğini bildiren yayıncı tarafı teknolojisi olan Tanımlayıcı ile Kimlik Altyapısı arasındaki çizgilerin bulanıklaşmasına tanık olduk.

Markalar için, kitle segmentlerini hangi evrensel kimlik üzerinden oluşturacaklarını seçmek kritik bir karardır. Yayıncılar için ise kimlik entegrasyonu, geliştirme maliyeti ve sayfa performansı üzerindeki potansiyel etkisiyle birlikte gelir.

Markalar, ID'leri değerlendirmek için aşağıdaki metodolojiyi kullanabilir. Bu metodoloji yayıncılar için de önemlidir, çünkü markaların karar verme süreçlerinin arkasındaki etkenleri anlamaları gerekir.

a) **Küresel bölgelerde kullanılabilirlik:** İlk adım, markaların ve yayıncıların müşterilerine ulaşmak istedikleri ülkelerdeki ID önemini anlamaktır.
b) **Veri hedefleme türüne göre yetenekler:**
    i. Çevrim dışı birinci parti verileri: Bir ID, müşteri veritabanından ne tür bilgileri alabilir ve etkinleştirebilir? Tüm doğrulanmış kimlikler e-postalara dayanır. Telko tarafından doğrulanmış kimlikler, birinci parti çereze geri bağlantı sağlayan gizlenmiş bir telefon numarasıyla ilişkilendirilir. Buna ek olarak, işletmelerin bir kimliğin telefon numarası, fiziksel adres, ad ve soyad gibi diğer bilgilerle de ilişkilendirilip ilişkilendirilemeyeceğini belirlemesi gerekebilir.
    ii. Site ziyaretçileri: Yeniden hedeflemeyi etkinleştirmek için, bir kimliğin markaların üçüncü parti çerezleri kullanmadan sahip olunan mülklerde bir tanımlayıcı oluşturmasına izin vermesi gerekir. Bu da markaların tıpkı yayıncıların yaptığı gibi kimlik altyapısını entegre etmesini gerektirir. Yeniden hedefleme yapan ancak kimliği doğrulanmış kullanıcılara sahip olmayan markalar, e-postaya dayanmayan çıkarılmış kimlikleri veya Telko onaylı kimlikleri düşünmelidir.
    iii. Üçüncü parti veriler: Yeni müşterileri hedefleyen markaların, evrensel kimliklerin tercih ettikleri üçüncü parti veri sağlayıcılarının kitle segmentlerinde kullanılabileceğinden emin olmaları gerekir.

Markaların, yayıncıların ve platformların evrensel kimliklerin yeteneklerini daha iyi anlayabilmeleri için kimlik sağlayıcılarına aşağıdaki soruları sormaları önerilmektedir.

ÖLÇEK
Ülkeye göre kullanılabilirlik ve ölçek
Bölgeye / ülkeye göre mevcut SSP entegrasyonları
Bölgeye / ülkeye göre gelecekteki SSP entegrasyonlarının zaman çizelgesi
DSP entegrasyonları
Birinci parti adreslenebilirlik çözümü ile entegre yayıncıların listesi
Safari / Firefox / Edge'de görülen aylık aktif adreslenebilir kullanıcılar
Satıcının teknik tasarımı, tarayıcı satıcılarının siteler arası izleme, parmak izi veya ağ düzeyinde izlemeyi (örneğin VPN hizmeti veya İSS satıcısı tarafından izleme) azaltmayı amaçlayan önerileriyle çelişiyor mu?
Anonim 'hayalet' web kullanıcıları tanımlanabilir ve etkinleştirilebilir mi?

GİZLİLİK
PII: Kimliğinizin oluşturulması kullanıcıların PII (e-posta, telefon numarası, adres vb.) sağlamasına bağlı mı?
Tüketici tercihi: Şirketiniz tüketici tercihlerini (opt-in/opt-out) kimliğinize bağlıyor mu, yoksa bu tercihlerin kaydı eski tanımlayıcılara mı (üçüncü parti çerezleri gibi) bağlı?
Tüketici tercihi: Lütfen kimlik çözümünüzün entegre olduğu veya uyumlu olduğu onay çerçevelerini listeleyin
Gizlilik koruması nasıl sağlanıyor? Kanıtlanmış uygulamaları olan patentli çözümler var mı?
Çözümünüz https://webkit.org/tracking-prevention-policy/ ile nasıl örtüşüyor?
Çözümünüz https://w3cping.github.io/privacy-threat-model/ ile nasıl örtüşüyor?

KAPASİTELER
Teknik: Çözümün teknik olarak nasıl çalıştığını açıklayabilir veya bir akış diyagramı sunabilir misiniz?
Kimlik kullanıcı düzeyinde mi? Dinamik ve gerçek zamanlı mı?
Üçüncü parti çerez çözümü: Kimlik, çerez kısıtlaması olan tarayıcılarda adreslenebilirlik sağlıyor mu?
Üçüncü parti çerez çözümü: Kimlik, çerez kısıtlamalı tarayıcılarda adreslenebilirliği nasıl sağlar? Tanımlayıcıyı yaymak için adım adım iş akışı nedir? (teknik açıklama veya belgelere bağlantılar sağlayın)
IDFA opt-in: Kullanıcı IDFA'yı tercih etmediğinde kimlik iOS uygulamalarında adreslenebilirlik sağlayacak mı?
IDFA opt-in: Evet ise, kimlik iOS uygulamalarında nasıl adreslenebilirlik sağlayabilir? Tanımlayıcıyı yaymak için adım adım iş akışı nedir? (teknik açıklama veya belgelere bağlantılar sağlayın)
CTV: Kimlik CTV kaynağında mevcut mu?
CTV: Evet ise, hangi SSP'ler ile?

CTV: Evet ise, kimlik CTV cihazlarını kullanıcılarla nasıl ilişkilendirebiliyor? Tanımlayıcıyı yaymak için adım adım iş akışı nedir? (teknik açıklama veya belgelere bağlantılar sağlayın)
Doğruluk: Hedefleme ne kadar doğru? Deterministik mi yoksa olasılıksal mı?
Birlikte çalışabilirlik: Kimlik çözümü tek başına mı yoksa diğer kimliği doğrulanmış kimliklerle birlikte mi çalışıyor? Çözüm ne kadar esnek?
Geleceğe Hazır: Programatik ekosistemde veya düzenleyici ortamda daha fazla değişiklik olması durumunda çözüm ne kadar sağlam?
Çapraz platform: Kimlik hem mobil hem de masaüstünde hem web hem de uygulama özelliklerinde çalışıyor mu?

FAYDALAR
Kimliğin değer önerisi beyanı nedir? (Satış broşürlerine, tek sayfalara ve diğer pazarlama teminatlarına bağlantılar sağlayın)
Kimliğin başlıca faydaları nelerdir?
Kimliğin pazardaki diğerlerine kıyasla farklılaştırıcı unsurları nelerdir?
Kimliğin uygulanması kolay mı?
Tüketici Deneyimi: Tüketici için verilerinin nasıl kullanıldığını anlamak ve yönetmek ne kadar kolay?

5.5 Hedefleme Kararları Vermek İçin Kullanılabilen Diğer Veriler, ör. Etkileşim (engagement), Maruz kalma (exposure)

Bir reklam sunumunun etkisinden tüketici katılımının temel boyutlarına kadar tahmine dayalı veriler sağlayan veri çözümlerinin kullanımı, kampanya performansını artırmak için önemli bir alternatiftir.

Veri noktalarının gerçek zamanlı olarak bir tüketicinin etkileşimiyle birlikte analiz edilmesi, ekrandaki payı, video sunumu, sesli vb. metrikler aracılığıyla etkileşim hedeflemesine imkân tanır.

Gerçek zamanlı olarak, bu veri öğesi, hızlı ancak basit veya karmaşık ancak yavaş olarak kabul edilebilecek mevcut araçlara kıyasla avantajlıdır. Dijital reklamla ilişkilendirilen tahmine dayalı veriler, markaların iş hedefleriyle uyumlu olarak dijital yatırımlarında netlik ve güvene sahip olmalarını sağlayacaktır.

Dijital reklam harcaması arttıkça, bu tedbirlerle gösterim kaynağında bir reklamın düşük performans gösteren alanlarını saptamak ve bir kampanyanın performans eğilimini tahmin etmeyi mümkün kılmak, reklamverenlerin yatırım getirisini maksimize etmesine ve gerçek ticari sonuçlar elde etmesine yardımcı olabilir.

DSP'ler, kazanılan ve bir dönüşümle ilişkilendirilen gösterimlere ilişkin bağlamsal ayrıntılar, tipik olarak sayfa düzeyinde bilgiler (alan adı, ülke kodu vb.), teklif düzeyinde bilgiler (teklif fiyatı, reklam öğesi boyutu, satıcı adı vb.) ve tarayıcı düzeyinde bilgiler (cihaz türü, aile tarayıcısı, aile işletim sistemi vb.) sağlar.

Bu bilgiler daha sonra bir DSP kullanıcı kimliğiyle ilişkilendirilir ve bu kimlik normalde GDPR bölgelerinde DSP tarafından karma hale getirilir veya sıfırlanır.

Her DSP tarafından sağlanan kampanya günlüklerinin tam içeriğine teknik belgelerinden erişilebilir ve talep üzerine sağlanabilir.

Reklam teknolojisi ekonomisi çeşitlidir ve teknoloji bolluğu vardır. Örneğin, yapay zekâ alanındaki gelişmeler burada ve yöntemleri, reklamverenler için performans ve ölçek oluşturmak amacıyla kullanıcı gizliliğini ihlal etme ihtiyacının ötesine geçmektedir. Bunun yerine yapay zekâ, markalar ve tüketiciler arasında daha iyi bir uyum yaratmak için web sitelerindeki teklif taleplerinden elde edilen bol miktarda, zararsız, kullanıcıya özgü olmayan meta verileri kullanır. Bu teknoloji sadece çerez ve kişisel tanımlayıcıların sınırlamalarını ortadan kaldırmaya değil, aynı zamanda pazarlamada gizlilik ve performans arasındaki talihsiz ilişkiyi çözmeye de hazırlanmaktadır.

Makine öğrenimi ve yapay zekâ, bu yeni veri kaynaklarından en iyi şekilde yararlanmanın ve üçüncü parti çerezlerin bıraktığı boşlukları doldurmanın anahtarıdır. Bu araçlar, örneğin K-anonimlik veya diferansiyel gizlilik gibi anonimleştirme prosedürleri izlenerek anonimleştirilmiş ve belirli bir kullanıcının ayrıntılarına inmeyi imkânsız hale getiren kohort verilerini işleyebilecektir. Ayrıca, web içeriğiyle kullanıcıya özgü olmayan etkileşimlerden rutin olarak elde edilebilen kolay erişilebilir, bol miktarda veri noktasının analizine dayalı olarak kullanıcı davranışlarının modellenmesine ve tahmin edilmesine yardımcı olacaklardır. Bu, reklamverenler ve tedarik zincirleri için verimlilik ve ölçek sağlamaya yardımcı olacaktır.

5.6 Bağlamsal Hedefleme (Contextual Targeting)

Bağlamsal hedefleme, prensip olarak yeni değildir. Aslında bu, pazarlamacılar için denenmiş ve test edilmiş bir yaklaşımdır.

Benzer bir yaklaşım, belirli yayınların veya editoryallerin, ürününüze/hizmetinize açık oldukları doğru anda doğru tüketicilere ulaşmak için ilgili reklamlarla eşleştirildiği yazılı basında onlarca yıldır kullanılmaktadır. Ancak, bağlamsal hedefleme, Büyük Veri ve AI çağında önemli ölçüde gelişmiştir.

Gelişmiş istatistiksel yöntemlerin, makine öğreniminin ve semantik analizin bir araya getirilmesi, geniş ölçekte içgörüler oluşturma potansiyeline sahiptir. Programatik kanallar aracılığıyla bu içgörülerin anında kullanılması imkânı ile birleştiğinde, bağlamsal hedeflemenin "1998'e geri dönmekten" daha fazlası olduğu görülebilir.

Bu durum, tüketicilerin %94'ünün çevrim içi içeriğe göz atarken çevrim içi veri gizliliğinin kendileri için çok önemli veya önemli olduğunu söylediği gizlilik öncelikli bir çağla uyumlu bir durumdur.

GDPR gibi tüketici gizliliği ve güvenliğiyle ilgili düzenlemeler, reklamverenlerin hedefleme, optimizasyon ve analiz için toplayıp kullanabileceği kişisel verilerin kullanımını kısıtlamaktadır. Bu bağlamda, içeriksel hedefleme teklif veya gösterim verileri değil, sayfanın içeriğiyle ilgili bilgiler kullanıldığından, reklamverenler çereze dayalı hedeflemenin yerine geniş ölçekte bağlamsal hedeflemeyi kullanabilirler. Pazarlamacılar, kullanıcıların kişisel verilerine ihtiyaç duymadan, satın alma döngüsünde nerede olduklarını anlamak için ayrıntılı semantik konseptleri kullanarak, geniş bağlamsal kategorilerin ötesine geçebilirler.

Bağlamsal hedefleme, daha önceki göz atma davranışını veya geçmiş içerik tercihleri analiz etme süreci değildir. Bu, çerezlere dayalı işlem yapılmadığı anlamına gelir. Bunun yerine, sayfa bağlamının daha derin bir şekilde anlaşılmasına odaklanılır. En basit şekliyle bu işlem, belirli bir sayfayı sınıflandırmak üzere bir sayfada anahtar sözcüklerle arama yaparak gerçekleştirilebilir.

Daha gelişmiş yaklaşımlarla, reklamverenlerle alakalı daha derin bir bağlam sağlamak amacıyla, sayfadaki kelimeler arasındaki ilişki analiz edilebilir ve değerlendirilebilir. Bu süreç, "ontoloji" olarak adlandırılır. Bu yaklaşımı açıklamanın bir başka yolu, reklamverenlerin kampanyalarını bir reklamın etrafındaki yerleştirmelere ve içeriğe dayalı olarak, onları görüntüleyen müşterilerin tutumuna uyacak şekilde tasarladıkları tüketici merkezli bir strateji olan "davranış pazarlaması" (mindset marketing)dir.

Teknik anlamda ontoloji, hiyerarşik olan ve tüm kavramları, varlıkları ve bunların semantik ilişkilerini içeren titiz ve kapsamlı bir dil organizasyonunu ifade etmektedir. Bu, anahtar kelimelerin ötesine geçme fırsatı verir ve sonuç olarak reklamveren kampanyaları için daha yüksek bir hedefleme doğruluğu imkânı sağlar.

Diğer taraftan konular, çok sayıda belgede birlikte görülme eğiliminde olan terimlerden oluşur. Bu, tek anahtar kelimelerin kısıtlamalarını aşmanın bir başka yolunu sağlar ve daha soyut bir anlamsal düzeyde hedeflemeyi mümkün kılar. Sonuç olarak, bu yaklaşım, anahtar kelimeler doğrudan değil, taşıdıkları anlamlar aracılığıyla eşleştirildiği için daha geniş erişimlere izin verir.

Bununla birlikte, bağlamsal etkileşimin daha etkili olabilmesi için pazarlamacılar, maruziyetten sonra ne olduğunu ölçmek ve bu yayıncılara uygun şekilde kredi atfetmek için yayıncılar arası tanımlayıcılara ihtiyaç duyar. Örneğin, yukarıda belirtilen gerçek zamanlı geri bildirim olmadan aynı bağlamsal konuyu iki yayıncıda hedeflemek, pazarlamacılara hangisinin pazarlamacının sahip olduğu web sayfasında daha değerli davranışlara yol açtığına dair iç görü sağlamayacaktır. Bu nedenle bağlamsal hedefleme, yayıncılar arası tanımlayıcılara dayanan etkili kullanıcı etkileşiminin temel bir parçasıdır. Özünde, doğru kitleyle doğru bağlamda etkileşim kurmaktır.

Çerez içermeyen bağlamsal çözümleri değerlendirirken, başarı için en önemli beş husus şu şekildedir:

1. **Kampanyanızın erişimini ve bağlantı düzeyini artırmak için taktiksel terimler kullanıyor musunuz?**

Kampanyanızı yaratırken, ürünlerinizle gerçekten ilgilenen ve tekliflerinizi önemseyen kitlelere ulaşmanızı sağlayacak doğru terimleri stratejik olarak planlamak için zaman ayırın. Anahtar kelimeler iyi bir başlangıç olsa da markaların sayfanın tamamını kapsayan bağlamsal çözümler seçmesi, yani anahtar kelimeleri tek başına kullanmaması kritik önem taşır.

Örneğin, bir outdoor giyim perakendecisi, reklamlarını kamp, doğa yürüyüşü, evde egzersizi ve diğer açık hava etkinlikleriyle bağlantılı içeriğin etrafına yerleştirebilir. Bununla birlikte, reklamlarının doğa belgeselleri, seyahat tavsiyeleri, barbekü tarifleri, yoga blogları veya köpek eğitimi gibi diğer bağlamlarda da oldukça etkili olduğunu görebilir. En iyi potansiyel müşterilerinizin belirli içerik konularını nasıl sık kullandığını ve bunlarla nasıl etkileşim kurduğunu analiz ederek medya harcamalarınıza daha iyi odaklanabilirsiniz.

2. Markanızın zararlı ortamlardan korunduğundan emin misiniz?

Markaların yaklaşık %52'si, tüketici algısı problemlerine yol açan marka uygunluğu sorunlarıyla birden çok kez karşı karşıya gelmiştir. Yanlış ayarlanan içerik, marka değerlerinin belirtisi olarak değerlendirilebilir.

Günümüzde markalar, itibarlarını zedeleyecek ve marka imajlarını yok edecek konular veya tartışmalarla ilişkilendirilmek istememekte ve bağlam burada devreye girmektedir. Negatif maruz kalma riski her kampanya için kritiktir.

Kampanyalarda yalnızca genel marka uygunluğu konularına dikkat etmek değil, belirli reklam öğelerinde tepkiye neden olabilecek nüansları düşünmek de akıllıca olacaktır. Örneğin, bir araba kazasıyla konulu bir reklamda yer alan bir minivan görüntüsü, markaya uygun değildir.

3. **Markanızın kendine özel ve kampanya hedefleriyle uyumlu özelleştirilmiş bağlamsal segmentasyon oluşturuyor musunuz?**

"Doğru" bağlamın ne anlama geldiğini düşünmenin birçok yolu vardır. Markanız için neyin uygun olduğunu belirlemeniz için bazı ipuçları:

- Müşteri ihtiyaçlarıyla uyumlu olmak - örneğin, ürettiğiniz içerik hedef kitlenize uyumlu olmalıdır.
- Kişilerle/yaşam tarzlarıyla uyumlu olmak - içeriğinizin kişisel hobiler ve etkinliklerle (seyahat, yabancı kültür, yemek ilgi alanları vb.) ilgili olması gerektiği anlamına gelir.
- Daha geniş marka hedeflerini güçlendiren marka değeri oluşturma içeriğiyle uyumlu olmak. Örneğin, bir marka önemli bir ünlü tarafından destekleniyorsa, reklamı o kişiyle ilgili içerikle uyumlu hale getirmek.

4. **İçerik hedeflemenizi gerçek zamanlı olarak otomatize etmenize yardımcı olacak bir bağlamsal analiz çözümü kullanıyor musunuz?**

Bir bağlam ortağının kullanılması, özelleştirilmiş anahtar kelime hedeflemelerinin gerçek zamanlı olarak elde edilmesine yardımcı olabilir.

Bu durum, ortaya çıkan popüler trendlerden yararlanmanıza ve yayınlanırken yeni, marka açısından güvenli bir içeriğin yanında görünmenize olanak tanır. En iyi sonuçları elde etmek için bir içerik semantik-bağlam ortağına sorabileceğiniz sorular şunlardır:

- Hem insan esaslı kullanıcı kitlesini hem de bağlamsal kullanıcı kitlesini kullanmanın değeri nedir ve bunları birbirinin yerine nasıl kullanırsınız?
- Gerçek alıcıları bulmada bağlamsal hedefleme ne kadar etkilidir?
- Trend olan içeriği ne kadar hızlı ve hangi ölçekte belirleyebilirsiniz?
- Özelleştirilmiş segmentleri ne kadar hızlı kullanılabilir hale getirebilirsiniz?
- Mesajımın doğru ortamlarda görüneceğini nasıl garanti edersiniz?
- Anahtar kelimelerin tam sayfa veya sayfa düzeyinde bir analizini sunuyor musunuz?
- Semantik-bağlamsal segmentlerinizin performansı nasıl?

5. **Kampanyanızı optimize ediyor ve yaratıcı hale getiriyor musunuz?**

Kampanyanızı geliştirmek için ilgili içerik terimlerini kullanın. Bunu yapmak, ilgili ortamlarda yeni kitlelere ulaşmanıza, ilgi uyandırmanıza ve mesajlaşmayı uyumlu hale getirmenize olanak tanır. Ayrıca, kampanyanızı renklendirmenin bir yolu olarak da gerçek hayattaki olayları ve durumları kullanarak yaratıcı olabilirsiniz.

Oreo, 2013 Super Bowl sırasındaki elektrik kesintisine öykünen "Dunk in the Dark" kampanyasıyla, bağlamı kullanma konusunda müthiş bir örnektir. Bu, hızlı düşünmenin gücünü ve güçlü bir mesaj vermek için ortamı anlamanın önemini gösteren bir örnek olmuştur.

Bir marka için neyin uygun olup olmadığına karar vermek, anlaşılması çok basit ancak başarılması zor olabilecek bir konudur. Hedef kitlenizi başarıyla bulup onlara ulaşabilmek, reklam kampanyanızın başarısını belirleyecektir. Bir sonraki kampanyanıza bağlamsal reklamı dahil etmek, ilgili içerikle güvenli ortamlarda kitleleri hedeflemenizi sağlayabilir.

Bağlamsal Reklamcılık hakkında daha fazla bilgi için lütfen IAB Europe Bağlamsal Reklamcılık Kılavuzu'na bakın.

BÖLÜM 6 – PAYDAŞLAR ÇÖZÜMLERE NASIL KATKIDA BULUNUR?

Birçok grup ve bireysel paydaş şu anda üçüncü taraf çerezlere erişimin azaldığı bir dünyada sürdürülebilir ve sağlıklı dijital reklamcılık ekosistemini destekleyecek politika ve teknik çözümler üzerinde çalışmaktadır.

Şu anda bu sorunlarla uğraşan gruplar arasında IAB Tech Lab, W3C ve Prebid.org gibi teknik standart organizasyonlarının yanı sıra IAB Europe gibi sektörel ekipler de yer almaktadır. Bireysel paydaşlar arasında ise kendi özel kimlik ve hesap verebilirlik çözümleri üzerinde çalışan şirketler yer almaktadır.

Şirketlerin bu çabalara ve çözümlere nasıl katılmayı seçtikleri şirket koşullarına göre değişir. Ancak, bu alandaki stratejinizi belirlemenize yardımcı olacak bir bağlam sağlamak için bu çabalar ve girişimler hakkında bazı ayrıntılar aşağıda özetlenmiştir.

6.1 Standart Kuruluşları ve Sanayi Ticaret Grubu Girişimleri

Prebid.org

2017 yılında kurulan Prebid.org, sektör genelinde adil, şeffaf ve verimli header teklifleri sağlamak ve teşvik etmek için tasarlanmış bağımsız bir kuruluştur. Aralık 2020 itibarıyla Prebid.org'un 80'in üzerinde üye şirketi bulunmaktadır.

Prebid.org, Prebid.js, Prebid Mobile, Prebid Server, Prebid Video, Prebid Native açık kaynak projelerinin yanı sıra yayıncı liderliğindeki Kullanıcı Kimliği modülü SharedID'yi yönetmektedir. Prebid.org, reklam teknolojisi satıcılarından yayıncılara ve diğerlerine kadar programatik ekosistemin bir parçası olan tüm şirketlere açıktır. Prebid.org, alıcıların ve satıcıların tamamen programatik bir ekosistemde geniş ölçekte işlem yapmasını kolaylaştıracak reklamcılık için standartlaştırılmış, şeffaf teknolojiyi teşvik etmektedir.

Prebid.org'un yayıncılar tarafından yönetilen Kimlik Ürün Yönetimi Komitesi, Prebid.org'un kimliğin geleceğindeki rolünü belirlemekten ve uygulama çabalarını koordine etmekten sorumludur.

Bu komite tarafından yönetilen Prebid, kısa süre önce ücretsiz, bağımsız, şeffaf, açık kaynaklı bir tanımlayıcı olan SharedID'nin piyasaya sürüldüğünü duyurdu. SharedID hem birinci hem de üçüncü taraf çerez ayak izini bir araya getirmekte ve daha önce Epsilon tarafından sahip olunan ve işletilen PubCommon tanımlayıcısı ile birleştirilmektedir. Bu birleştirilmiş tanımlayıcı artık Prebid.org'a aittir ve onun tarafından işletilmektedir.

W3C

World Wide Web Consortium (W3C), Web'in uzun vadeli büyümesini sağlamak için açık teknik özellikler ve standartlar geliştiren uluslararası bir topluluktur.

W3C bu teknik spesifikasyonları, fikir birliği sağlayacak ve W3C topluluğunun onayını kazanacak şekilde geliştirmeyi amaçlamaktadır. Bu, Chrome ekibinin Gizlilik Sandbox'ında belirtilen standartlar konusunda sektörden geri bildirim almak için başvurduğu forumlardan biridir. 2021'de kurulan Özel Reklam Teknolojisi Topluluğu Grubu, reklam önerilerinin tartışılacağı ve tarayıcıların, reklam teknolojisi satıcılarının, yayıncıların ve pazarlamacıların çözümleri tartışabileceği bir örnektir. GitHub'da da Privacy Sandbox API'leri üzerine tartışmalar yürütülmektedir.

Çabalara katılabilmeniz için çeşitli yollar vardır. W3C, konuyla ilgili kişileri tartışma listeleri, etkinlikler, bloglar, çeviriler ve diğer yollarla W3C'ye katılmaya davet etmektedir. W3C Topluluk ve İş Gruplarına katılım herkese açıktır. W3C Çalışma Gruplarına (ve diğer türlere) katılım W3C Üyelerine ve diğer davetli taraflara açıktır. W3C grupları, spesifikasyon incelemelerinin yanı sıra kullanım örnekleri, testler ve uygulama geri bildirimlerinin katkıları yoluyla halkla birlikte çalışır.

Mevcut gelişim açısından en önemli gruplar:

1. Gizlilik Topluluğu Grubu - gelişmiş tarayıcı davranışı yoluyla web'de kullanıcı gizliliğini iyileştirmek için gizlilik odaklı web standartları ve API'ler geliştirmek

2. Web Reklamcılığını Geliştirme Grubu - Web'in kendisindeki standartların ve değişikliklerin kullanıcılar, reklamcılar, yayıncılar, dağıtımcılar, reklam ağları, ajanslar ve diğerleri için ekosistemi ve deneyimi iyileştirebileceği alanları belirlemek

3. Özel Reklam Teknolojisi Topluluğu Grubu - özellikle güçlü gizlilik güvenceleri sağlayarak kullanıcıların çıkarları doğrultusunda hareket ederken reklamcılığı destekleyen web özelliklerini ve API'leri kuluçkaya yatırmak.

4. Web Incubator Topluluk Grubu - yeni web platformu özelliklerinin önerilmesi ve tartışılması için mekân

Reklamla İlgili Teklifler

İsim	Kullanım Durumu	Aktif Katkıda Bulunanlar
FLEDGE API	Hedefleme, Reklam yayını	Criteo, Google, Magnite, NextRoll, RTB House
Topics API	Hedefleme	Google
Core Attribution	API Raporlama	Google, Yahoo Japan
First-Party Sets API	Aynı kuruma ait birden fazla web sitesini 1. parti çerez etiketi altında gruplandırma	Google
Parakeet	Hedefleme, Reklam yayını	Microsoft
Private Click Measurement	Raporlama	Apple
Interoperable Private Attribution (IPA)	Raporlama	Meta, Mozilla
Federated Credentials Management	Siteler arası izleme olmadan e-posta tabanlı Tek Oturum Açma hizmetini koruma	Google
Trust Tokens API	Spam ve Fraud ile mücadele	Google, Yahoo Japan
Gnatcatcher	IP Parmakizi iile mücadele	Google

IAB Tech Lab – Rearc Projesi

Üçüncü parti tanımlama bilgilerinde ve diğer tanımlayıcılarda yaklaşan değişikliklerle birlikte, Project Rearc, tüketici gizliliği ve kişiselleştirmeyi dengelerken, dijital tedarik zincirindeki paydaşların, sektörü desteklemek, dijital pazarlamayı yeniden düşünmeleri ve yeniden tasarlamaları için küresel bir eylem çağrısıdır.

IAB Tech Lab, üye ve üye olmayan paydaşları eğitmek ve "varsayılan olarak gizlilik" adreslenebilir reklamcılık ve ölçümlemeyi yönlendiren yeni teknik standartların ve kılavuzların geliştirilmesine küresel girdiyi kolaylaştırmak için iş birliğine dayalı bir süreç düzenlemektedir.

Ekiplerinizin iş, prensip ve teknoloji perspektiflerinden küresel olarak tartışmaya katılmaları için çeşitli yollar vardır.

Tech Lab üyesi olmayanlar da, çeşitli küresel paydaşlardan girdi toplayan Rearc Ekibi'ne katılabilirler.

IAB Tech Lab üyelerine açık olan daha derinlemesine çalışma grupları aşağıdakilerden oluşmaktadır:

- Adreslenebilirlik için gizlilik merkezli uygulamalara bağlılığı sağlamak üzere bir çerçeve geliştirecek olan **Hesap Verebilirlik** Çalışma Grubu; ve
- İleriye dönük olarak tanımlayıcıların gizlilik merkezli kullanımına yönelik teknik standartları tanımlamayı amaçlayan **Adreslenebilirlik** Çalışma Grubu
- Teknik gizlilik standartlarını tekil bir şema ve kanallar genelinde düzenleyici ve ticari pazar taleplerine uyum sağlayabilecek bir dizi araç haline getirmeyi amaçlayan **Küresel Gizlilik** Çalışma Grubu Bu çalışmalara nasıl dahil olunacağına ilişkin daha fazla bilgiye buradan ulaşabilirsiniz.

IAB Europe - Üçüncü Parti Çerez Sonrası Çalışma Grubu

IAB Europe, IAB Fransa ile ortaklaşa olarak 2020 yılının ortasında "Üçüncü Taraf Çerez Sonrası Görev Gücü" adlı ortak bir girişim başlattı. Görev gücü, W3C ve IAB Tech Lab'in "Project Rearc" kapsamında dijital reklamcılığın evrimi ve potansiyel yeni paradigmalar üzerine yürütülen düşüncelere Avrupa'dan güçlü bir girdi sağlanmasına yardımcı oluyor.

Alt Çalışma Grupları

Çalışma Grubunun üç alt çalışma grubu bulunmaktadır:

- Hesap Verebilirlik Çalışma Grubu
- Adreslenebilirlik Çalışma Grubu
- W3C Çalışma Grubu

Üçüncü Parti Sonrası Çalışma Grubu'na katılmak ister misiniz? Katılım tüm IAB Europe, IAB Fransa ve diğer Ulusal IAB üyelerine açıktır. Bu çalışmalara nasıl katılabileceğiniz hakkında daha fazla bilgiyi burada bulabilirsiniz.

6.2 Özel Çözümler

Giderek artan sayıda şirket, üçüncü parti tanımlama bilgilerine dayanmadan tanımlama yetenekleri sağlayan çözümler geliştirmiş ve pazara sunmuştur. Bunların çoğu, tanımlayıcılarının benimsenmesini kolaylaştırmak için Prebid'de kullanılabilen kimlik modülleri oluşturmuştur. Bu şirketlerden bazıları, reklam teknolojisi platformları ve yayıncılar tarafından kullanılabilen ve reklam değer zincirinde aktarılabilen tanımlayıcılar sunmaktadır. Diğerleri ise yalnızca iş ortakları ve müşterileriyle dahili olarak kullanılabilecek ve tanım gereği evrensel olarak kabul edilemeyecek tanımlayıcılar oluşturmuştur.

Kullanıcılar için veri koruma, şeffaflık ve kontrol konularında açık bir taahhüt tüm kimlik çözümü sağlayıcıları için kilit önemde olmalıdır.

Tarafsızlık bir diğer önemli farklılaştırıcı unsurdur. Reklamcılık ekosisteminde aktif olarak faaliyet gösteren bazı şirketler (alıcı taraf, satıcı taraf veya veri çözüm platformları) kimlik çözümlerini ana işlerini tamamlayıcı bir hizmet olarak sunmaktadır. Öte yandan, yalnızca sektörün faaliyet göstermesi için bir kimlik altyapısı oluşturmaya odaklanan kimlik sağlayıcıları da vardır.

Tarafsızlığın olmaması, bazı reklam teknolojisi platformları rakiplerinin tanımlayıcısını kullanmaktan kaçınabileceğinden, bir tanımlayıcının benimsenmesini etkileyebilir. Benimsenme oranı Kimlik çözümleri için çok önemli bir ölçüttür: bir tanımlayıcıyı ne kadar çok yayıncı ve platform kullanırsa, o kadar etkili ve performanslı olur.

Prebid'de kimlik sağlayıcıların tam listesi:

- Akamai
- Admixer
- Adtelligent
- Audigent
- AMX RTB
- Britepool
- Criteo
- Deepintent
- DMD
- Epsilon
- FLoC
- ID+
- ID5
- Idx
- IntentIQ
- Intimete Merger
- Justtag
- Kinesso
- LiveInent
- Liveramp
- Lotame Panorama
- MediaWallah
- Merkle
- Navegg
- NetId
- NextRoll
- Neustar Fabrickld
- Novatiq
- Parrable
- Pubcommon (şu an sahibi Prebid)
- PubProvided
- Quantcast
- Retargetly Idx
- Shared (şu an sahibi Prebid)
- tapad
- Trade Desk UnifiedId
- Turspid
- Verizon
- Yahoo
- Zeotap ID+

En güncel Prebid listesine buradan erişebilirsiniz.

Kişiye Özel Çözümler

Birçok bireysel şirket, yukarıda 5. bölümde özetlenenler gibi üçüncü parti çerezlerin olmadığı bir dünyada dijital reklam kullanım durumlarını desteklemek için alternatif kişiye özel teknolojiler ve standartlar geliştirmek için çalışmaktadır.

6.3 Yeni Paradigmanın Devam Eden Başarısının Sağlanması

Dijital reklamcılık sektöründekiler üçüncü parti çerezlerin olmadığı bir dünyada hangi standartları ve teknik çözümleri benimsemeyi seçerse seçsin, düzenleyicilere yeni paradigmanın tüketicilerin GDPR gibi yasalar kapsamında verilen gizlilik haklarıyla uyumlu olduğunu gösterme ihtiyacı olacaktır.

Bu katılım çabalarının neye benzeyeceği duruma ve yargı yetkisine göre değişecektir, ancak şirketler genellikle yerel düzenleyicilerle güçlü bağlantıları ve başarılı bir katılım geçmişi olan IAB'leri aracılığıyla etkileşim kurmaya çalışmalıdır.

Örneğin, 2019'da IAB UK, reklam teknolojisi ve gerçek zamanlı teklif verme ile ilgili bir rapor yayınlamalarına yanıt olarak İngiltere Information Commissioner's Office ile sektör katılımını başarıyla yönetti. Daha fazla bilgiye buradan ulaşabilirsiniz.

ÖZET

2021, üçüncü parti çerezleri hakkındaki konuşmalar açısından çalkantılı bir yıl oldu. 24 Haziran 2021'de Chrome, üçüncü parti çerezlerin aşamalı olarak kaldırılması için 2024 sonuna kadar uzatılan gecikmeli bir zaman çizelgesi açıkladı. Chrome'un gecikmesi, sektörün yeni teknik ortamı öğrenme ve buna uyum sağlama ihtiyacını yansıtıyor.

Üçüncü parti çerezleri daha iyi kontrol etme ihtiyacı, GDPR veya CCPA gibi birçok mevzuat eyleminde tasvir edilen veri toplama ve tüketici gizliliği hakkında artan konuşmalarla belirgin hale geldi. Sektördeki herkes kullanıcının gizliliğini daha iyi koruma ihtiyacını destekliyor, ancak büyük değişiklikler reklamverenler ve yayıncılar için zorlukları da beraberinde getiriyor.

Bu güncellenmiş kılavuzda, sektörün yaklaşan değişikliklerle nasıl başa çıktığını, hangi yeni teknolojilerin ortaya çıktığını ve reklamverenlerin ve yayıncıların üçüncü taraf çerezleri sonrası dönemde en iyi şekilde nasıl öğrenebileceklerini, hazırlanabileceklerini ve gelişebilecekleri inceleniyor.

Söz konusu yayıncılar olduğunda, "sırada ne var?" sorusunun yanıtı oldukça basit: Birinci parti veri. Birçok yayıncı, özellikle de premium içeriğe, oturum açmış kullanıcılara ve her türlü aboneliğe sahip olanlar, kullanıcıları hakkında potansiyel reklamverenlerin ilgisini çekmede büyük bir değer olabilecek değerli bilgilere zaten sahip.

Öte yandan, reklamverenlerin programatik ortamın alıştırdığı bazı özellikler olmadan çalışmayı öğrenmeleri gerekecek. Frekans sınırlama, çapraz yayıncı tanımlayıcıları ve hatta DMP'ler gibi özelliklerin mevcut halleriyle uzun süre kullanılamayacağından eminiz. Ayrıca, reklamverenlerin kampanyalarına maruz kalmayı ölçme biçimleri de doğrudan etkilenecek ve maruz kalma ve ilişkilendirme ölçümü için üçüncü partif çerezlerinin yerine kullanılabilecek mevcut çözümlerin bir listesini sunuyoruz.

Sektör, reklamverenin frekans sınırlaması ve/veya hedefli, optimize edilmiş reklamcılığa yardımcı olmak için cihaz veya kullanıcı düzeyinde kullanabileceği reklam tanımlayıcıları gibi çözümlere giderek daha aşina hale gelmektedir.

Dahası, zaten iyi bilinen bazı çözümler yeniden doğuyor. Bağlamsal hedefleme, CRM ve e-posta gibi çözümlere farklı bir perspektiften bakılıyor ve sektör zaten anladıkları ve ellerinde olanları yeni bir avantaj için nasıl kullanabileceklerini merak ediyor.

Son olarak, sektör önümüzdeki 12 ay ve sonrasında gelişmek ve ilerlemek için eşsiz bir fırsata sahiptir ve tüm paydaşları sektöre katkıda bulunmak ve sektör için çözümler geliştirmek üzere ilgili sektör gruplarına nasıl dahil olabileceklerini keşfetmeye teşvik ediyoruz.

Yerel düzeyde, birçok ulusal IAB, geliştirilen çözümleri tartışmak ve geri bildirimde bulunmak için görev güçleri oluşturmuştur, bu nedenle nasıl dahil olabileceğinizi öğrenmek için IAB ile iletişime geçebilirsiniz.

Avrupa düzeyinde, IAB Eurpe'un, W3C ve IAB Tech Lab'in Rearc Proje'sinde değerlendirilenler gibi sektör önerilerini gözden geçirmek ve geri bildirim sağlamak için IAB Europe kurumsal ve ulusal IAB üyelerini bir araya getiren özel bir çalışma grubu vardır.

Kılavuzun bu versiyonu, bugün bildiğimiz bilgi ve bilgileri yansıtmaktadır. Sürekli gelişen sektörümüzde olduğu gibi, önümüzdeki 12 ay boyunca daha fazla gelişme ve ilerleme olacaktır. Bu nedenle, Programatik Ticaret Komitesi (PTC), tüm paydaşları bilgilendirmek ve ilham vermek için kılavuzu güncellemeye ve yeni versiyonlar yayınlamaya devam edecektir.

BU VERSİYONA KATKIDA BULUNANLAR

Yasal Uyarı: IAB üyesi şirket çalışanları, IAB Europe Programatik Ticaret Komitesi'nin üyeleri olarak bu rapora katkıda bulunmuştur. IAB üyesi şirket çalışanları, şirketlerinin iş veya faaliyetlerine ilişkin bilgilerin tamamını sağlamamıştır. Bu raporda yansıtılan genel içerik ve perspektifler, IAB üyesi şirketlerin değil Komite'nin eseridir.

IAB Europe, bu kılavuzun hazırlanmasına katkı sağlayan aşağıdaki destekçilerine teşekkür eder.

Alex Berger, Kıdemli Pazarlama Direktörü, Satın Alma Tarafı Ürünler, Adform

Xara McDonald, Çözümler Mühendisi, Amobee

David Goddard, İş Geliştirme Başkan Yardımcısı, DoubleVerify

Emmanuel Josserand, Kıdemli Direktör Marka, Ajans ve Sektör Freewheel

Ben Geach, Danışmanlık Lideri, gTech Profesyonel Hizmetler, Google

Jamie Penkethman, Kimlik Ürün Pazarlama, Index Exchange

Elżbieta Kondzioła, Çevrim içi Satış Direktörü, LOVEMEDIA and

Łukasz Włodarczyk, Programatik Ekosistem Büyümesi & Yenilikler Başkan Yardımcısı, RTB House, IAB Polonya'yı temsilen

Ines Talavera de la Esperanza, Kamu Politikası Sorumlusu, IAB Europe

Ryan Afshar, İngiltere Yayıncılar Başkanı & **Tim Geenen**, Genel Müdür, Avrupa Adreslenebilirlik, LiveRamp

Garrett McGrath, Kıdemli Başkan Yardımcısı, Ürün Yönetimi, Magnite

Ferdinand David, VP, Ürün Politikası ve Uyumluluk Lideri, , MediaMath

James Kerr, Bölge Danışmanı ve Veri Koruma Sorumlusu, EMEA ve APAC, MediaMath

Tanya Field, Kurucu Ortak & CPO, Novatiq

Rémi Lemonnier, Kurucu Ortak ve Başkan, Scibids

Patrick Jähnichen, Küresel Ürün Direktörü, Veri ve Makine Öğrenimi, ShowHeroes Group

Zuzanna Zarebinska, Starteji Analisti, Yieldbird

Florian Lichtwald, Genel Müdür, CBO, Zeotap

ÖNCEKİ VERSİYONLARA KATKIDA BULUNANLAR

Alex Berger, Kıdemli Pazarlama Direktörü, Satın Alma Tarafı Ürünler, Adform

Emily Roberts, Programatik Ticaret Müdürü EMEA, BBC Global News

Ben Hancock, Programatik Ticaret Küresel Başkanı, CNN International

Akshay Bhattacharjee – İskandinav ve CEE Bölgesi Programatik Çözümler Uzmanı, IAS

Ian Maxwell, IAB Ireland'ı temsilen Converge Digital

Thibault Montanier, Veri Yöneticisi ve Entegrasyon Uzmanı, Sirdata & IAB Europe Üçüncü Parti Çerez Sonrası Çalışma Grubu Eş Başkanı

Alex Cone, Kıdemli Direktör, Ürün Yönetimi, Jordan **Mitchell**, Kıdemli Başkan Yardımcısı, Tüketici Gizliliği, Kimlik ve Veri, IAB Tech Lab

Sara Vincent, Kıdemli Direktör, Stratejik Ortak Geliştirme, Index Exchange

Gökberk Ertunç, Programatik Müdürü, OMD Türkiye / IAB Türkiye

Laine Rosa, Ürün Müdürü, Outbrain

Maria Shcheglakova, Pazarlama Direktörü EMEA, PubMatic

Garrett McGrath, Başkan Yardımcısı, Ürün Yönetimi, Magnitide

Alwin Viereck, Programatik, Reklam Teknolojisi ve Ürün Başkanı, United Internet Media

Gabrielle Le Toux, Kıdemli Pazarlama Müdürü, Xandr

Szymon Pruszyński, Büyüme Başkanı Yieldbird

Valbona Gjini, Pazarlama Direktörü, ID5

Zara Erismann, Avrupa Yayıncılar Başkanı, LiveRamp

William Lee, Mgr, Ürün Politikaları ve Uyum Müdür, **Chris Keenan**, İş Geliştirme Bölge Başkan Yard. ve **Jamie Penkethman**, Kıdemli Ürün Pazarlama Direktörü

Tanya Field, Kurucu Ortak & CPO, Novatiq

Miles Pritchard, GM – Veri Yönetimi Çözümleri, OMD

Carlotta Zorzi, Küresel Marka İş birlikleri, Oracle Data Cloud

Joshua Koran, Yenilik Lab GM, Zeta Global

Livia Busseni, Küresel Çözümler Mühendisliği Başkan Yardımcısı, Zeotap

IAB Europe İletişim

Lauren Wakefield
Marketing & Industry Programmes Director
wakefield@iabeurupe.eu

Marie-Clare Puffett
Senior Manager, Marketing & Industry Programmes
puffett@iabeurope.eu

www.iabeurope.eu

www.iabtr.org