

# 디지털 광고 - 거대하고, 은밀하고 위험한 시장

...

2022년 4월 6일

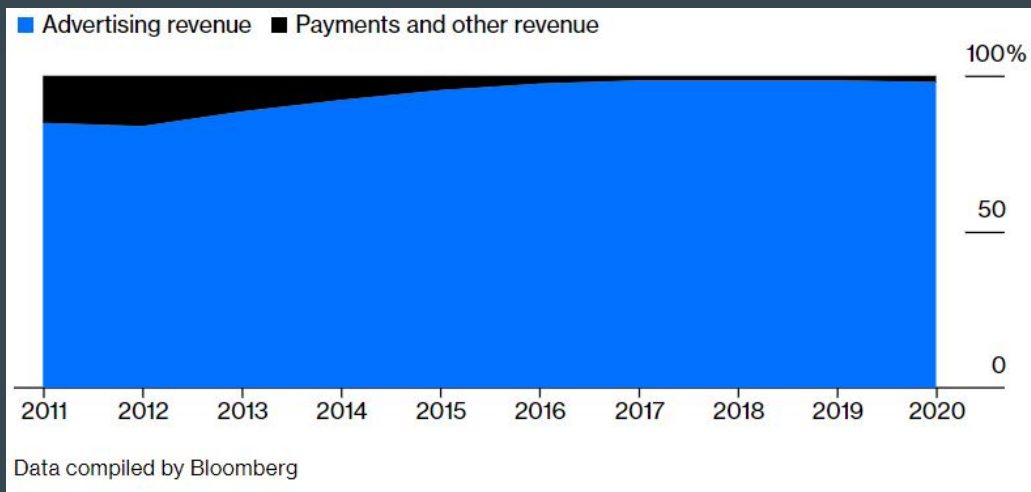
이은우(법무법인 지향)

“Senator, we run ads.”(2018, Mark Zuckerberg)



2020, 메타 수익의 98%, 알파벳 수익의 81%는 광고수익

## 메타(Facebook)의 수익 중 광고 비중(2011~2020)



출처 : 블룸버그

# 온라인 광고 (검색 광고 / 분류 광고 / 디스플레이 광고)

## Q4 2021 Earnings Are In.

∞ Meta Alphabet  
amazon

### The Advertising Revenues of Alphabet, Meta and Amazon in 2021 (vs 2020)

Global Ad Spend (2021 vs 2020)  
\$ Billions, % YoY change

ebiquity



\* Amazon breaks down its earnings by 'Advertising Services' for the first time in Q4 2021, this was bundled in 'Other' before. Historical data is provided from Q3 2020. Q1 & Q2 revenues have been normalized using 6 quarter averages.

Sources: quarterly earnings reports & eMarketer

ebiquity

전세계 광고지출 중 알파벳, 메타, 아마존의 비중

# Cookie, 1994~2022, 1994(Netscape), 1995(Explorer)



루 몬툴리(당시 23세)



“How ads follow you around the internet” 인터뷰 (2020. 2. 3.)

# Cookie의 역할



“도리, 도리? 그게 뭐지? 아~ 내 이름이지!”

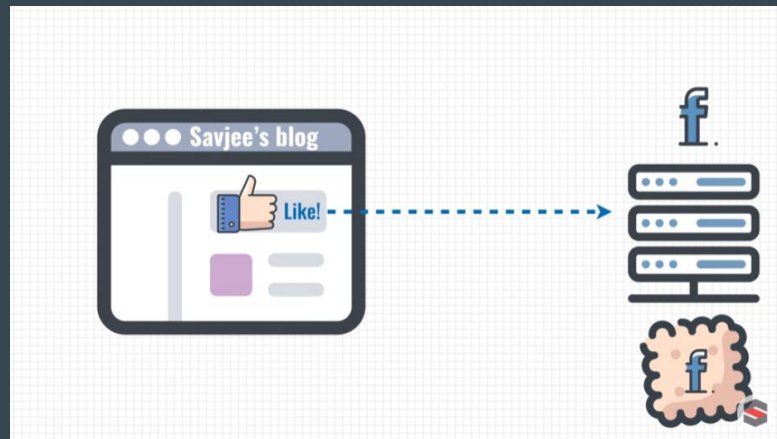
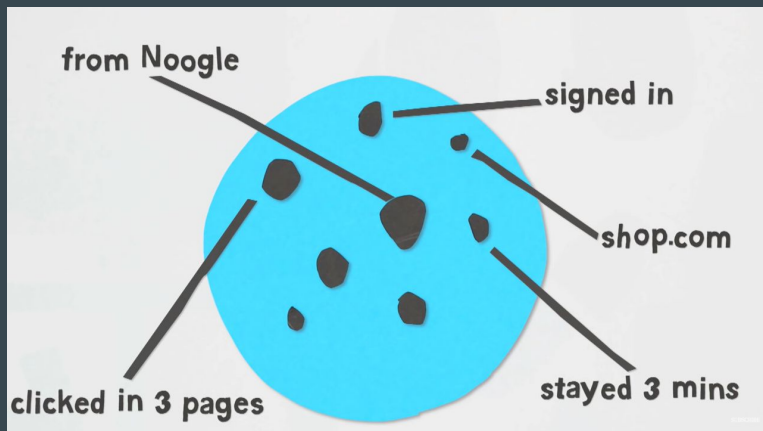
# The Cookie That Ate The World (teconomy.com, 2018. 12.)

쿠키가 세상을 먹다!!!

- 쿠키(300 cookies, 4096 bytes, scoped to domain name)의 변질



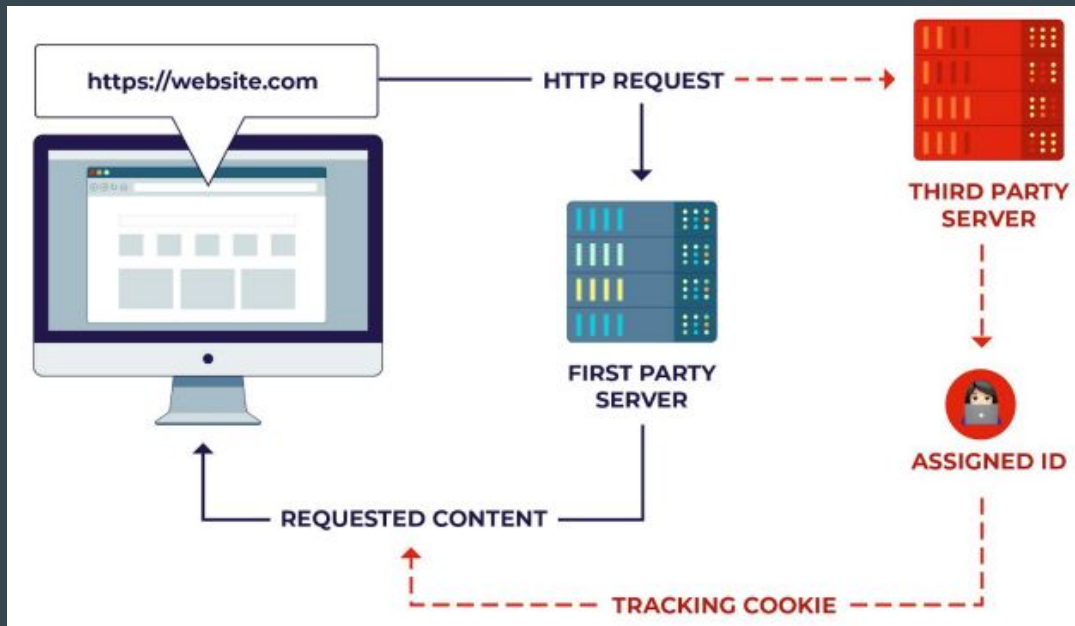
# 세상을 먹은 Cookie - “제3자 쿠키”



Website cookies explained(Guardian Animations)(2014. 9. 12.)

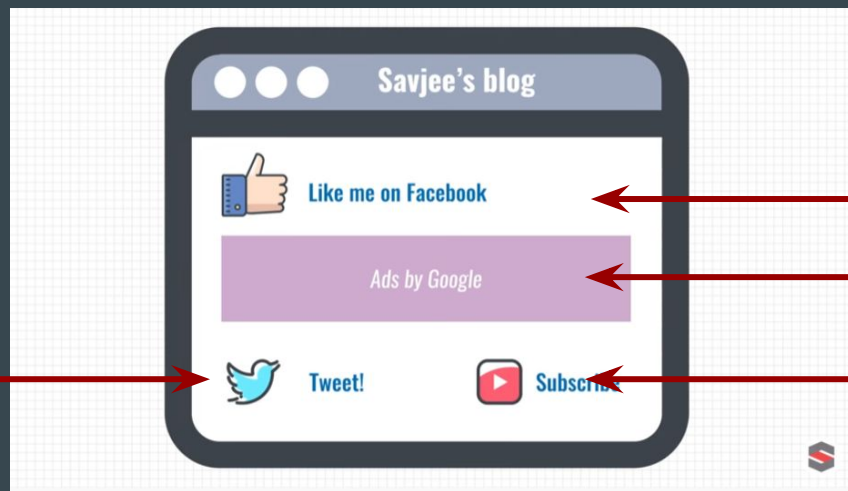


# 추적 쿠키의 작동 구조



Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(2019, EFF)

# 제3자 쿠키(Third party cookies)

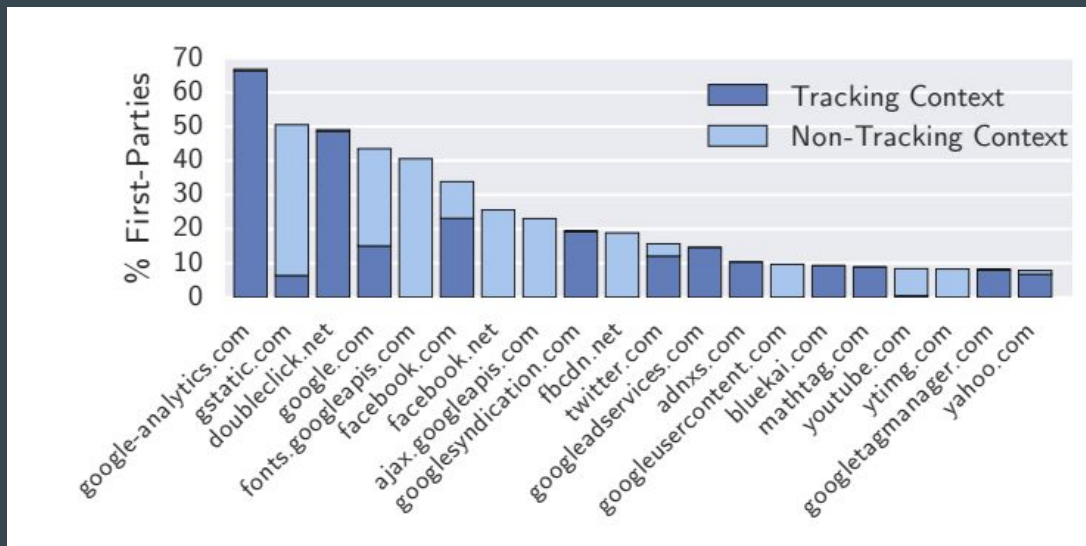


SDK(Software Development Kit) : 소프트웨어 개발 키트(SDK)의 일부로 포함. 액세스 권한, 분석, 추적 및 광고 목적. **제3자로**  
**데이터 전송** : SDK를 제공한 제3자 공급업체로의 직접 데이터 전송을 용이하게 함. **은밀** : 데이터를 추적하거나 은밀하게 수집하는 데 사용할 수 있음. 상당한 기술적 전문 지식이 없으면 소비자는 앱에 있는지 여부를 알 수 없음. **기능 은폐** : 다른 사용자 기능을 **제공**하고, 그 내용으로 사용자에게 표시(예: Facebook "좋아요 버튼" 또는 포함된 YouTube 동영상)

# 추적(상위 100만개 사이트와 앱의 제3자 전송 분석)

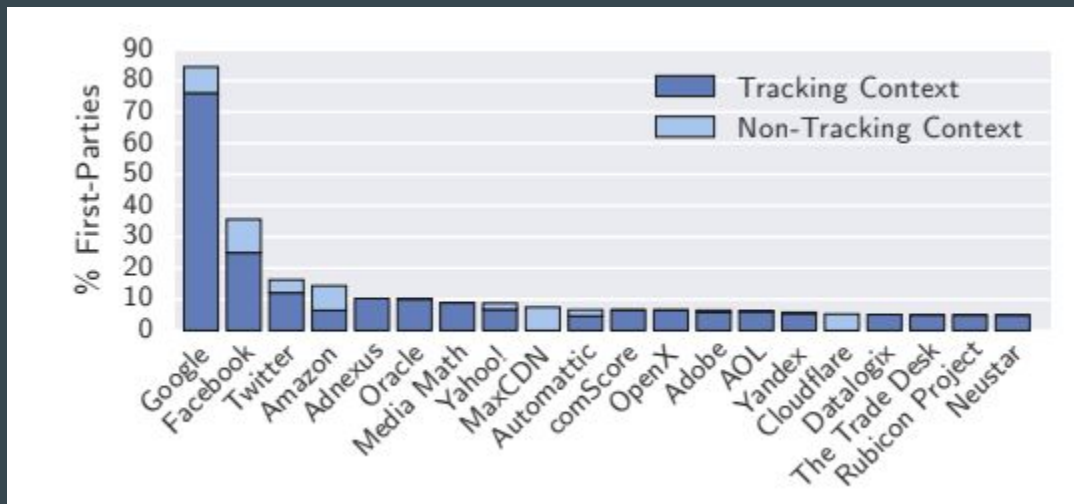
Online Tracking: A 1-million-site Measurement and Analysis(Steven Englehardt 외, 2016)

상위 100만 개(alexa) : 웹 사이트는 평균 34개, 앱은 평균 10개의 제3자에게 데이터 전송



상위 100만개 사이트에서 정보를 가져가는 제3자 순위와 비율

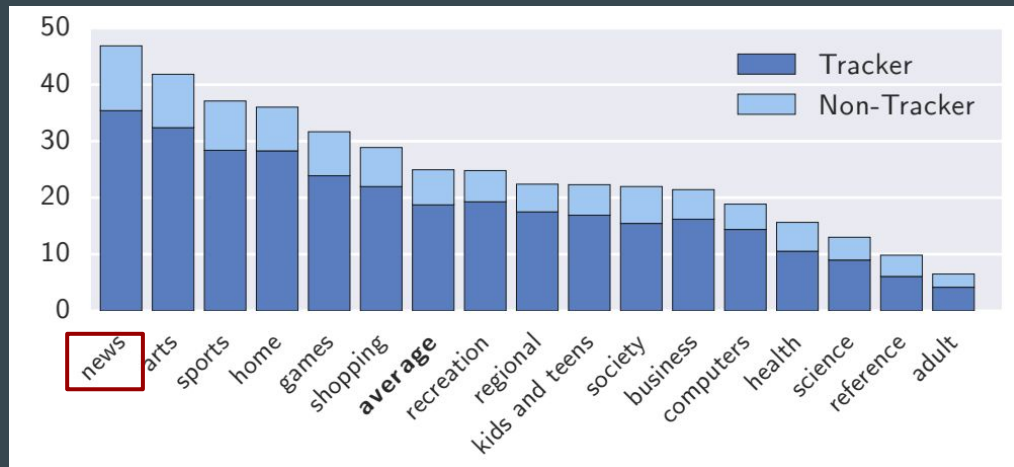
# 추적(상위 100만개 사이트와 앱 분석)



상위 100만개 사이트에서 정보를 가져가는 제3자 순위와 비율

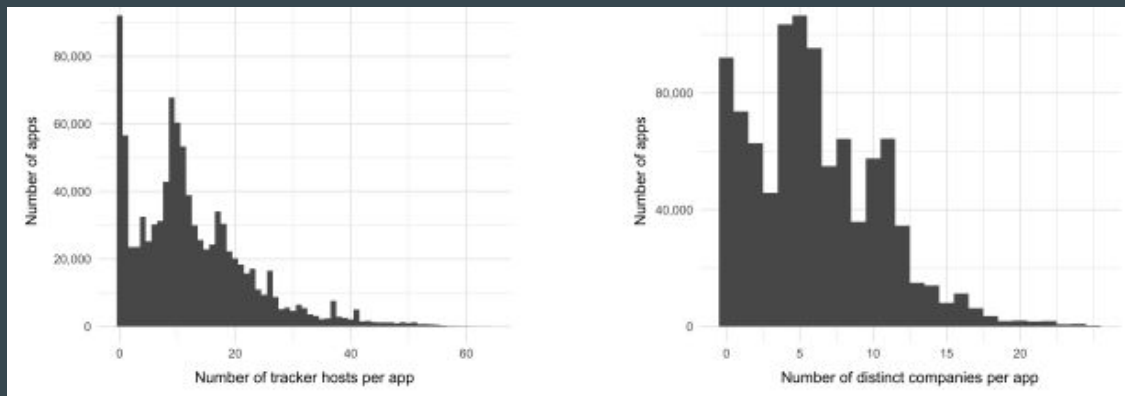
Google Play 스토어에서 사용할 수 있는 959,000개의 앱에 대한 연구(2018, "Third Party Tracking in the Mobile Ecosystem", Reuben Binns 등, <https://arxiv.org/abs/1804.03603>) - DoubleClick, Admob 및 AdSense는 모든 앱의 88% 이상에 존재, Facebook은 42% 이상에 추적기를 통합

# 각 카테고리별 제3자 추적기의 평균 숫자(2016)



뉴스 사이트의 추적기가 많다는 것의 의미는?

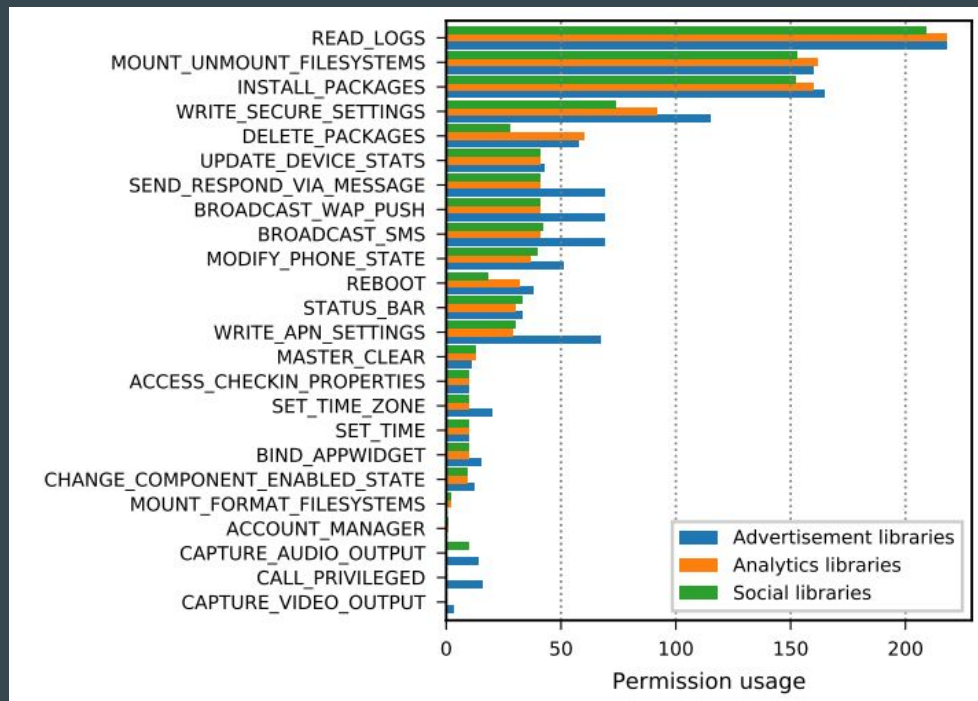
# 추적(상위 100만개 사이트와 앱 분석)



Root parent	% apps	Subsidiary	% apps	Country
Alphabet	88.44	Google	87.57	US
		Google APIs	67.51	US
		DoubleClick	60.85	US
		Google	39.42	US
		Analytics		
		Google Tag Manager	33.88	US
		Adsense	30.12	US
		Firebase	19.20	US
		Admob	14.67	US
		YouTube	9.51	US
Facebook	42.55	Facebook	42.54	US
		Liverail	1.03	US
		Lifestreet	<0.01	US
Twitter	33.88	Twitter	30.94	US
		Crashlytics	5.10	US
		Mopub	2.51	US

상위 100만개 앱의 제3자 추적기 숫자와 제3자 순위와 비율

# System permissions requested by pre-installed apps embedding TPLs



An Analysis of Pre-installed Android Software (2019, Julien Gamba 외)

# An Analysis of Pre-installed Android Software (2019, Julien Gamba외)

Accessed PII type / behaviors		Apps (#)	Apps (%)
Telephony identifiers	IMEI	687	21.8
	IMSI	379	12
	Phone number	303	9.6
	MCC	552	17.5
	MNC	552	17.5
	Operator name	315	10
	SIM Serial number	181	5.7
	SIM State	383	12.1
	Current country	194	6.2
	SIM country	196	6.2
	Voice mail number	29	0.9
Device settings	Software version	25	0.8
	Phone state	265	8.4
	Installed apps	1,286	40.8
	Phone type	375	11.9
	Logs	2,568	81.4
Location	GPS	54	1.7
	Cell location	158	5
	CID	162	5.1
	LAC	137	4.3
Network interfaces	Wi-Fi configuration	9	0.3
	Current network	1,373	43.5
	Data plan	699	22.2
	Connection state	71	2.3
	Network type	345	10.9
Personal data	Contacts	164	11
	SMS	73	2.31
Phone service abuse	SMS sending	29	0.92
	SMS interception	0	0
	Disabling SMS notif.	0	0
	Phone calls	339	10.7
Audio/video interception	Audio recording	74	2.4
	Video capture	21	0.7
Arbitrary code execution	Native code	775	24.6
	Linux commands	563	17.9
Remote conn.	Remote connection	89	2.8

Volume of apps accessing / reading PII or showing potentially harmful behaviors.

Organization	# of apps	# of domains
Alphabet	566	17052
Facebook	322	3325
Amazon	201	991
Verizon Communications	171	320
Twitter	137	101
Microsoft	136	408
Adobe	116	302
AppsFlyer	98	10
comScore	86	8
AccuWeather	86	15
MoatInc.	79	20
Appnexus	79	35
Baidu	72	69
Criteo	70	62
PerfectPrivacy	68	28
Other ATS	221	362

모바일의 상위 15개 광고 추적 서비스 업체들과 연결된 앱들



# “디지털 지문” - 삭제할 수 없는 추적기



<https://www.flickr.com/photos/93243105@N03/8477734222>


사용자별로 고유한 브라우저와 특정 하드웨어 설정의 특성 목록  
브라우저가 웹사이트에 액세스하기 위해 보내야 하는 정보 포함.  
추적 스크립트가 수집한 걸보기에 중요하지 않은 데이터(예: 화면 해상도 및 설치된 글꼴)도 포함.  
추적 사이트는 모든 작은 조각을 함께 연결하여 장치의 고유한 그림이나 "지문"을 형성할 수 있음.  
쿠키와 달리 디지털 지문은 삭제할 수 없음.

# Digital Fingerprintings - 브라우저 지문

AmIUnique

 My fingerprint

 My history

 My extension ▾

 Global statistics

 FAQ

 Privacy policy

 Privacy tools

 Links

## Learn how identifiable you are on the Internet



Help us investigate the diversity of web browsers.

This website aims at studying the diversity of browser fingerprints and providing developers with data to help them design good defenses. Contribute to the efforts by viewing your own browser fingerprint or consult the current statistics of data provided by users around the world!

[View my browser fingerprint](#)

If you click on this button, we will collect your browser fingerprint, we will put a cookie on your browser for a period of 4 months. More details are available in the privacy policy

[Check out the blog post for our new NDSS 2022 paper on GPU fingerprinting with WebGL!](#)

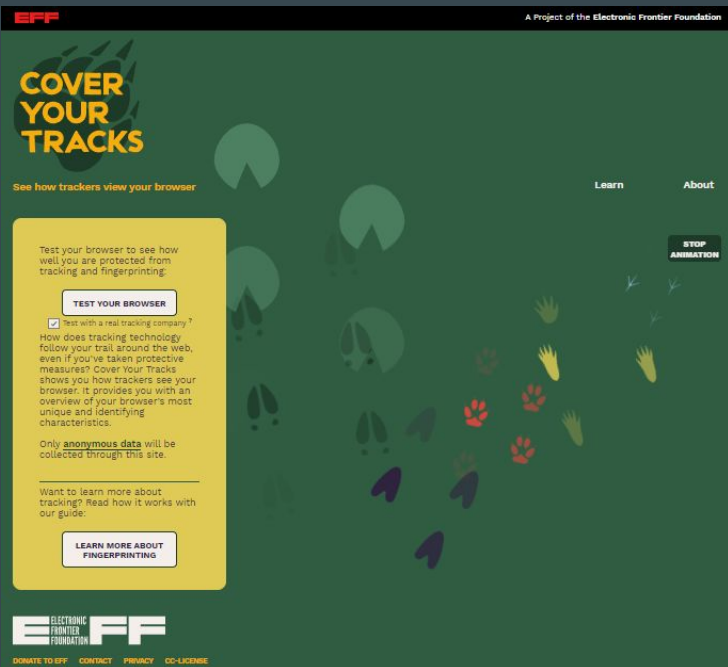
Thanks to everybody who visits the site and helps us collect data to find these privacy bugs.

Are you unique?

**Yes! (You can be tracked!)**

<https://amiunique.org/>

# 당신의 브라우저는 201,970번의 테스트 중 유일!



The image shows the 'Cover Your Tracks' website interface. At the top, it says 'EFF' and 'A Project of the Electronic Frontier Foundation'. The main heading is 'COVER YOUR TRACKS'. Below it, there's a sub-heading 'See how trackers view your browser' and links for 'Learn' and 'About'. A yellow box contains the text: 'Test your browser to see how well you are protected from tracking and fingerprinting.' Below this is a 'TEST YOUR BROWSER' button. A checkbox is checked with the text 'Test with a real tracking company?'. The text continues: 'How does tracking technology follow your trail around the web, even if you've taken protective measures? Cover Your Tracks shows you how trackers see your browser. It provides you with an overview of your browser's most unique and identifying characteristics. Only anonymous data will be collected through this site. Want to learn more about tracking? Read how it works with our guide.' At the bottom of the yellow box is a 'LEARN MORE ABOUT FINGERPRINTING' button. The background is dark green with colorful handprints and footprints.

Our tests indicate that you are not protected against tracking on the Web.

#### IS YOUR BROWSER:

Blocking tracking ads?	<u>No</u>
Blocking invisible trackers?	<u>No</u>
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

## Your Results

Your browser fingerprint **appears to be unique among the 201,970 tested in the past 45 days.**

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.62 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here.](#)

## Detailed Results

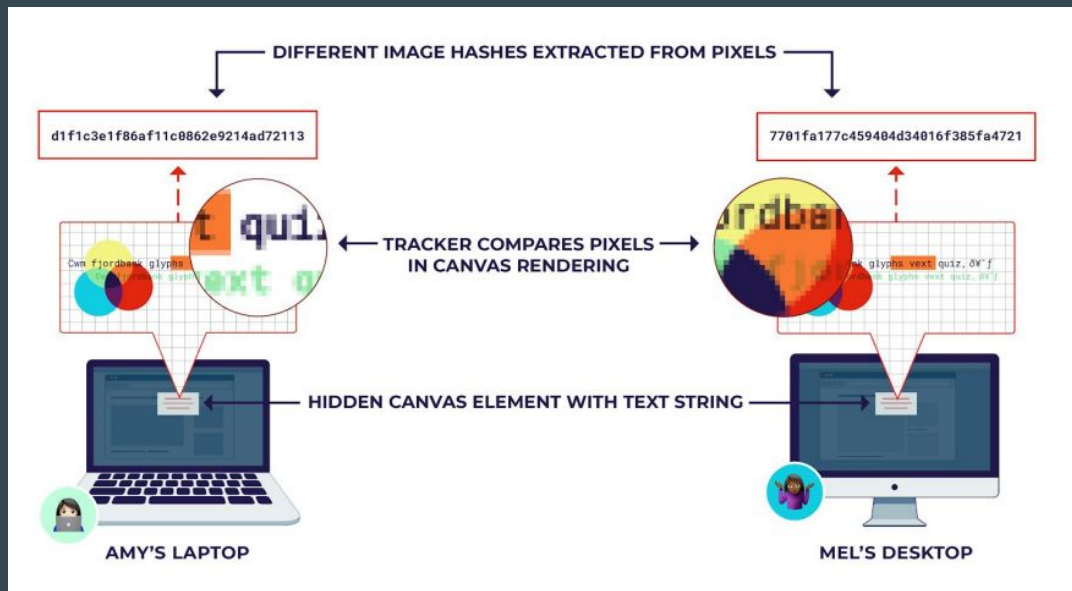
Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

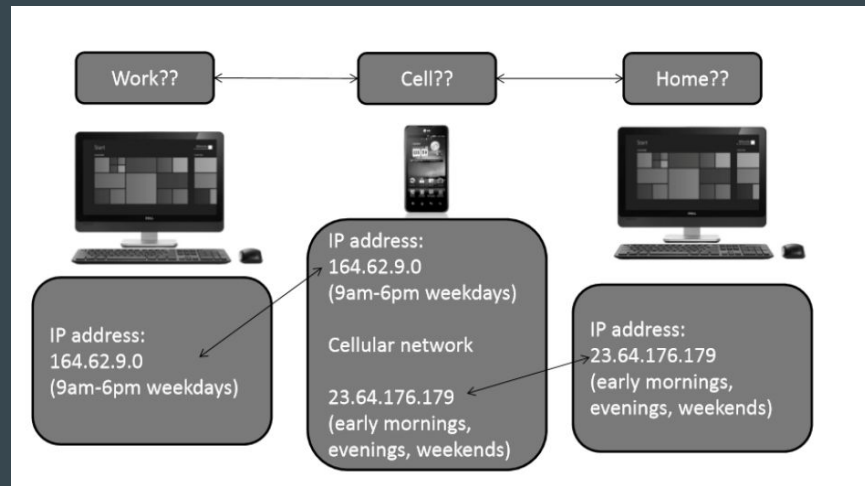
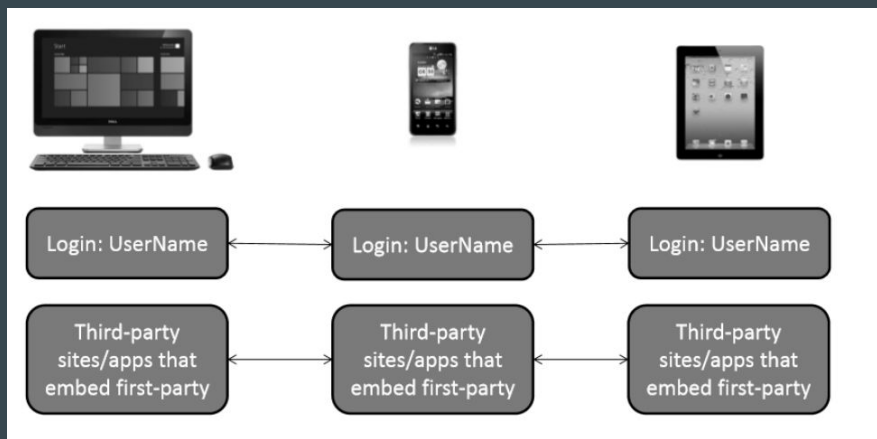
<https://coveryourtracks.eff.org/> 를 통한 테스트

# Digital Fingerprintings - Canvas 지문



추적기는 도형, 그래픽 및 다른 글꼴의 텍스트를 렌더링한 다음 그려지는 픽셀의 "해시"를 계산합니다. 해시는 하드웨어, 펌웨어 또는 소프트웨어가 작은 차이만 있어도 장치마다 다릅니다. "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)"

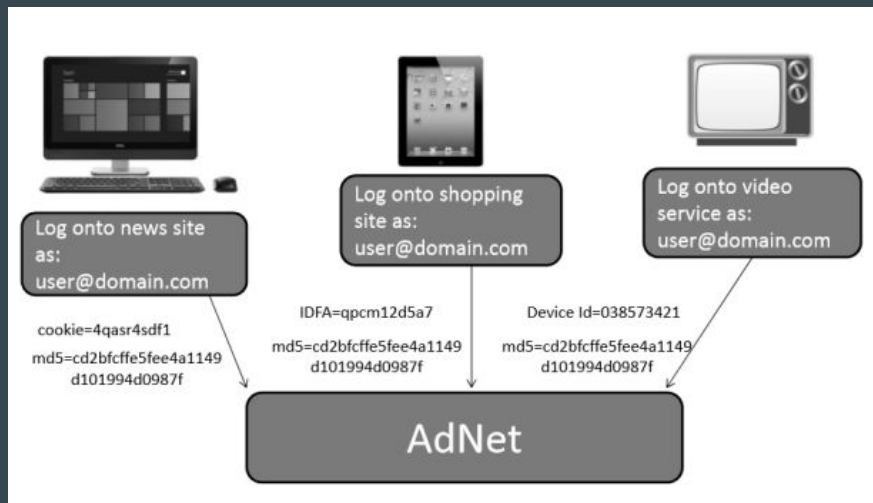
# 추적의 기술 : 기기간 매칭(결정적 vs 확률적)



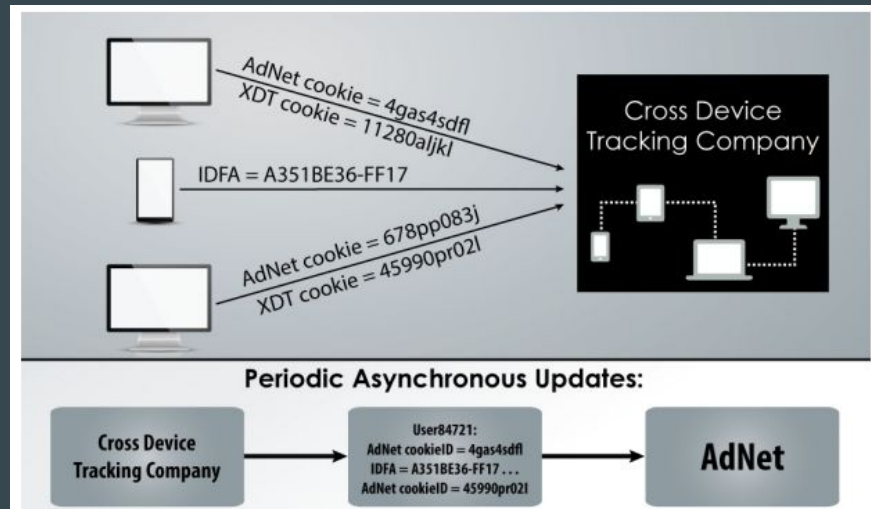
동일한 이름으로 로그인한 여러 기기

휴대폰이 근무시간에 접속한 IP와 주말에 접속한 IP

# 추적의 기술 : Device Graph 통합



ID를 통한 통합



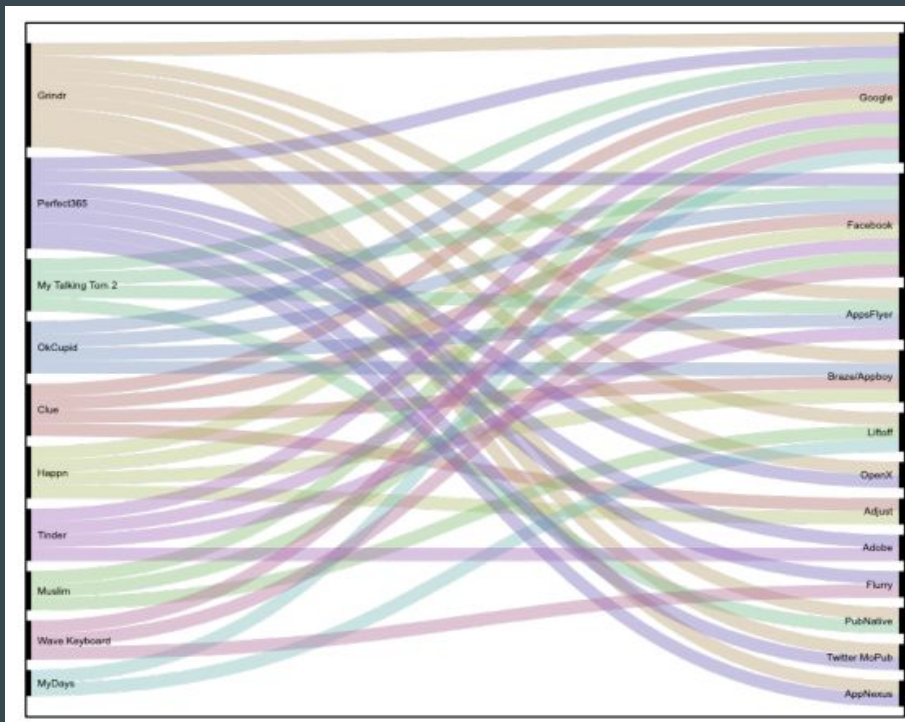
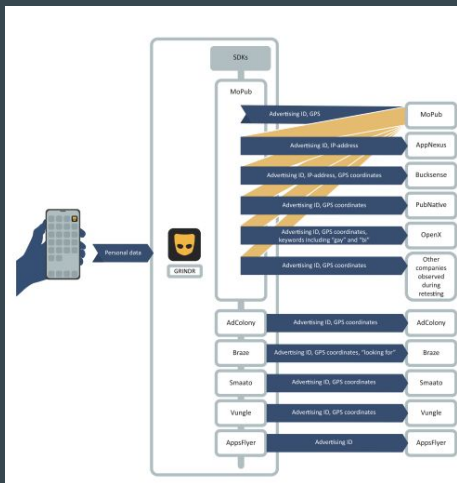
Cookie 동기화

## 그 밖에도...

- CAPTCHAs, reCAPTCHA v3
- Embedded media players
- Analytics and tracking pixels
- Session replay services
- WiFi hotspots and wireless beacons

“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)”

# 앱과 추적기, 데이터 브로커



Mnemonic, "Review of communication from apps" <https://www.forbrukerradet.no/out-of-control/>



# 데이터 브로커 - Fysical

**High Accuracy Place Visit Data**  
Enhance your offering with the most accurate dataset of place visitors on earth

GET ACCESS NOW

- Movement Data**  
We maintain a human movement SDK that is installed across hundreds of mobile applications. This generates the highest accuracy ground-truth location data.
- Place Visit Data**  
We use location data truth sets, combined with a proprietary Fysical Places database, to provide the most accurate visit data.
- Fysical Places**  
We maintain the most accurate US commercial POI dataset for our own business needs and yours.

## Fysical

"지구상에서 가장 정확한 방문자 데이터 세트"를 자랑하는 샌프란시스코 기반 위치 데이터 브로커

"수백 개의 모바일 애플리케이션에 설치되는 인간 움직임 SDK를 통해 수집된 데이터는 인구의 25%에 대한 인간 움직임 데이터가 포함된 데이터베이스를 유지하는 데 사용".

Fysical이 앱에서 GPS 좌표와 광고 ID를 지속적으로 수신, 1분에 여러 번 GPS 좌표를 수신

"우리는 수백 개의 모바일 애플리케이션에 설치된 인간 움직임 SDK를 유지 관리합니다. 이것은 가장 정확한 지상 실측 위치 데이터를 생성합니다."

Fysical은 데이터를 "최종 사용자가 관심을 가질 수 있는 콘텐츠, 광고, 제안 또는 기타 마케팅 솔루션의 전달을 촉진하거나 활성화"하기 위해 이 데이터를 사용합니다. 수집 후 7년이 지나면 데이터를 삭제하거나 비식별화한다고 주장

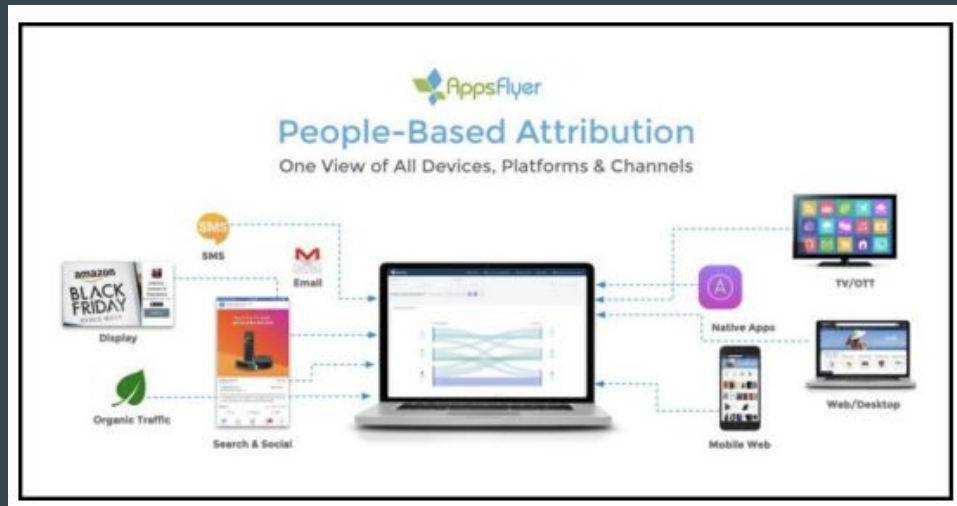
# 데이터 브로커 - AppsFlyer

AppsFlyer 웹사이트 "전 세계에 연결된 84억 개의 장치"  
에서 얻은 통찰력을 활용한다고 주장. "전 세계  
스마트폰의 98%"

- 사용자의 광고 ID, GPS 좌표, 생일, 성별 및 "목표 성별"에 대한 정보를 수신하는 것을 관찰
- 장치의 자력계, 자이로스코프 및  
가속도계로부터 상세한 센서 데이터를 수신

## AppsFlyer SDK

- AppsFlyer SDK는 분석, 광고 리타게팅 및 통합 광고 네트워크를 포함한 다양한 기능
- 230억 건의 앱 설치와 450억 건의 앱 열기를 추적
- 15,000개 이상의 앱.
- 주요 브랜드, 광고 네트워크 및 데이터 브로커를 포함하여 2000개 이상의 "통합 파트너"를 보유



# 데이터 브로커- MoPub



# 데이터 브로커 - Safegraph, Fluxloop

The screenshot shows the Safegraph website homepage. At the top left is the Safegraph logo, a blue cube-like icon. To its right is the text 'SAFEGRAPH'. Further right are navigation links: 'USE CASES', 'CASE STUDIES', 'DOCS', 'CONTACT SALES', and a 'BUY DATA' button. The main heading reads 'IMPROVE LOCATION-BASED MARKETING WITH SAFEGRAPH PLACES'. Below this is a paragraph: 'SafeGraph Places, a dataset of 5 million Points-of-Interest (POI), empowers advertisers to create more accurate and efficient location-based marketing solutions.' At the bottom are two buttons: 'Preview & Buy Data' and 'Contact Sales'.

The screenshot shows the Fluxloop website homepage. At the top left is the Fluxloop logo, a red grid icon followed by the text 'fluxloop'. To the right are navigation links: 'HOME', 'PINCH', 'PRIVACY', and 'ABOUT US'. The main content area features three large statistics: '> 5500 Physical sensors', '>76 Apps with Pinch', and '>1500k Unique end users'. Below these are five icons representing different data types: 'Location data' (a location pin), 'Behaviour data' (a person icon), 'Customer data' (a group of people icon), 'Live reports and visuals' (a bar chart icon), and 'Find your ideal target group' (a person icon). At the bottom are three more icons: 'Operational dashboards' (a pie chart icon), 'Automated real-time contextual marketing' (a speech bubble icon), and 'Deep insight drivers' (a pair of glasses icon).

# 데이터 브로커 - Unacast, Placer

## Transform Human Mobility Data into Actionable Insights.

Understanding human behavior is critical to every business - discover how the  
Strategic Human Mobility Insights can help.



# 데이터 브로커 - Placed, Receptiv/Verve

## Placed Targeting Segments

Placed uses the following elements to construct segments that can be used for targeting.

### TARGETING ATTRIBUTES



**Business Visitation**  
Top 200 Businesses



**Gender**



**Operating System**



**Age Range**  
(18-24, 24-34, 35-44)



**Marital Status**



**Income**



**Geography**



**Apps**



**Education**



**Children**



## IDENTIFY YOUR AUDIENCE

Location intelligence uncovers why your audiences go where they go. Discover who they are and identify ideal moments to connect.

Show me how



# 데이터 브로커 - Verve, Neura



## PROVEN BEHAVIORAL CHANGE

Track specific audiences over time and optimize their experiences to shape habits and loyalty.



## DEMONSTRATION OF INCREMENTALITY

Receive granular detail on how your experiences change what consumers do and where they go.

NEURA

Product ▾ Industries ▾ Resources ▾ Developers ▾ Pricing Company ▾

**1:1 Relationships**  
Talk to individual people, at scale.

**Real-World Behavior**  
Live segments that adapt as your users change their lifestyle and routines.

**Moment-Based Engagement**  
Capture the right moment for each user.

# 아이덴티티 그래프(Criteo)



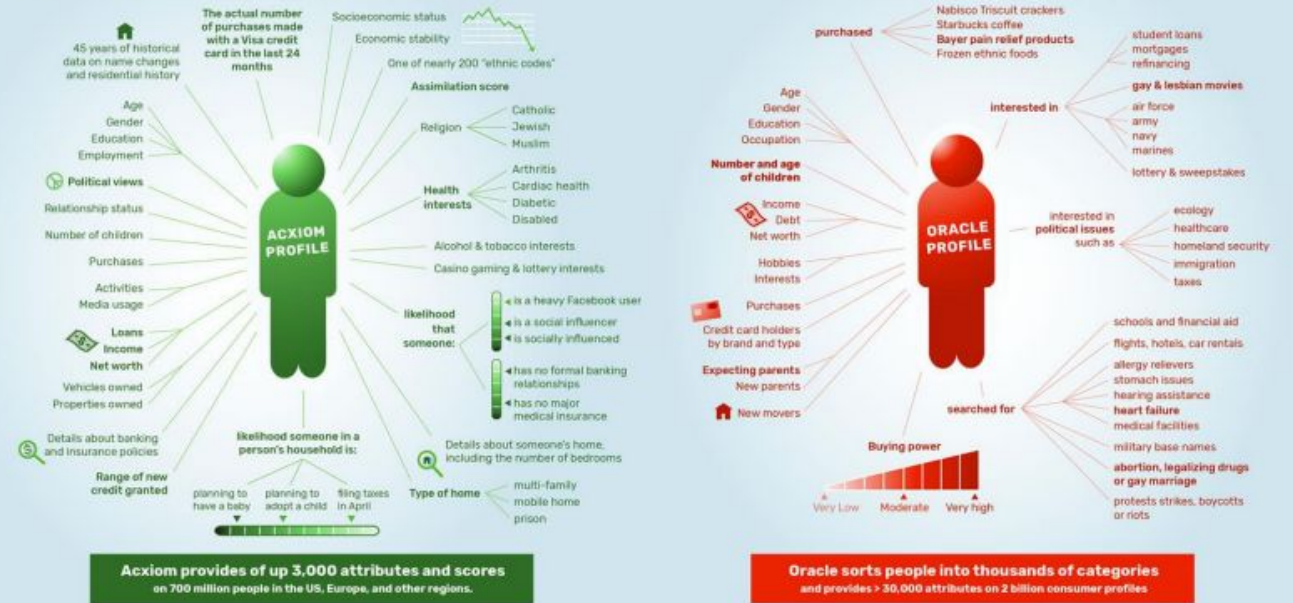
4 Source: "Identity Resolution & Criteo Shopper Graph", Criteo  
[https://criteo.investorroom.com/download/July+2019\\_Criteo-Shopper-Graph.pdf](https://criteo.investorroom.com/download/July+2019_Criteo-Shopper-Graph.pdf) [accessed November 29, 2019]



# 디지털 트윈(Adobe)

## DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Axiom and Oracle

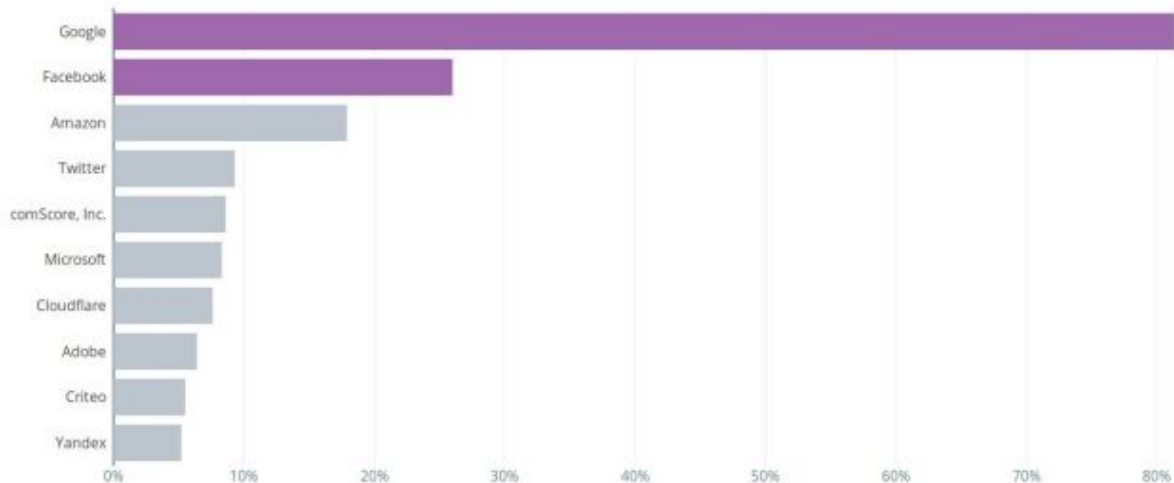


© Cracked Labs CC BY-SA 4.0. April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Axiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Axiom annual reports, developer website (API doc), Oracle press release, help center website, audience sizebook, taxonomy update for January, 2017 (Excel document). For details about the sources see the report "Corporate Surveillance in Everyday Life".

# 추적기 시장 점유율(Google, Facebook, Amazon 등)

## TRACKER MARKET SHARE

Proportion of the web traffic tracked by these companies.



“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)”

# 최대의 브로커 - Google과 Meta

“Google은 잘 알려진 소비자 브랜드임에도 불구하고 수입의 대부분을 차지하는 광고 제국의 세부 사항은 일반 사용자에게는 매우 불투명하고 전문가조차도 거의 이해하기 어렵다. Google은 다른 서비스의 데이터를 결합하여 광고주가 다양한 기준, 속성 및 특성에 따라 개별 소비자를 타겟팅할 수 있도록 한다.”

## 구글과 메타

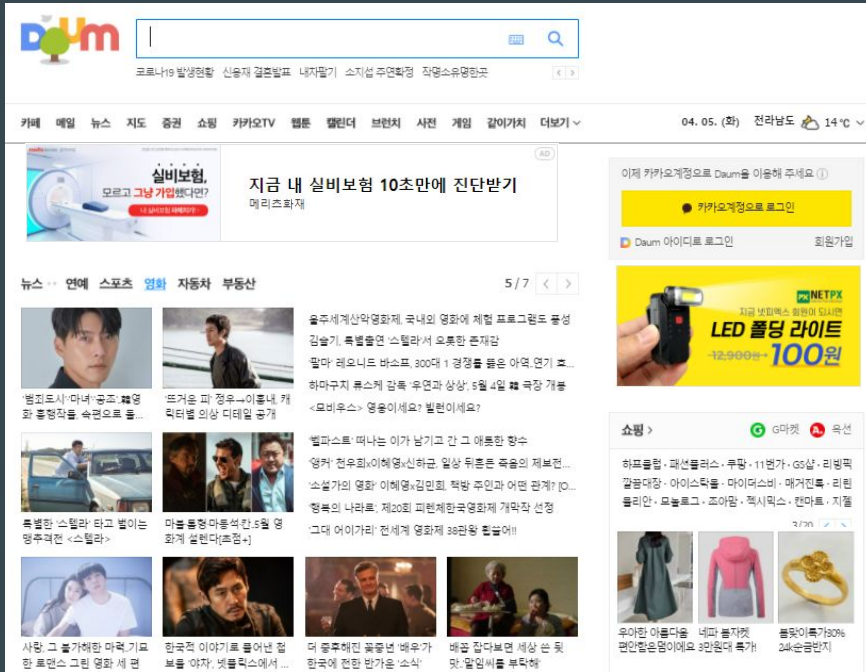
구글 “애드테크 산업에서 Google은 시장과 유통 시스템을 모두 소유하는 단일 기업” vs 메타 “Facebook은 많은 웹사이트 및 앱에서 사용자 데이터를 수집하여 이를 소셜 네트워크의 데이터와 결합하여 Facebook과 제3자는 Facebook 사용자에게 대한 상당한 추가 통찰력과 타겟팅 가능성을 얻을 수 있다.”

## 최대의 추적기

Google Play 스토어에서 사용할 수 있는 959,000개의 앱에 대한 연구(2018, Third Party Tracking in the Mobile Ecosystem”, Reuben Binns 등, <https://arxiv.org/abs/1804.03603>)

- DoubleClick, Admob 및 AdSense는 모든 앱의 88% 이상에 존재
  - Facebook은 42% 이상에 추적기를 통합

# 디스플레이 광고의 실시간 경매



1. 페이지 클릭 → 판매할 광고 슬롯 수 식별합니다.
2. 광고 공간을 판매하기 위한 '입찰 요청'을 컴파일합니다.
3. 이 입찰 요청을 컴파일하기 위해 웹사이트는 가능한 한 많은 정보를 수집합니다.
4. 여기에는 이전 방문의 개인 정보와 쿠키 및 브라우저로부터 구매한 기타 프로필 데이터와 같은 다른 출처에서 수집된 데이터가 포함되며, 사용자의 상세 프로필을 만듭니다.
5. 표준 입찰 요청에는 다음이 포함됩니다.
  - i. '고유한' 사용자 ID, ii. URL, iii. 생년, iv. 성별, v. 위치, vi. IP 주소, vii. 이미 수집 및 분석된 데이터에서 파생된 관심분야 또는 세그먼트, viii. 기존 프로필을 기반으로 추가로 추론된 데이터
6. 입찰 요청에 포함된 정보는 광고주를 위해 일하는 주요 측 플랫폼이 특정 광고를 표시할 수 있는 권리를 얻기 위해 경매에 입찰할지 여부와 입찰할 경우 입찰 금액을 결정하도록 사용됩니다.
7. 낙찰자는 귀하가 보고 있는 페이지에 광고를 게재하고 입찰 요청시 받은 데이터 사본을 보관하게 됩니다.

# 실시간 경매(RTB)시 공급측 플랫폼에 전달되는 데이터



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

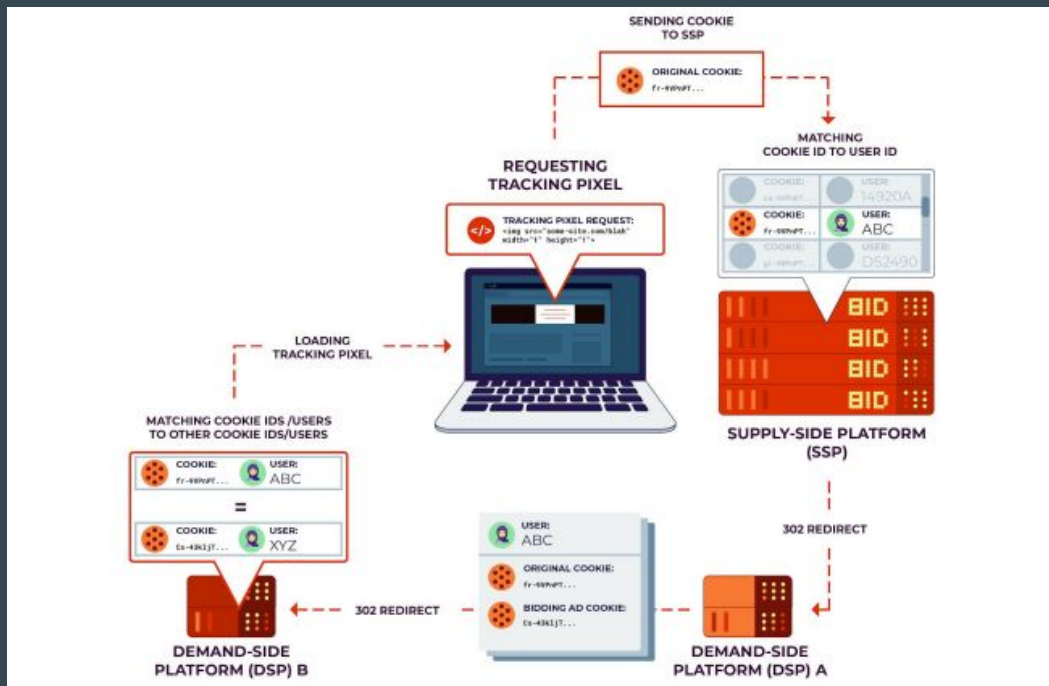
Source: <https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object--user>

# 광고 경매 승자(DSP)는 추가로 개인정보를 획득함



“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)”

# SSP에 의한 쿠키 동기화



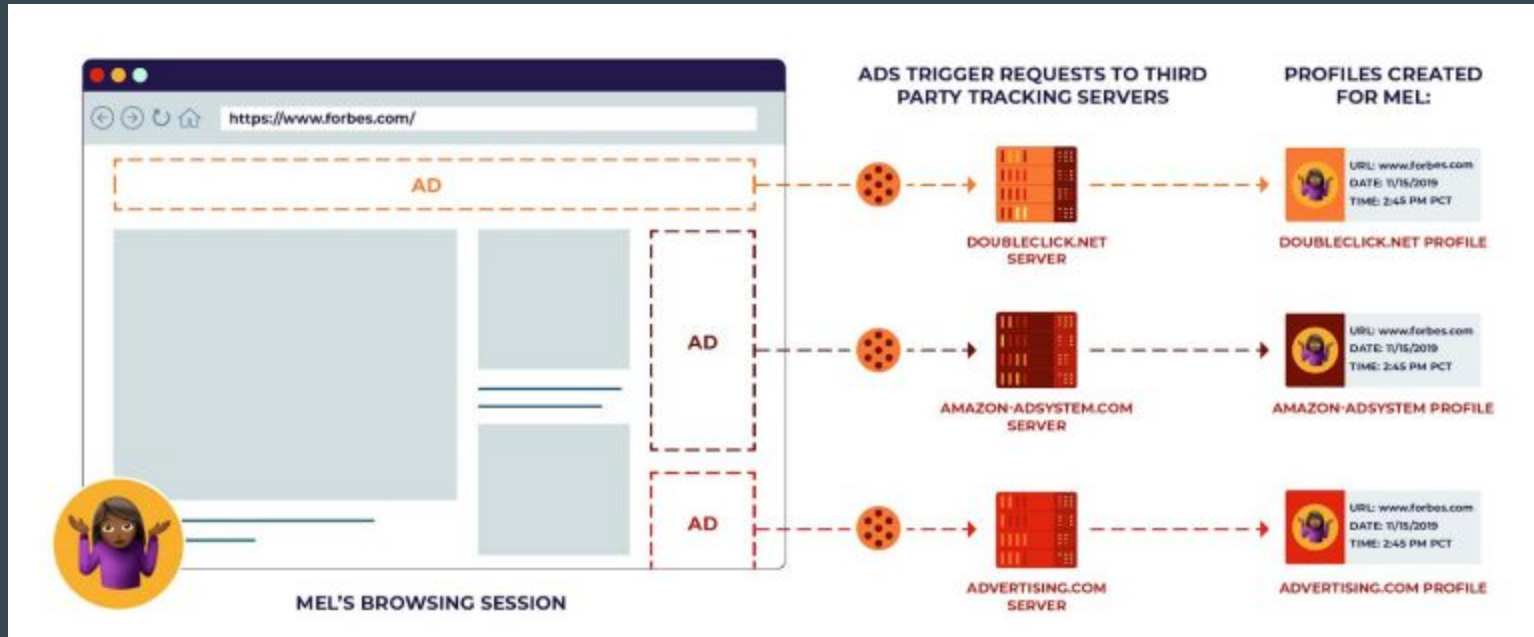
페이지의 보이지 않는 '픽셀'  
→ 광고 장터(ad exchange)/  
공급측 플랫폼(SSP)에 요청  
→ 사용자를 DSP로 리디렉션  
→ 리디렉션 URL에 SSP의  
쿠키에 대한 정보가 포함  
→ DSP가 자체 식별자에 연결할  
수 있도록 함.

SSP는 한 번에 여러 DSP에 대한  
쿠키 동기화를 유발

“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)”



# AD 네트워크는 추적기



“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance(EFF, 2019)”

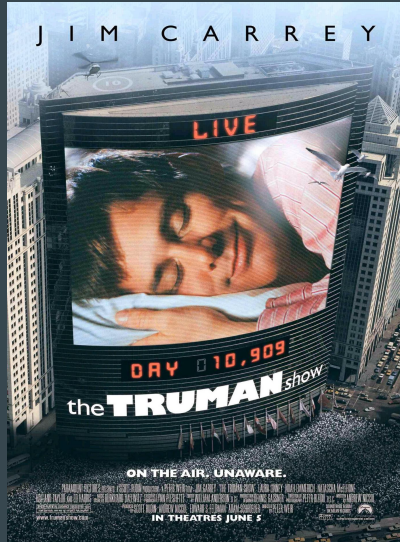


# 트루먼 쇼 (The Truman Show)(1988)



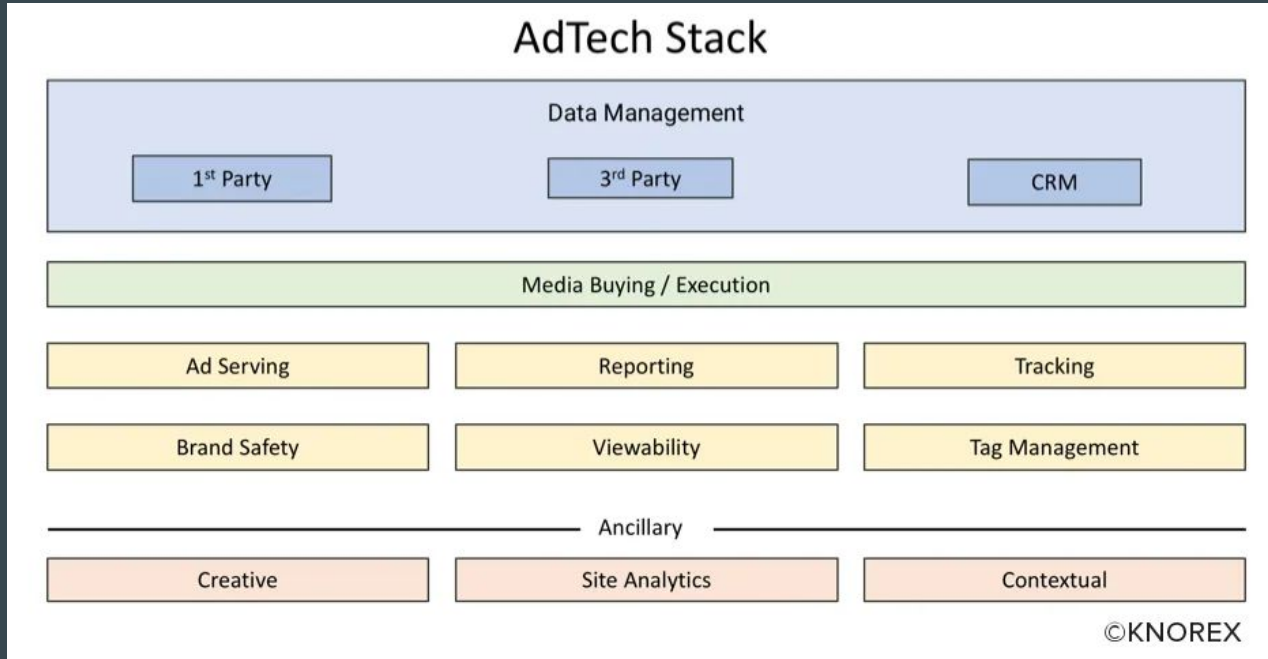
“우리는 누구나 보여지는 세상이 진실이라고 믿고 살기 마련이다.”

# “누구의 인생도 ‘RTB’라는 쇼로 방송중”



단방향 거울의 뒤편에서  
Behind the One-Way Mirror: A Deep Dive Into the  
Technology of Corporate Surveillance(EFF, 2019, 표지)

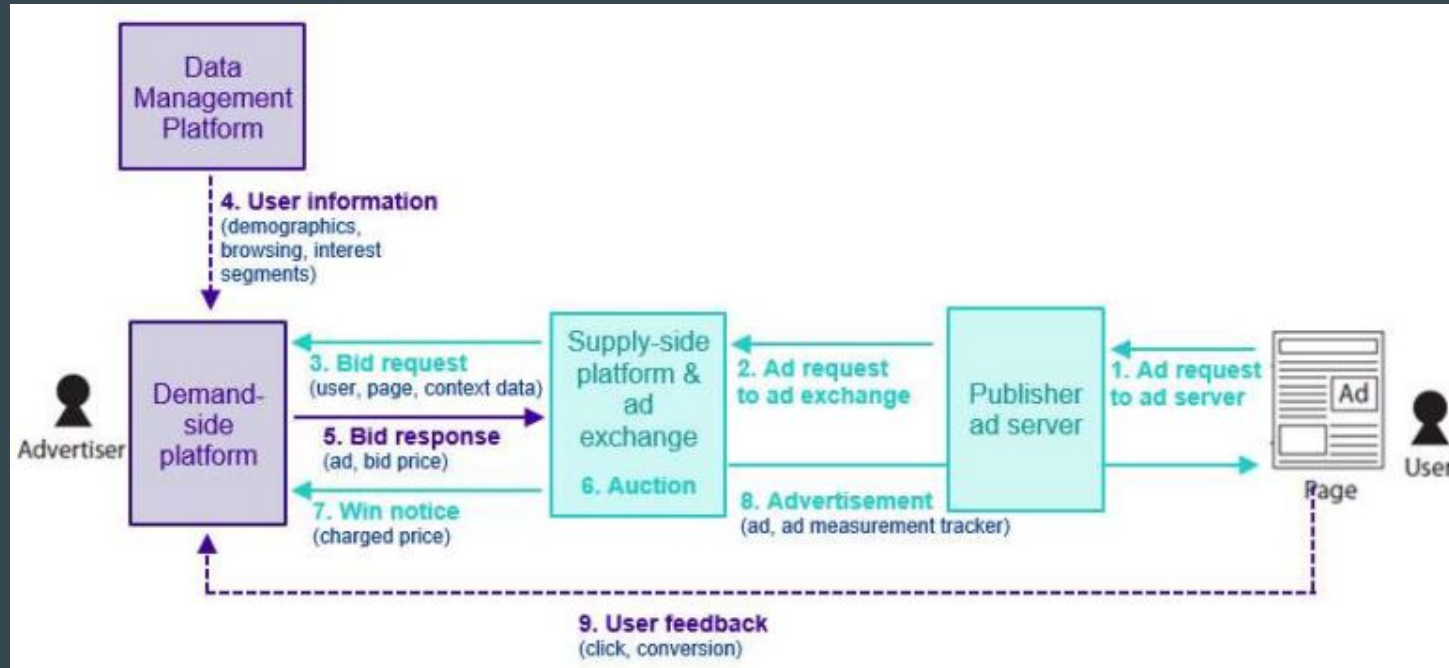
# 광고 기술 기업의 역할



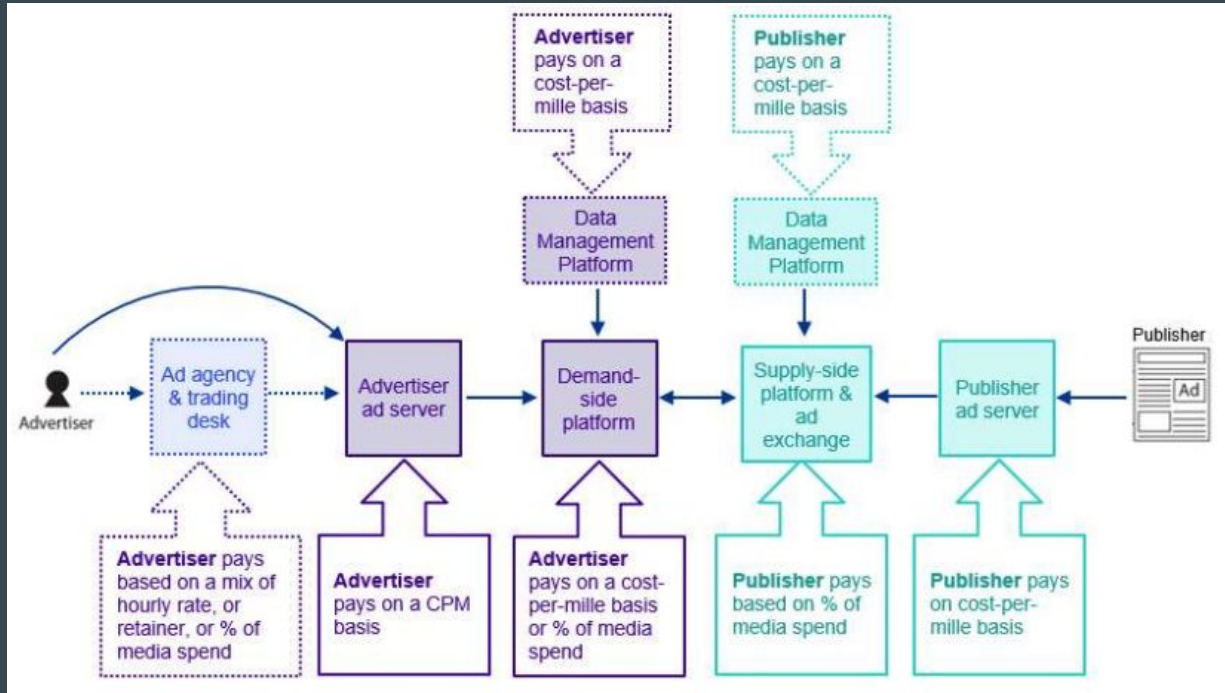
<https://www.knorex.com/blog/articles/select-demand-side-platform-adtech-stack>



# 광고 실시간 경매(RTB)시 ad tech 흐름

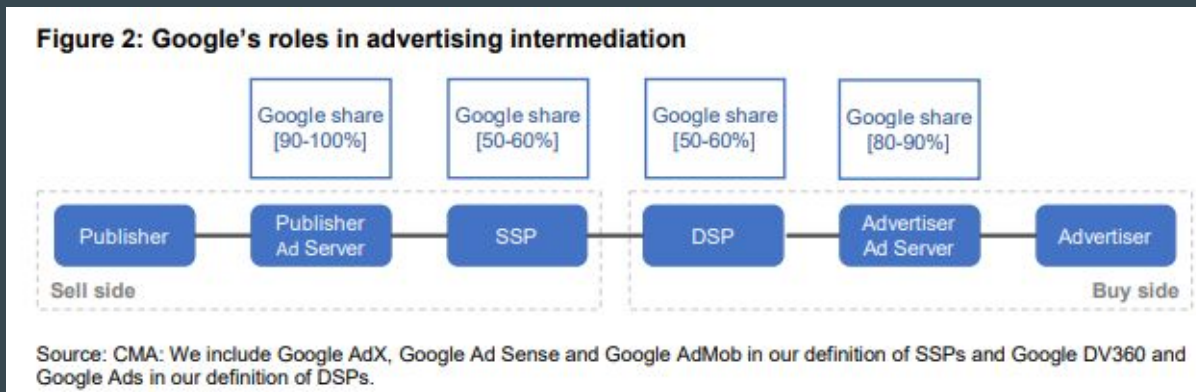


# 온라인 광고 관련 수수료의 지급 구조



Ad Tech Inquiry Issues Paper(ACCC, 2020)

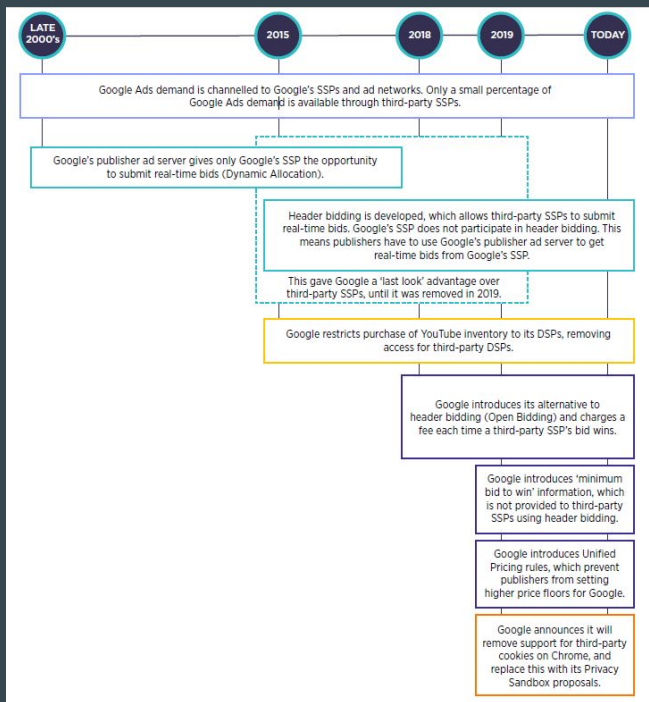
# Ad Tech에서 구글의 비중



Online platforms and digital advertising market study(2020, CMA)



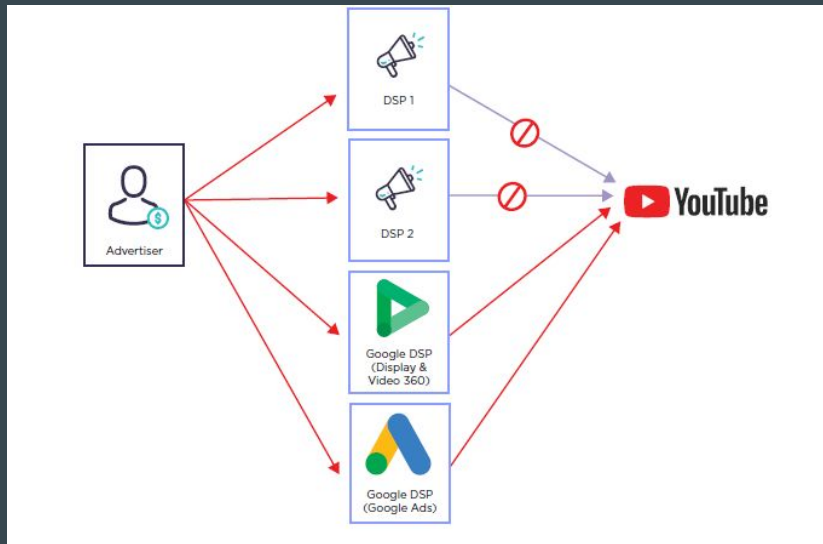
# Google의 불공정 행위(2000 ~ 2022)



Digital advertising services inquiry(2020, ACCC)

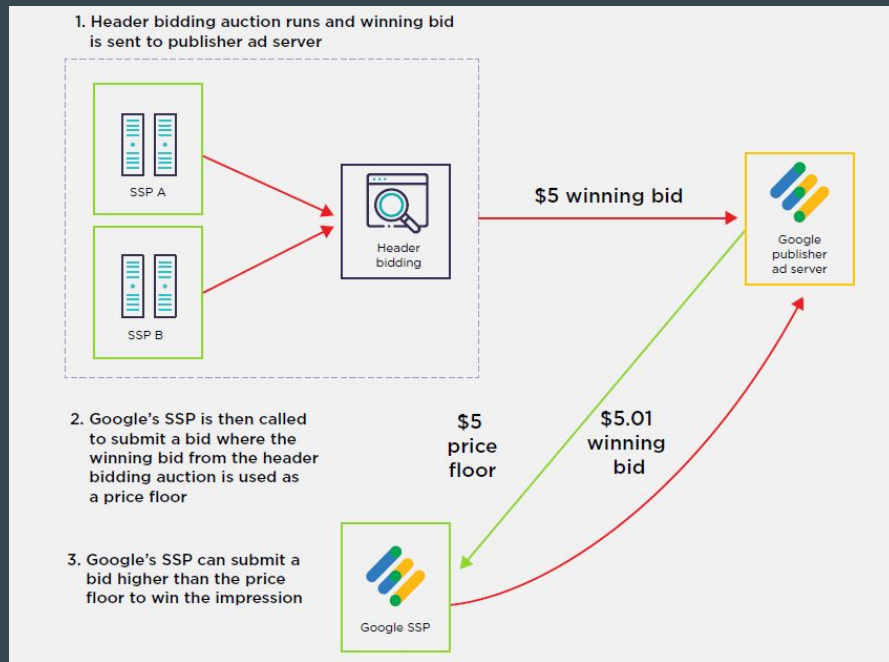


# Google의 광고 인벤토리는 자체 DSP로만 구매 가능



Digital advertising services inquiry(2020, ACCC)

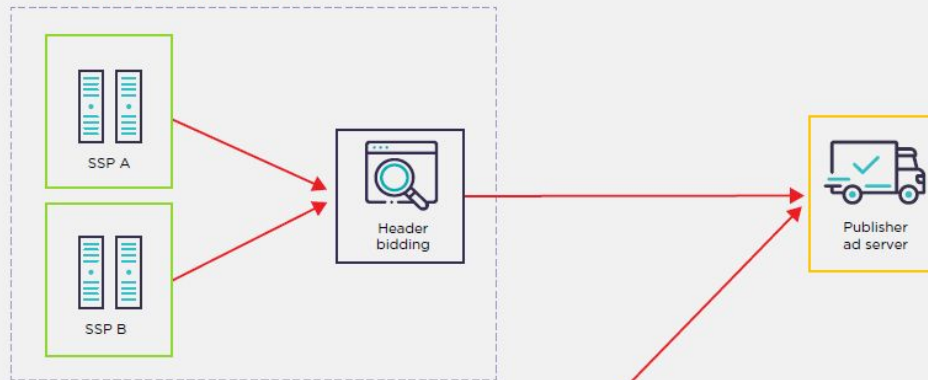
# Google SSP에게 유리한 대우 - 'last look'의 권한



Digital advertising services inquiry(2020, ACCC)

# 1차 낙찰가 결정 후 Google SSP

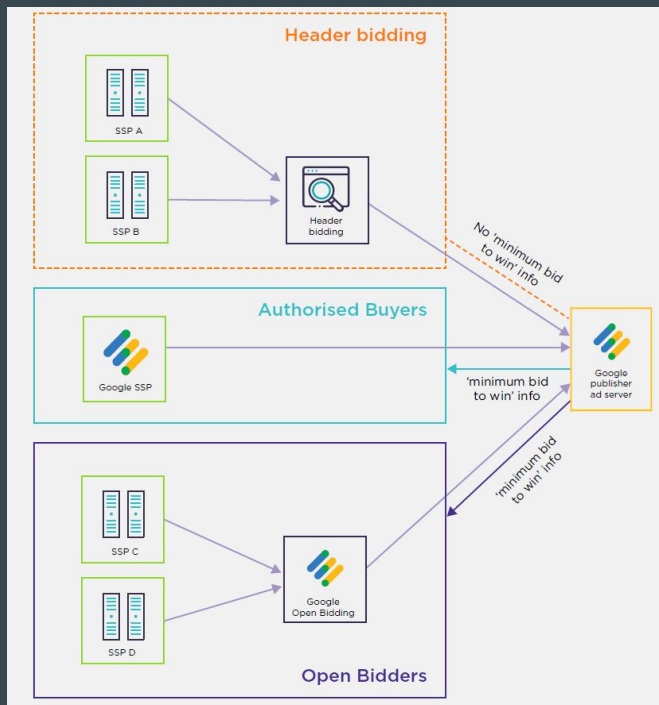
1. Header bidding auction runs and winning bid is sent to publisher ad server



2. Google's SSP is then called to submit a bid where the winning bid from the header bidding auction is used as a price floor

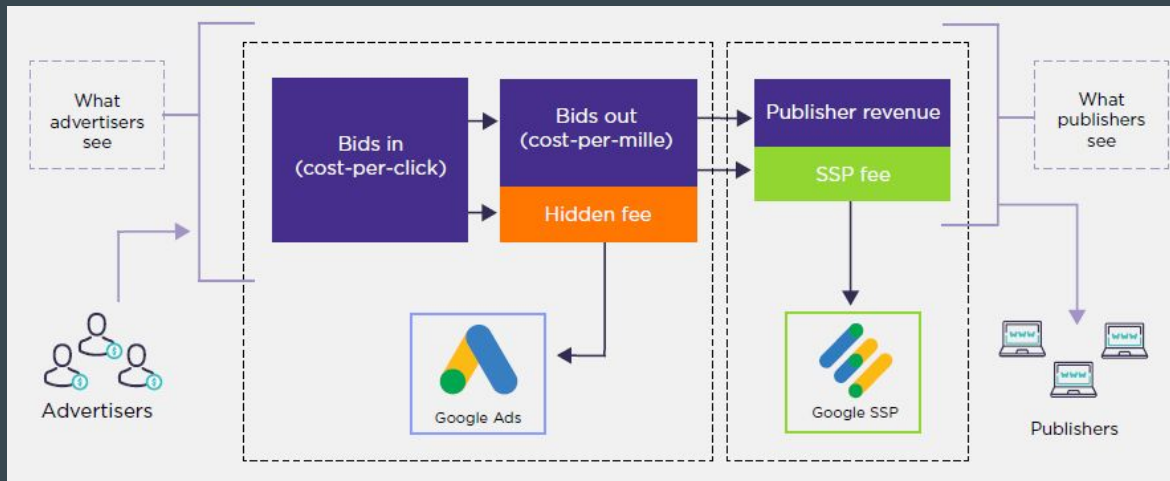


# minimum bid to win 정보는 Google SSP에게만 제공



Digital advertising services inquiry(2020, ACCC)

# 불투명한 광고 수수료



Google Ads는 클릭당, Google SSP는 노출당(100만)

Google이 양자의 비율 조정. 다른 당사자는 Google의 수익률을 알 수 없음

# 온라인 광고의 개인정보보호법(GDPR) 위반

2018

OpenRTB - Interactive Advertising Bureau의 실시간 입찰 방식과 Google의 Authorized Buyers RTB가 GDPR을 위반한다고 신고 <https://brave.com/adtech-data-breach-complaint/>

Privacy International 7개의 데이터 중개인 및 신용 조사 기관 GDPR 위반 신고 <https://privacyinternational.org/press-release/2424/press-release-privacyinternational-files-complaints-against-seven-companies>

프랑스 데이터 보호 기관인 CNIL(2018년 10월) - 프랑스 DSP Vectaury(6,700만 명 이상의 개인 데이터를 소유)가 개인 데이터를 처리하기 위한 유효한 법적 근거가 없다고 결정, - IAB 동의 프레임워크를 이용함.

2019

ICO(영국) - 애드테크 산업 내에서 GDPR 미준수의 문제가 있는 여러 사례를 요약한 보고서를 발표 <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-timebidding-report-201906.pdf>

# 온라인 광고의 개인정보보호법(GDPR) 위반

2020~2022

Grindr - GDPR 위반 제재

Google, Facebook - GDPR 위반 제재

Youtube - COPPA 위반 제재

Tiktok - COPPA 위반 제재

IAB - GDPR 위반 제재

감사합니다