Google의 FLoC 적용과 프라이버시 고려사항

이진규
네이버 주식회사
이사

이재림
네이버 주식회사
리더

Ⅰ. 들어가며

이 글에서는 Google이 맞춤형 온라인 광고 추천을 위해 Chrome 브라우저 API로 제공한 코호트 연합학습(Federated Learning of Cohorts; FLoC)의 개요와 배경, 프라이버시에 대한 함의를 살펴본다. FLoC은 이용자의 관심사 등 행태정보를 서버로 이전하지 않고 로컬 기기(여기서는 브라우저가 설치된 기기를 의미함)에서만 보유하고 이로써 모델을 훈련하는 방식으로 프라이버시를 보존하면서도, 로컬 기기에서 수행한 모델의 결과값을 광고 타게팅에 활용할 수 있는 ID로 변환함으로써 온라인 광고 생태계의 지속가능성도 보장하고자 한다. 즉, 프라이버시 보존 데이터분석(privacy-preserving data analysis)에 있어 비식별화의 대안으로 주목받고 있는 연합학습(federated learning) 기법을 응용하여 기존의 제3자 쿠키 등에 의한 웹 추적의 한계를 극복하고자 한 것으로 볼 수 있다.

FLoC은 Google의 Privacy Sandbox 이니셔티브의 일환으로 기획된 것이므로, 먼저 Privacy Sandbox의 전체적인 배경을 이해할 필요가 있다. Google은 2019년 8월, 공식 블로그에 <보다 사적인 웹(private web)의 구축>이라는 포스팅을 게시하고 웹에서의 프라이버시를 근본적으로 강화하기 위한 오픈 스탠다드(open standard) 개발 이니셔티브인 Privacy Sandbox를 공개했다.[1) 2)] 광고를 보다 연관성 있게 만드는 과정에서 당초 설계 의도와는 달리 프라이버시에 대한 이용자의 기대에 미치지 못하는 데이터 처리 행태가 만연하게 되었고, 이러한 상황에 대응하기 위해 여러 브라우저 제작사가 각기 다른 프라이버시 강화 조치를 적용하게 되었는데, 이러한 방식은 의도하지 않은 결과를 낳을 수 있다며 Google이 오픈 스탠다드 개발에 착수한 배경을 설명했다. 특히, ① 쿠키를 대규모로 차단하는 경우 '핑거프린팅(fingerprinting)' 등 불투명한 기술의 사용을 촉진하여 오히려 광고 생태계가 이용자들의 프라이버시를 침해하는 방향으로 나아갈 수 있고, ② 연관성 있는 광고를 제공할 수 있는 대안을 제공하지 않은 채 쿠키를 차단하는 경우 웹사이트 운영자의 주요 수익원을 심각하게 감소시킬 것이며, 이로 인해 '생기 있는 웹(vibrant web)'의 미래가 위험에 처할 수 있어 Privacy Sandbox 이니셔티브를 제안한 것이라는 설명도 덧붙였다. 전자는 이용자의 프라이버시 보호를, 후자는 온라인 광고 생태계의 지속가능성을 강조한 것으로 이해되는 대목이다.[3)]

이와 함께 Google은 <디지털 광고에서 사용되는 이용자 데이터에 대해 더 큰 투명성, 선택권, 통제권을 부여하기 위한 제안서 Version 1.0>도 공개했다.[4)] Google은 해당 제안서를 통해 "광고 산업계가 이용자의 프라이버시에 대한 기대를 충족하기 위한 조치를 탐색하는데 있어 투명성, 선택권, 통제권 등 세 가지 원칙에 기반해야 한다." 면서 ▲ 이용자에게 노출되는 광고를 통해 이용자에게 제공되어야 하는 정보의 종류와 전달 방식 ▲ 이용자 선택을 우회하는 시도 및 프라이버시 침해 행태(예: 핑거프린팅과 그에 따른 이용자 트래킹 등)의 예방 방식 ▲ 광고 정보에 대한 쉬운 접근 및 통제권 부여 방식 ▲ 광고 산업계와의 표준 설정 절차 착수를 위한 주요 논의 사항 등을 제안했다. 특히, 표준 설정과 관련한 산

1) Google, "Building a more private web", 2019. 8. 22., URL: https://www.blog.google/products/chrome/building-a-more-private-web/

2) 오픈 스탠다드(open standards)란 일반 대중에게 공개되고 협력 및 합의 중심의 절차를 통해 개발, 승인, 유지되는 표준을 의미한다. 보다 자세한 내용은 다음 국제전기통신연합(ITU) 웹페이지를 참조 - ITU, "Definition of Open Standards", URL: https://www.itu.int/en/ITU-T/ipr/Pages/open.aspx (최종 방문 2021. 4. 9.)

3) Google은 쿠키를 제거하여 온라인 광고가 이용자의 관심사에 보다 덜 연관성(less relevant) 있게 되는 경우, 웹사이트 운영자(publishers)에게 돌아가는 수익이 평균적으로 52%가 감소했다며 연관성 있는 광고 제공의 중요성을 강조하는 연구결과를 발표했다. Google은 Google Ad Manager의 광고 제공 시스템을 통해 임의로 선정한 소수의 이용자를 대상으로 A/B-test를 수행했는데, 그 결과 쿠키를 제외한 트래픽에서의 광고 수익이 52% 감소했으며, 개별 웹사이트 운영자의 수익 감소 중간 값(median)은 64%에 달했다고 밝혔다. 쿠키를 제거한 웹사이트에서 노출되는 광고는 컨텍스트 광고(contextual ads)와 같은 비개인화 광고라고 Google은 설명했지만, 구체적으로 얼마만큼 연관성 있는 비개인화 광고가 노출된 것인지, 광고 모델은 CPC(Cost-Per-Click) 방식으로만 제공된 것인지 등에 관한 자세한 정보는 공개하지 않아 Google의 연구 결과가 현실에서 얼마나 실효적인지 확인하는 것은 어렵다. 해당 연구결과는 다음을 참조할 수 있다. Deepak Ravichandran, Nitish Korula, "Effect of disabling third-party cookie on publisher revenue", 2019. 8. 27., URL: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf

4) Google, "Giving users more transparency, choice and control over how their data is used in digital advertising", 2019. 8., URL: https://services.google.com/fh/files/misc/industry_request_for_comment_v1.0.pdf

업계와의 논의에 대해 Google은 ① 수집 데이터를 이용자에게 제시하는 표준 ② 광고에 메타데이터(주: 여기에선 광고주, 광고 제공 절차에 관여한 기업명, 광고에 노출되는 이용자 선정 기준 등을 의미함)를 함께 제공하는 표준 ③ 광고 노출에 관여하는 기업을 노출하는 표준 ④ 광고 제공에 참여하는 기업을 등록할 수 있는 중앙집중적 등록체계(centralized registry) 마련 ⑤ 산업계 논의를 통해 달성한 표준을 우회하는 행태에 대한 이해의 공유 등 표준 설정 영역 및 지속가능한 규율을 위한 논의의 필요성을 제안했다.

Google은 현재 Privacy Sandbox 이니셔티브를 크게 세개의 명확히 구분되는 트랙으로 나누어 그 가능성을 탐색하고 있다. 첫째, 크로스 사이트 추적(cross-site tracking)에 의해 제공되는 기능을 대체하는 것, 둘째, 웹 추적의 주요 방식인 제3자 쿠키를 제거하는 것, 셋째, 표준 우회 가능성에 대응하는 것 등이 바로 그것이다.[5] 특히, 첫 번째 트랙의 실제 적용 사례로서 '광고 타게팅' 하위 영역인 '관심기반 광고' 제공 방식으로 Google은 FLoC을 제시한 것이다. Privacy Sandbox 이니셔티브를 통해 제시된 매우 다양한 가능성 가운데 FLoC이 가장 주목받는 배경에는 여러 이유가 있으나, 제3자 쿠키를 제거하여 웹에서의 추적을 제한하겠다는 선언을 한 여러 브라우저들 가운데 가장 많은 이용자를 보유하고 있다는 점, 기존의 광고 효과성을 유지하면서도 프라이버시를 보호할 수 있다는 기대, 기존의 문제점을 해결하는 대신 새로운 문제점을 양산할 것이라는 비판, 기존에 Google이 누려왔던 온라인 광고 생태계에서의 독점적 지위를 더욱 강화할 것이라는 우려 등이 종합적으로 작용한 것으로 이해된다. 즉, 기대와 우려가 섞인 관심을 받고 있는 것이다. 이 글은 FLoC의 작동 방식, 프라이버시 보호에 대한 기대, FLoC에 제시되는 우려, 그리고 해당 이슈가 제시하는 시사점 등을 살펴본다.

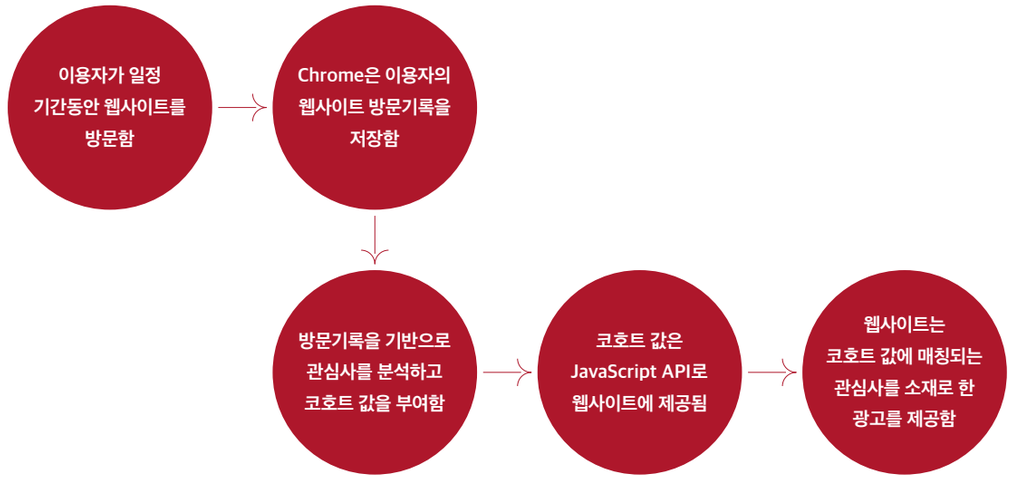
5) Google, "The Privacy Sandbox", URL: https://www.chromium.org/Home/chromium-privacy/privacy-sandbox (최종방문 2021. 4. 4.)

Ⅱ. FLoC의 작동 방식

1. FLoC 코호트의 개념

통계학에서 주로 사용되는 용어인 코호트(cohort)는 '공통적인 특성을 가진 사람들의 집단'을 의미한다. 우리나라는 지난 2015년 메르스(MERS-CoV, Meddle East Respiratory Syndrome) 유행 때, 전국에서 10여개의 병원이 14일간 '코호트 격리'되는 경험을 겪으면서 코호트라는 표현을 일상에서 사용하는 것이 더 이상 낯설지 않다. 온라인(모바일) 마케팅 영역에서 코호트는 공통의 식별자(common identifier)를 사용하여 그룹으로 묶을 수 있는 이용자들의 집단을 의미한다. 공통성(commonality)이 존재한다면 어떤 정보라도 코호트 생성에 기여할 수 있다. 예를 들어, 특정한 기한 내에 동일한 지역에서 특정 앱을 설치한 이용자들을 코호트로 그룹화 하는 것도 가능하다.[6]

'FLoC 코호트'는 이용자의 웹 브라우징 히스토리를 기반으로 브라우저가 추론(derivation) 과정을 거쳐 형성한다. 이는 이용자들의 브라우징 행태를 기반으로 추론한 공통의 관심사를 기반으로 수천명의 사람들을 '공통의 식별자'로 묶어낸 것이다. 즉, 하나의 코호트에는 공통의 관심사를 공유하는 매우 많은 수의 사람들(정확하게는 그 사람들이 이용한 '브라우저')이 포함된다. 브라우저는 이용자가 웹을 이용하는 여정을 일정한 시간에 걸쳐 기록하고, 이를 기반으로 코호트를 업데이트한다. 이러한 FLoC 코호트는 관심사별로 코호트 값(예: "#1975", 이하 "코호트 ID")을 부여받으며, 브라우저는 JavaScript API를 통해 코호트 ID를 웹사이트에 제공한다. 코호트 ID가 생성되는 절차 및 Chrome 브라우저가 이를 웹사이트에 제공하는 절차는 아래 그림 1.과 같다.



[그림 1] FLoC 코호트 생성 및 코호트 ID의 제공 절차

브라우저는 특정 시점에 오직 하나의 코호트 ID를 부여받는다. 단, 브라우저가 단 하나의 코호트 ID를 부여받는다고 하여, 해당 브라우저가 오직 한 개의 관심사를 반영하는 것은 아니다. 예를 들어, 특정한 코호트 ID는 '여행과 사진 촬영'이라고 하는 두 개의 관심사를 동시에 반영한 것일 수 있다. 이와 같은 FLoC 코호트는 매 7일마다 업데이트 된다. 이런 의미에서 FLoC 코호트는 동적(dynamic)이라고 평가할 수 있다. 이용자의 웹 브라우징 행태가 변함에 따라 이에 기반하여 추론한 관심사도 변화한다. 결국 코호트 ID는 변화한 관심사를 반영하여 새로운 값으로 바뀐다.[7]

2. 브라우저가 코호트 ID를 부여받는 방식

브라우저는 코호트 ID를 다음과 같은 방식으로 배정받게 된다. FLoC은 오픈소스에 기반하여 개발되기 때문에 어느 브라우저나 이를 적용할 수 있지만, 편의상 Chrome 브라우저에 한정하여 설명한다.[8]

6) Adjust, "Cohorts: The Adjust Mobile Measurement Glossary", URL: https://www.adjust.com/glossary/cohort/ (최종방문 2020. 4. 1.)

7) Google, "Federated Learning of Cohorts", URL: https://www.privacysandbox.com/ (최종방문 2021. 4. 5.)

8) Sam Dutton, "What is Federated Learning of Cohorts", 2021. 3. 31., URL: https://web.dev/floc/#floc-algorithm

① Chrome 브라우저가 사용하는 'FLoC 서비스'는 모든 가능한 웹 브라우징 히스토리를 '다차원의 수학적 표현(multi-dimensional mathematical representation)'으로 변환하여 생성한다. Google은 이를 "코호트 공간(cohort space)"이라 부른다(아래 그림 2. 참조).[9)]

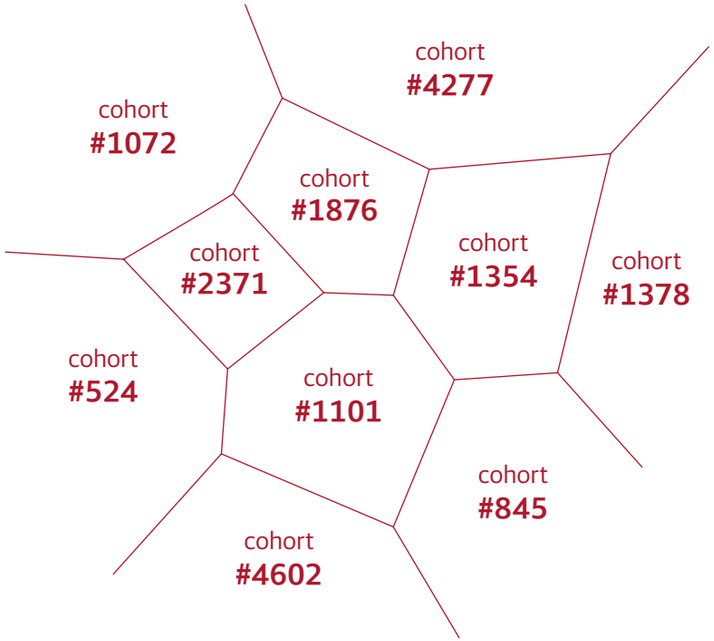
② FLoC 서비스는 이 코호트 공간을 수천개의 세그먼트(영역)로 분할한다. 개별 세그먼트는 '유사한 브라우징 히스토리'를 공유하는 수천명의 사람(정확히는 수천개의 브라우저)으로 구성된 하나의 클러스터를 의미한다. 개별 세그먼트가 나뉘는 방식은 실제 브라우징 히스토리를 분석하는 방식 아니라, 코호트 공간에 임의로 세그먼트 중심을 배치하거나 무작위의 선을 이용하여 코호트 공간을 나누는 방식이다.

③ 이렇게 나뉜 개별 세그먼트는 코호트 ID를 배정받는다.

④ Chrome 브라우저는 FLoC 서비스로부터 코호트 공간을 묘사하는 데이터를 제공받는다.

⑤ 이후, 이용자가 웹을 탐색하면, Chrome 브라우저는 이용자의 웹 브라우징 히스토리에 가장 가깝게 대응되는 코호트 공간의 영역(즉, 어느 코호트 ID를 배정받아야 하는지)을 주기적으로 계산하는 알고리즘을 이용하여 코호트 ID를 브라우저에 부여한다.

9)
'FLoC 서비스'가 정확하게 무엇을 의미하는지는 분명하지 않으나, 맥락상 웹 브라우저가 코호트 ID를 형성할 수 있도록 하는 모델(알고리즘)을 제공하는 주체를 의미하는 것으로 이해된다. 통상적으로 웹 브라우저를 제공하는 주체가 FLoC 서비스가 될 수 있을 것이나, 양자가 반드시 일치하는 것은 아닐 수도 있다. 예를 들면 Chrome 브라우저의 경우 Google이 FLoC 서비스가 될 것이다. 그런데, Chrome이 아닌 다른 브라우저(예: Microsoft Edge 브라우저)가 FLoC API를 지원하지만, 해당 브라우저가 FLoC 코호트를 형성하도록 하는 역할을 Google에 맡기는 경우라면 브라우저 제공 주체(Microsoft)와 FLoC 서비스(Google)가 일치하지 않게 된다.

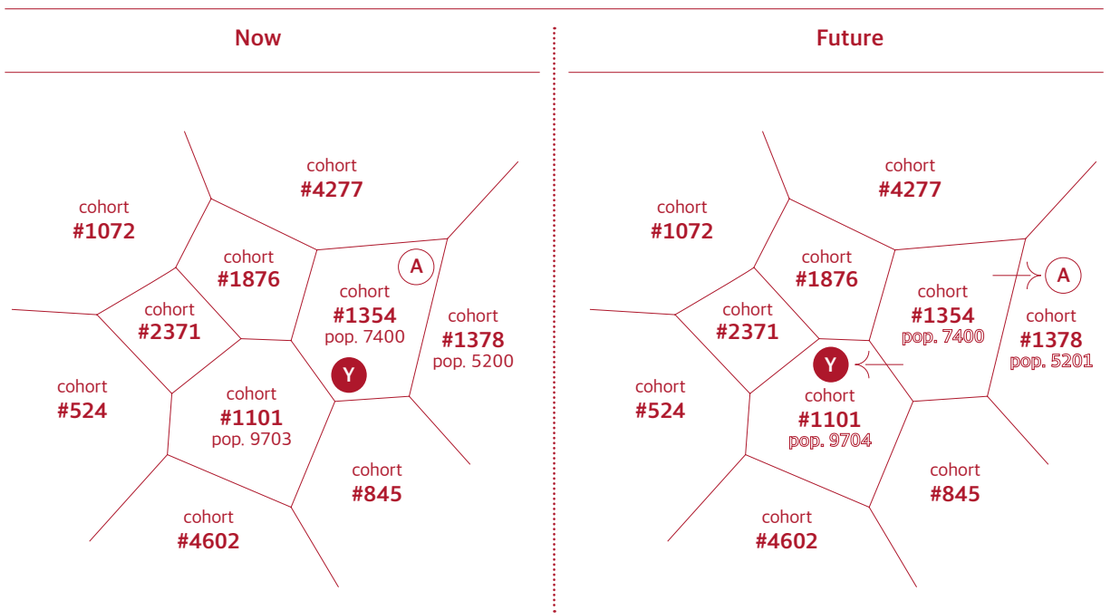


[그림 2] FLoC 서비스가 코호트 공간을 관심사에 매칭하는 세그먼트로 분할한 화면 (출처: Google)

상기 그림 2.에서 보는 바와 같이 각 코호트 세그먼트의 크기는 다르다. 이것은 특정한 코호트 ID에 배정되는 사람들의 수(정확히는 브라우저의 수)가 다르다는 것을 의미한다. 특정 코호트 ID에는 최소 수천명의 사람(브라우저)이 배정되는데, 이는 이용자를 "군중에 숨기기(hide in a crowd)" 위함이다. 이러한 의미에서 최소한 k 명의 이용자가 공통으로 배정받는 코호트 ID는 k-익명성을 보장한다고 설명할 수 있다. 숫자 k가 높을수록 해당 코호트는 프라이버시를 더 높은 수준으로 보존할 수 있다.

FLoC 코호트 값은 7일 간격으로 다시 산정된다(아래 그림 3. 참조). 따라서, 특정한 주에 동일한 코호트 값(#1354)을 부여받은 2명의 이용자(브라우저)는 그 다음주에 각기 다른 코호트 값(#1354 → #1101, #1378)을 부여받을 수 있다. 기존과 다른 코호트 값을 배정받는 이유는 브라우징 행위를 통해 확인되는 이용자의 관심사가 그 전 7일의 관심사와 달라졌기 때문이거나, FLoC 서비스가 코호트 공간을 묘사하는 데이터에 변화를 주었기 때문일 수 있다. 특히, 후자는 FLoC 코호트 값을 더욱 세분화하거나, 특정한 FLoC 코호트 값에 대응되는 이용자의 관심사가 공개되어 FLoC 코호트 값을 변경해야 하는 사정 등에 기인할 수 있을 것으로 생각된다.

10)
그림 3.의 Alex(A)와 Yoshi(Y)는 각기 공통의 관심사(코호트 ID #1354)를 가지고 있었으나, 7일간 각자의 브라우징 활동으로 인해 관심사가 나뉘어서 각기 다른 코호트 ID(이 경우 Alex는 #1378, Yoshi는 #1101)를 배정받은 것을 보여준다. 여기에서 "pop."는 population, 즉 해당 코호트에 배정받은 사람의 수(정확하게는 브라우저의 수)를 의미한다.



[그림 3] 코호트 ID를 배정 7일 후, 새로운 코호트 ID를 배정받는 과정 (출처: Google)[10)]

3. FLoC 작동 방식

FLoC는 다음과 같은 방식으로 작동한다. 여러 주체가 관여하기 때문에, 각 주체에 대한 설명을 우선 제시한다.

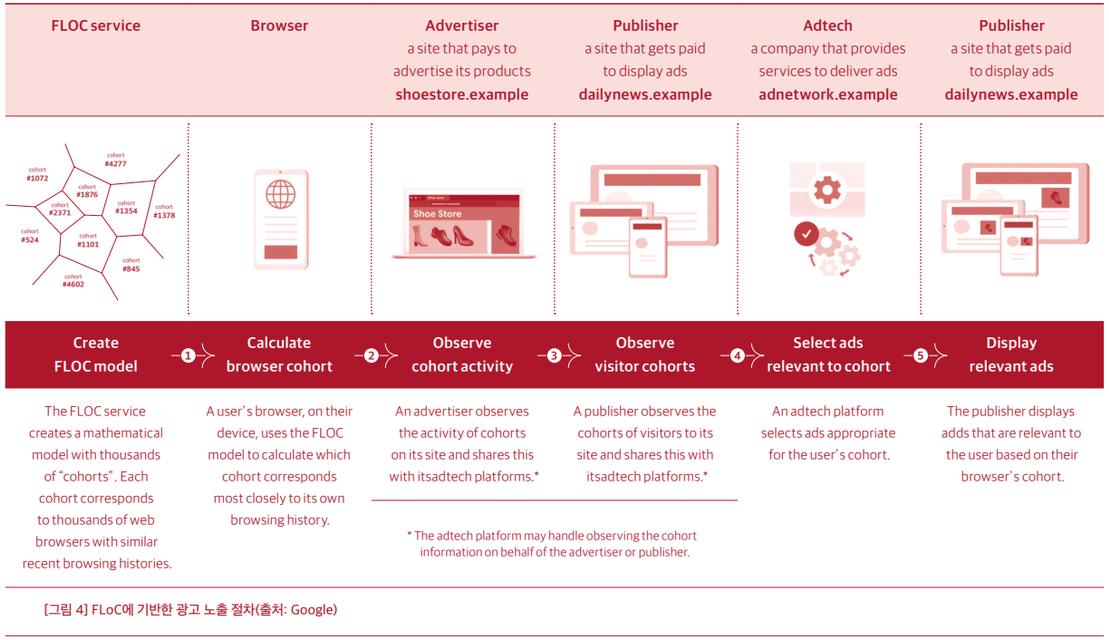
관여 주체	역할
FLoC 서비스	수 천개의 코호트를 담고 있는 수학 모델(FLoC model)을 생성함 (개별 코호트는 유사한 브라우징 히스토리를 기록한 웹 브라우저에 대응됨)
브라우저	FLoC 모델을 이용하여 브라우저의 FLoC 코호트 ID를 계산함
광고주 (advertiser)	광고를 발주하는 웹사이트. 웹사이트를 방문한 이용자(브라우저)의 코호트 ID와, 이용자가 관심을 보인 콘텐츠를 매칭하여 광고 플랫폼에 전송함 예: #1975 - 등산화
광고 웹사이트 (publisher)	광고주의 광고를 노출하는 웹사이트. 방문한 이용자(브라우저)의 코호트 ID를광고 플랫폼에 전송함 예: #1975
광고 플랫폼 (adtech)	A. 광고주로부터 코호트 ID와 관심사가 매치된 정보(예: #1975 - 등산화)를 제공받아 저장하고 있다가, B. 광고 웹사이트로부터 방문 이용자의 코호트 값(#1975)를 제공받아 이것을 조합(A+B)하여 방문객의 관심사에 연관성 있는(relevant) 광고(여기에선 등산화)를 광고 웹사이트에 노출함

[표 1] FLoC 작동에 관여하는 주체 및 역할

이용자의 브라우저는 '모든 이용자의 브라우징 활동을 상징하는 다차원 공간을 생성하는 수학 모델에관한 데이터'를 FLoC 서비스로부터 제공받는다. 즉, FLoC 서비스는 브라우저에 모든 생성가능한 코호트 세그먼트를 생성할 수 있는 데이터를 브라우저에 전달한다. 브라우저는 코호트 공간의 어느 영역이 최근의 브라우징 행태에 가장 유사하게 매치되는지를 수학 모델(FLoC model)의 알고리즘을 사용하여 계산한다. 이러한 과정을 통해 브라우저는 이용자의 웹 브라우징 행태에서 추론되는 관심사에 매칭되는 FLoC 코호트 ID를 배정받게 된다. 이 과정은 매 7일마다 반박되며, 업데이트된 코호트 값이 새롭게 브라우저에 부여된다.

특정한 코호트 값(예: #1975)를 배정받은 이용자(브라우저)가 아웃도어 사이트(광고주 M)를 방문하여 등산화 구매에 관심을 보였다면, 광고주 M은 코호트 값과 관심사(#1975 – 등산화)를 매칭하여 저장한다. 그리고, 이 정보를 광고 플랫폼 A에 전송한다. 해당 이용자가 다른 웹사이트(예: 뉴스 사이트 P)에 방문을 했는데, 마침 뉴스 사이트 P가 광고 플랫폼 A와 광고계약을 맺은 경우라고 가정해본다. 해당 뉴스 사이트 P는 방문한 이용자의 코호트 값을 광고 플랫폼 A에 전송한다. 광고 플랫폼 A는 기존에 광고주 M으로부터 해당 코호트가 등산화에 관심을 보였던 기록을 전송받아 보유하고 있었기 때문에, 뉴스 사이트 P의 광고 영역에 광고주 M의 등산화 광고를 노출한다. 이와 같은 방식을 통해 광고주 M, 광고 플랫폼 A, 뉴스 사이트 P는 해당 이용자가 누구인지 알지 못하며, 그를 식별하거나 추적(cross-site tracking)하지 않고서도 그의 관심사에 연관성 있는 광고를 노출할 수 있게 된다.

이상의 과정을 정리한 그림은 아래와 같다(그림 4.)



[그림 4] FLoC에 기반한 광고 노출 절차(출처: Google)

Ⅲ. FLoC에 제시되는 프라이버시 보호에 대한 기대와 우려

1. 프라이버시 보호에 대한 기대

FLoC에 제시되는 기대는 한마디로 "이용자에 대한 프라이버시를 보호하면서도 연관성 있는 광고를 이용자에게 제공할 수 있다"는 것으로 요약할 수 있다. 다수 온라인 사업자들은 자사 사이트에 방문 트래픽을 발생시키기 위해 광고에 의존한다. 그리고, 웹 사이트들은 광고 영역(advertising inventory)을 판매하여 웹 사이트에 게시하는 콘텐츠를 지원한다. 광고가 보다 '연관성 있는' 경우, 광고를 노출하는 웹사이트에 더 많은 수익이 발생하며, 이를 통해 더 좋은 콘텐츠를 지원할 수 있으며, 더 많은 이용자를 유치할 수 있게 된다. 일련의 선순환 구조가 발생하는 것이다. 기존에 이와 같이 '연관성 있는' 광고를 제공하기 위해 가장 널리 사용되었던 방식은 제3자 쿠키(3rd party cookie)에 의존하는 방식이었다. 제3자 쿠키는 이용자가 방문한 웹사이트가 아닌 다른 웹사이트에 의해 생성된, 이용자의 브라우저 내에 저장된 일종의 '트래킹 정보'다. 이용자가 A라는 사이트를 방문했으나, 실제 해당 웹사이트에는 A가 아닌 다른 주체(Z)가 존재할 수 있는데, 이 경우 Z가 이용자의 브라우저에 A사이트를 방문한 기록을 저장해 놓는 경우 해당 정보는 제3자 쿠키에 해당한다. 만약 Z가 A~Y 등 여러 사이트에 방문한 특정 브라우저를 대상으로 모두 제3자 쿠키를 저장한다면, Z는 이용자가 A~Y 사이트

를 방문한 기록을 추적(tracking)할 수 있는 것이다. 이러한 제3자 쿠키는 이용자 추적을 가능하게 하여 그의 관심사를 지속적으로 분석하고, 연관성 있는 광고를 노출할 수 있게 하는 기반을 제공하였다.

그런데, 제3자 쿠키는 프라이버시 측면에서 매우 복잡한 문제점을 야기한다. 우선 이용자는 자신이 방문한 웹사이트에 얼마나 많은 '숨겨진 주체'들이 제3자 쿠키를 설치하고, 자신의 웹 브라우징 활동을 추적하는지 알 수 없다. 브라우저의 설정 메뉴를 통해 쿠키가 브라우저에 저장되는 것을 차단할 수 있으나, 대다수 이용자들은 이와 같은 설정이 존재하는 사실조차 잘 모른다. 또한, 쿠키 저장을 전면적으로 차단하는 경우 반드시 필요한 기능도 제한되기 때문에 이용자의 웹 경험 품질이 낮아지게 되는 문제도 있다.

이러한 측면에서 FLoC는 이용자의 웹 이용 경험(UX)을 저하시키지 않고, 여러 사이트에 걸쳐 이용자의 활동을 추적하고 그 결과를 중앙 서버(centralized server)에 전송하여 외부에서 알 수 없는 방식으로 분석 및 활용하는 것을 더 이상 지원하지 않는다. 이용자의 브라우징 활동은 브라우저 내에서만 모델에 의해 분석되고, 그 결과는 코호트 ID로 변환되어 웹사이트에 제공된다. 웹사이트는 특정한 이용자(브라우저)에게 부여된 코호트 ID를 광고 사업자에게 전송하여, 해당 코호트 ID에 매칭되는 연관성 있는 광고를 노출할 뿐 코호트 ID를 통해 방문자의 관심사를 직접적으로 확인하거나 할 수 없다. 이러한 방식으로 이용자의 프라이버시는 보호되고, 광고 연관성은 매우 높은 수준에서 제3자 쿠키에 기반한 타게팅 광고의 동등한 수준으로 보장된다. FLoC은 제3자 쿠키를 제거하면서 여전히 광고의 연관성을 보장하는 '대안'으로서의 기대와 제3자 쿠키를 통해 중앙의 웹 서버에 전송되었던 정보를 이용자 기기(로컬)에서 처리하도록 하여 이용자 프라이버시 보호를 강화할 수 있다는 기대를 받고 있다. 이와 같은 기대에 대해 한 매체는 "No more individual tracking, no sacrifice"라고 표현하여 개인에 대한 추적 및 광고 효과의 희생을 더 이상 경험하지 않아도 된다는 점을 나타냈다.[11)]

2. 프라이버시 측면에서의 우려

(1) 감시 자본주의(surveillance capitalism)의 지속

Google이 Privacy Sandbox 이니셔티브를 발표한 '19년 8월, 전자프런티어재단(EFF, Electronic Frontier Foundation)은 해당 이니셔티브에 포함된 여러 기술적 제안을 평가했는데, 캡챠(CAPTCHA)와 핑거프린팅 대응 제안은 잘한 것(the good)으로, 전환 측정(conversion measurement)은 나쁜 것(the bad)으로, FLoC은 추한 것(the ugly)으로 평가를 했다. EFF는 FLoC 코호트 ID가 실질적인 '행태 신용 점수(behavioral credit score)'로 작용할 것이라고 언급하면서, 이를 기존의 이용자 프로파일 정보와 결합하는 경우 트래킹을 수행하는 주체는 이용자에 관한 민감한 정보를 접할 수도 있다며 우려를 표했다. 특히, Google은 브라우저로 하여금 '민감한' 정보를 추출하지 않게 하는 절차를 적용할 것이라 하였으나, "어떤 데이터가 민감한 것인지는 사람마다 다르다."라는 측면에서 프라이버시에 대한 '누구에게나 동일한' 접근법은 많은 이용자를 위험에 처하게 할 수 있다는 점을 지적했다.[12)]

Google은 FLoC을 소비자 프라이버시를 위한 매우 중요한 발전이라 마케팅하지만, 실제 이는 '프라이버시 극장(privacy theater)'에 다름없다고 평가를 받기도 한다.[13)] 즉, 감시 기반의 행태 광고에 기반하여 쌓아 올려진 산업의 다이내믹스를 바꾸는데 있어 Google이 전혀 관심이 없다는 것이다. 정보주체는 개인으로서 추적당하는 것을 피할 수는 있을지는 몰라도 사람들의 행태를 관찰하고, 그 결과를 이용하여 광고를 제공하는 것에 기반한 경제 체계 속에 살아가야 한다는 것은 기존과 변화가 없다는 것을 의미한다. 결국 정보주체는 이와 같은 감시 자본주의의 톱니 사이에서 살아갈 수밖에 없다는 지적이다.[14)]

FLoC은 결국 이용자에 대한 '타게팅'을 지속할 수 있는 수단이 되는 것인데, 이는 사람의 행동을 추적하는 것에 기반하여 획득할 수 있는 데이터를 기반으로 한다. 즉 사람은 광고를 타게팅하는데 필요한 데이터를 생산해내는 객체가 되는데, "If you are not paying, you are the product(당신이 제품에 돈을 지불하지 않는다면, 당신이 제품이라는 의미이다)"라는 표현이 상기될 수밖에 없는 지점이다. Google이 제3자 쿠키를 제거하면서 개인을 타게팅 하지 않는 맥락 광고(contextual ads)를 활성화하지 않는 것은 감시 자본주의 체제를 버리지 않겠다는 선언과 다름없다 할 수 있다. 한 매체는 이와 같은 Google의 태도를 향해 "Google은 FLoC이 프라이버시 보호를 위한 것이라 말하지만, 실상 그것은 '이용자 추적활동'의 위치를 Google의 서버로부터 Chrome 브라우저로 옮긴 것에 지나지 않는다."라고 비판적 평가를 하기도 했다.[15)]

(2) 제3자 쿠키의 대체품이 아닌 한계

FLoC는 제3자 쿠키를 대신하여 광고주에게 충분한 광고 타게팅 효과를 제공할 수 있다는 점에서 실용화 가능성을 인정받고 있지만, FLoC이 제3자 쿠키를 완전히 대체하는 것은 아니다. 이런 측면에서 FLoC는 (현재로서는) Chrome 브라우저에서만 작동하며, cross-device (browser) 트래킹을 지원하지 못한다. FLoC는 이용자의 관심사를 확인할 수 있는 용도 외에 다른 활용 사례를 찾기 어렵다. 이에 반해 제3자 쿠키는 전통적인 마케팅 기술에서 사용했던 여러 기법들에 사용될 수 있는데, 일련의 광고 소재를 순서대로 배치하여 광고의 효과성을 향상시키는 '광고 시퀀싱(ad sequencing)' 기법, 특정 광고가 이용자에게 노출되는 횟수를 제한하여 광고의 피로도 증가를 억제하는 '빈도 제한(frequency capping)' 등이 바로 그것이다. 이와 같은 효과적인 기법을 FLoC에선 사용할 수 없거나, 별도의 우회 방식(workarounds)을 적용해야 한다.[16)] FLoC이 전통적인 마케팅에서 널리 사용되었던 제3자 쿠키가 가져다 주었단 다양한 이점을 제공할 수 있을 것인지는 현재로서는 미지수이다.

11) Fortune, "Google beefs up privacy promises as it prepares to upend its ad model", 2021. 3. 3., URL: https://fortune.com/2021/03/03/google-blocks-tracking-ad-tech-floc-privacy/

12) Electronic Frontier Foundation, "Don't Play in Google's Privacy Sandbox", 2019. 8. 30., URL: https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1

13) 보안 극장(security theater)은 실제 보안성을 향상시키기 위해 필요한 활동을 거의 또는 전혀 수행하지 않으면서, 마치 향상된 보안성의 느낌을 제공하려는 의도로 보안 조치를 적용하는 관행을 의미한다. 프라이버시 극장은 널리 사용되는 표현은 아니지만, 보안 극장이라는 표현의 맥락에서 유사한 의미로 이해할 수 있다.

14) WIRED, "Google and the Age of Privacy Theater", 2021. 3. 18., URL: https://www.wired.com/story/google-floc-age-privacy-theater/

15) Business Insider, "Google says it's taking privacy seriously after Apple's recent moves. But it's really just trying to convince users tracking is OK.", 2021. 5. 12., URL: https://www.businessinsider.com/google-privacy-nutrition-label-apple-app-store-user-tracking-2021-5

16) What's New In Publishing, "6 problems with Google's FLoC (and 1 silver lining)", 2021. 2., URL: https://whatsnewinpublishing.com/6-problems-with-googles-floc-and-1-silver-lining/

(3) 광고 연관성 저하

기존의 타게팅 광고는 "지난 2주 기간동안 H사의 K자동차 모델에 관심을 보인 서울 지역의 30대 남성 직장인을 대상으로 광고를 노출", "최근 1주일 동안 3회 이상 P사의 신규발매 립스틱 3종에 관심을 보인 대학생 및 30대 직장인 여성을 대상으로 광고를 노출" 하도록 하는 등 여러 조건을 병렬적으로 적용하는 방식으로 광고의 타겟 군(群)을 비교적 정밀하게 형성하는 동시에, 이들 타겟 군을 대상으로 하여 연관성 있는 광고 소재를 개발할 수 있었다. 그러나, FLoC이 제시하는 코호트 ID는 대략적인 관심사를 추정하는 것은 가능하게 하지만, 기존과 같이 정밀한 타겟 군을 형성하여 연관성 있는 광고를 노출하는 것은 어렵게 만든다. Google은 In-Market 및 affinity Google Audiences에 FLoC을 사용한 결과 "쿠키 기반 광고와 비교하여 지불한 광고 금액 대비 95%의 전환율(conversion)을 보였다" 라며 FLoC의 효과성을 강조한 바 있다. 그런데, 이와 같은 결과를 제시하면서 "특정 결과는 FLoC이 사용하는 클러스터링 알고리즘의 강도(strength) 및 도달 대상인 audience의 유형에 따라 달라질 수 있다." 라고 하여, 95%에 달하는 쿠키 기반 광고 대비 전환율을 안정적으로 기대할 수 있는 것은 아니라는 점도 밝혔다.[17] [18] 제3자 쿠키 대신 사용하는 FLoC으로 인한 광고 연관성 저하는 중소사업자(SME)들에게 특히 부정적 영향을 미칠 것으로 예상된다. 이들은 광고에 지출할 수 있는 재정적 기반이 취약하기 때문에 최대한 타겟 군을 좁게 형성하고, 연관성 높은 광고를 제공하여 광고에 기반한 즉각적 효과성을 기대하는 특성이 있다. 그런데, FLoC은 타겟군을 정밀하게 형성할 수 있는 여러 조건을 상세히 설명해주지 않는다. Google이 향후 FLoC 코호트 ID를(기존의 수 천 단위에서 수만, 수십만 단위로) 더욱 세분화할 가능성은 있으나, 여전히 광고업계나 광고주는 그러한 코호트 값이 어느 정도로 정밀한 타겟 군에 대응할 수 있는가를 확신할 수 없다.

3. 민감 정보에 기반한 타게팅 가능성

방문한 사이트에 기반하여 관심사에 매칭되는 코호트 ID를 생성하는 경우, 방문한 웹사이트의 성격에 따라 민감한 성격의 관심사(sensitive categories of interests)가 코호트 ID에 반영될 수 있다. 여기에는 인종, 성적취향(LGBTQ), 종교, 건강(정신병력 등), 자산 상황, 정치적 성향 등이 포함된다. 이와 같은 정보에 기반하여 생성된 코호트를 대상으로 타게팅 광고가 전달되는 경우, 기존에 존재했던 사회적 차별이나 개인의 고난, 곤궁 등을 '착취(exploitation)' 할 수 있는 가능성이 열리게 된다. 예를 들어, 갑작스러운 물가 상승으로 인해 크게 올라버린 전세금을 마련할 수 없는 사람들에게 단기의 고리 이자를 동반하는 대출 광고를 타게팅하여 노출하는 경우라든지, 가짜 정보가 담긴 광고를 통해 선거 상황에서 정치적 선택을 바꾸도록 심리전을 수행하는 광고를 노출하는 경우 등과 같은 방식이 그러한 착취를 가능하게 하는 사례로 꼽힌다.[19]

Google도 이와 같은 가능성을 사전에 인지하고 있는 것으로 확인된다.

17) Google 광고에서 In-Market Audiences는 현재 제품이나 서비스를 구매하기 위해 적극적으로 탐색을 하고 있는 잠재적 고객을 의미하며, Affinity Audiences는 브랜드에 대한 인식을 구축하기 위해 타게팅 하는 고객을 의미한다. 이에 대한 보다 자세한 정보는 다음 링크를 참조할 수 있다. - Search Engine Land, "Affinity audiences coming to Google Search campaigns", 2019. 10. 16., URL: https://searchengineland.com/affinity-audiences-coming-to-google-search-campaigns-323580

18) Google, "Building a privacy-first future for web advertising", 2021. 1. 25., URL: https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

19) 2019년 초, National Fair Housing Alliance v. Facebook, Inc. 사안에서 양자는 합의에 이르러 재판이 기각되었다. 합의에 따라 Facebook은 주거 및 일부 다른 시장에 대해서는 제한된 타게팅 도구만을 사용한 '고립된 광고 플랫폼'을 구축하기로 약속했다. 이에 따라 광고주들은 더 이상 성별, 우편번호, 나이 등을 기반으로 하여 '보호받는 사람들'을 대상으로 하는 광고를 집행하지 못하게 되었다. 이에 관한 보다 자세한 내용은 다음 링크를 참조할 수 있다. - Chandler Nicholle Spinks, "Contemporary Housing Discrimination: Facebook, Targeted Advertising, and the Fair Housing Act", Houston Law Review Vol 57, Issue 4, 2020. 5. 6., URL: https://houstonlawreview.org/article/12762-contemporary-housing-discrimination-facebook-targeted-advertising-and-the-fair-housing-act

20) Google, "Federated Learning of Cohorts (FLoC)", URL: https://github.com/WICG/floc/blob/main/README.md

21) Google이 개인화 광고(personalized advertising)에서 금지하는 유형(prohibited categories)은 다음 링크에서 확인할 수 있다. Google, "Advertising Policies Help: Personalized advertising", URL: https://support.google.com/adspolicy/answer/143465?hl=en (최종방문 2021. 4. 4.)

22) Electronic Frontier Foundation, "What is Fingerprinting?", last reviewed 2020. 7. 14., URL: https://ssd.eff.org/en/module/what-fingerprinting

23) n 'bits of entropy' 를 가지고 있는 정보는 이를 알아내기 위해 2^n의 추정을 수행해야 한다는 것을 의미한다.

Google은 "코호트는 민감한 정보를 노출할 수 있다. 이에 대한 첫 번째 완화 방안은 브라우저가 데이터를 수집할 때, 민감한 유형을 제거하는 것이다. 그러나, 이러한 조치로 인해 민감 정보의 유출이 발생하지 않는다고 할 수는 없다. 일부 사람들에게 민감하지 않은 것이 다른 사람에게는 민감하게 여겨질 수 있기 때문이다. 또한, 민감한 유형의 개념에 대해 보편적으로 받아들여지는 기준이 있는 것도 아니다." 라고 설명한다. 이어서, "코호트가 민감한 유형의 관심사에 대하여 프록시(proxy)로 사용되는 것을 예방하기 위해, 민감한 유형의 우세(prevalence)와 관련한 인구 수준의 인구통계 정보로부터의 편차(deviation)를 제한하고 평가하는 방식으로 코호트의 공정성(fairness)을 평가할 수 있다." 라고 부연한다.[20] 그러나, 이와 같은 접근법을 취한다 하더라도 민감 정보에 기반한 타게팅과 그로 인한 사회적 차별의 심화, 개인 상황의 착취 등을 완전히 예방하는 것은 가능하지 않다. 아울러, 민감한 성격의 정보를 기반으로 코호트 ID를 생성하지 않았다 하더라도, 맥락적으로 민감한 정보로 작용할 수 있는 상황도 얼마든지 발생할 수 있다. 따라서, 코호트 ID가 민감한 유형의 관심사를 노출하거나, 민감한 유형의 관심사에 대한 프록시로 기능하는 것을 원천적으로 차단하는 것은 가능하지 않은 것으로 보인다.[21]

4. 브라우저 핑거프린팅

브라우저 핑거프린팅은 이용자가 사용하는 브라우저로부터 여러 분절적 정보(discrete information)를 수집하여, 해당 브라우저를(=브라우저를 사용하는 이용자를) 지속적으로 식별하는 기법을 의미한다. 이용자를 추적하기 위한 기법으로서 핑거프린팅이 효과를 거두기 위해서는 지속성(persistence)과 고유성(uniqueness)를 충족해야 한다. 첫번째 특성은 정보를 브라우저 내에 저장하지 않고, 삭제가 불가능한 웹 서버에 저장하는 방식으로 충족할 수 있고, 두번째 특성은 여러 상이한 특성의 정보를 조합하여 고유한 정보를 생성하는 방식으로 충족할 수 있다.[22] Google은 낱개의 FLoC 코호트가 수 천명에 달하는 사람으로 구성되기 때문에 군중 속에 개인을 숨기는 방식으로 개인에 대한 추적을 예방할 수 있을 것으로 기대한다. 그러나, 특정한 트래커가 코호트 ID를 수집하게 되는 경우, 해당 트래커는 수천분의 1의 가능성으로 동일한 코호트 ID를 공유하는 사람들을 확인할 수 있게 된다. FLoC 코호트는 정식 배포 전의 테스트 단계에서 수 비트의 엔트로피(bits of entropy)를 보유하는 것으로 결정되었는데(최대 8비트), 이는 특정 브라우저가 노출하는 다른 정보와 상관관계를 맺지 않을 가능성을 상당한 수준으로 높이는 것이다. 따라서, 특정 브라우저로부터 수집하는 여타 정보와 코호트 ID가 결합하는 경우 매우 고유한 핑거프린트를 생성할 수 있게 된다.[23] 그런데, Google은 Privacy Sandbox 이니셔티브에 착수한 주요 배경으로 "쿠키를 대규모로 차단하는 경우 '핑거프린팅(fingerprinting)' 등 불투명한 기술의 사용을 촉진하여 오히려 사람들의 프라이버시를 침해하는 방향으로 나아갈 수 있다." 는 점을 제시했고 이에 따라 FLoC의 도입을 검토한 것인데, FLoC 코호

트 ID가 이용자를 추적할 수 있는 핑거프린트 생성 요소로 활용될 수 있다는 점은 Google의 Privacy Sandbox 이니셔티브 착수 배경과 모순된다는 점에서 큰 비판의 여지를 안고 있다.

Google은 이와 같은 문제점을 해결하기 위해 "Privacy Budget"이라는 개념을 도입하기로 했다. 이는 웹사이트가 Google의 API를 통해 수집할 수 있는 데이터의 총량을 제한하는 'Privacy Budget API'를 적용한다는 것인데, 마치 개별 웹사이트에게 활용할 수 있는 제한된 '재원(budget)'을 주는 것과 유사하기 때문에 Privacy Budget으로 불린다. 다만, Privacy Budget은 아직 초기 논의 단계에 그치고 있으며, 개별 웹사이트가 처리를 필요로 하는 정보 가운데 핑거프린팅에 사용될 수 있는 정보를 확인하는 작업(소위 'fingerprinting surface'에 대한 측정을 의미함) 등 복잡한 절차를 요구하는데다, 급변하는 웹 환경에 후행적으로 대응하는 과정에서 이용자의 사이트 이용 경험(UX)에 부정적으로 작용할 수 있는 등 여전히 개선해야 할 지점이 많은 것으로 평가된다.[24)]

5. 사람들의 관심사를 웹에 전달, 공개

FLoC API는 결국 사람들의 관심사를 코드화 하여 웹사이트에 전달하는 것인데, 이를 다시 말하면 개인의 일반적 웹 브라우징 히스토리에 관한 정보에 대한 접근(access)을 웹사이트에 오픈하는 것이다. 기존의 쿠키는 제한된 복수의 웹사이트 방문 기록을 조합하는 것에 그쳤다면, FLoC API는 이용자가 방문한 거의 전체 웹사이트를 브라우징하는 과정에서 발생한 정보에 대한 접근을 개방한 것이다. 만약 웹사이트가 이용자를 식별할 수 있는 정보를 사전에 보유하고 있는 상태라면, 이용자의 관심사가 웹사이트와 대중에 공개될 수도 있다. Google은 이에 대해 "자신에 관한 정보를 제공하는 것을 웹 생태계를 지속하기 위해 비용을 지불하는 것으로 받아들이지 못하는 사람들도 있을 것이다. 브라우저가 FLoC 코호트 ID를 웹사이트로 전송하도록 할 것인지, 또는 의미 없는 난수를 전송하도록 할 것인지는 (이용자로 하여금) 통제 가능하게 할 것이다."라는 설명을 제시한다.[25)] 그런데, FLoC 코호트 ID를 웹사이트에 전송하는 것과 관련하여 기본 설정(default settings)을 무엇으로 할 것인지, 웹사이트가 코호트 ID를 전송하도록 유도하는 Dark Pattern을 적용하는 행태가 확산되는 경우에 대한 적절한 대응이 가능할 것인지 등의 문제는 한동안 해결해야 할 과제로 남을 수밖에 없다.

Ⅳ. 시장 경쟁적 측면에서의 이슈

1. 기존 광고 생태계에서의 지위 강화

영국 반독점 당국인 CMA (Competition and Market Authority)는 '21년 1월 Google의 'Privacy Sandbox' 브라우저 변화에 대한 조사에 착수한다 밝혔다. 이와 같은 조사는 MOW (Marketers for an Open Web)라는 기업 연합체가 Google의 Privacy Sandbox를 중단하도록 요청 요청한 것에 기반한 것이다.[26)]

24) Privacy Budget에 대해 보다 자세한 설명은 다음 링크를 참조할 수 있다. - (1) Brad Lassey, "Combating Fingerprinting with a Privacy Budget", URL: https://github.com/bslassey/privacy-budget, (2) Chrome Dev Summit 2020, "Introducing the Privacy Budget", URL: https://toppicplay.com/v/395254

25) Google, 앞의 글(주 20)

26) Marketers for an Open Web, "Press Release: Marketers for an Open Web calls on UK Competition and Market Authority to block Google's 'Privacy Sandbox'", 2020. 11. 23., URL: https://marketersforanopenweb.com/marketers-for-an-open-web-calls-on-uk-competition-and-market-authority-to-block-googles-privacy-sandbox/

27) UK Competition and Markets Authority, "CMA to investigate Google's 'Privacy Sandbox' browser changes", 2021. 1. 8., URL: https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes

28) UK Competition and Markets Authority, "Online platforms and digital advertising: market study final report", 2020. 7. 1. p.295

29) The Verge, "Google antitrust suit takes aim at Chrome's Privacy Sandbox", 2021. 3. 16., URL: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy

30) Ad Exchanger, "Innovation Labs: Google's Chetna Bindra Gives The Lowdown On PPIDs, FLoCs And UID", 2021. 3. 17., URL: https://www.adexchanger.com/privacy/innovation-labs-googles-chetna-bindra-gives-the-lowdown-on-ppids-flocs-and-uid/

CMA는 Google의 제안이 경쟁사를 희생시키고 광고 비용 지불을 Google의 생태계에 더 집중하게 할 것인지를 살펴보겠다고 밝혔다. (FLoC을 포함하는) Google의 Privacy Sandbox 제안은 Chrome 브라우저에서 제3자 쿠키를 비활성화(disable) 하고 소비자 프라이버시를 강화하는 일련의 도구들을 적용하는 것인데, 이로 인해 웹사이트 운영자(publisher)들이 수익을 창출할 수 있는 역량을 약화시키고 디지털 광고 시장에서의 경쟁을 해할 것은 아닌가 하는 우려를 가지고 있다고 CMA는 밝혔다.[27)] CMA가 발간했던 온라인 플랫폼과 디지털 광고 시장에 대한 연구 조사 결과 보고서에서는 웹사이트 운영자가 광고를 판매하기 위해 사용하는 쿠키에 대한 접근을 차단하는 경우 웹사이트의 수익이 2/3가량 감소할 수 있다고 하는데, 특히 중소 지역 상공인들이 가장 크게 영향을 받고, 팩트 체크된 온라인 뉴스가 보다 큰 위협에 처해진다고 확인한 점도 이번 고발의 주요 논거로 사용되었다.[28)]

미국에선 '21년 3월에 미국 주 법무장관들이 Google을 대상으로 '수정된 고발장'을 접수했다. 주 법무장관들은 반독점 행태에 관여했고, 광고 산업 영역에서의 경쟁 제한을 위해 Facebook과 불법적인 협약을 체결했다는 이유로 Google을 '20년 12월에 고발한 바 있었다. 수정된 고발은 크게 다음의 세 가지 주요 요소를 담고 있다. 첫째, Google은 '19년 6월에 검색 알고리즘을 업데이트 하여 Google의 광고 솔루션에서 차등적 가격을 웹사이트에 적용했다. 둘째, Google은 WhatsApp 백업은 사적으로 관리될 것이라고 이용자들에게 설명했음에도, Google Drive에 백업된 WhatsApp 이용자의 통신 내용에 접근했다. 셋째, Privacy Sandbox 프로젝트는 인터넷 이용자들이 Chrome 브라우저를 이용하여 생성한 정보를 차단하는 동시에 Google 자신의 프라이버시 관행으로부터 규제의 관심을 빗겨내게 하려는 계획이다. 특히, Privacy Sandbox와 관련하여, Google은 브라우저 시장을 장악하고 있는데, 이로 인해 광고주들은 Google을 중개인(middle man)으로 활용할 수밖에 없고, Google 자신의 광고 시스템을 더욱 매력적으로 만들 것이라는 주장이다. 고발 당사자들은 고발장에서 "Google은 프라이버시를 구실로 참된 의도를 숨기고 있다. Google은 실제 이용자 프로파일링이나 타겟 광고를 중단하지 않는다. Privacy Sandbox는 Google의 Chrome 브라우저를 트래킹과 타게팅의 중심에 놓이게 할 것이다."라며 비판적 입장을 견지했다.[29)]

이와 같은 미국, 영국 정부의 공격적 태도와 프라이버시 비평가들의 우려 제기에 대해 Google의 '이용자, 신뢰, 프라이버시 및 투명성을 위한 그룹 제품 매니저'인 Chetna Bindra는 한 대담에서 "Google은 사람들이 웹을 브라우징 하는 동안 Google이 개별 이용자를 추적하기 위한 어떠한 유형의 기술을 만들거나 이용할 의도가 없다. 여기에는 Chrome login을 사용하는 것도 포함되는데, 이것은 현재 진행되고 있는 광고 수익화 노력과 전혀 관련이 없다."라고 설명했다. 또한, Google 부사장이자 광고 총괄 매니저인 Jerry Dischler는 한 행사에서 "우리는 (FLoC과 관련하여) 백도어를 만들지 않을 것이다."라고 발언하기도 했다.[30)] 그런데, Google의 Chetna Bindra가 Google login이 아닌 Chrome login을 언급한

지점은 Google이 Google login으로 수집한 first party 데이터를 광고 타게팅으로 사용하려는 의도를 감춘 것으로 추정되는 지점이다.

프라이버시 중심의 브라우저를 제공하는 Brave Software, INC(이하 "Brave")는 자사 브라우저에 FLoC을 적용하지 않을 것이며, 자사가 운영하는 웹서비스의 정보가 FLoC을 통해 분석되지 않도록 FLoC 옵트아웃을 적용할 것이라 밝혔다. Brave는 이와 같은 정책을 적용하는 여러 배경 가운데 하나가 FLoC이 웹사이트 운영자(sites and publishers)에게 해가 되기 때문이라는 점을 밝혔다. Brave는 가상의 예를 제시했는데, '폴카 음악'을 판매하는 웹사이트를 운영하는 운영자는 '다른 곳에서 제대로 된 폴카 음악 팬의 필요를 충족할 만한 음악 및 커뮤니티 서비스를 제공하지 못하기 때문에' 자신이 제공하는 서비스가 니치 마켓에 소구할 수 있어 성공적인 사업을 운영할 수 있다. 이러한 이유로 해당 웹사이트 운영자는 Amazon에서 제공하는 음악 서비스보다 더 비싼 값을 매길 수 있는 것이다. 그런데, FLoC은 Chrome 브라우저에 "폴카 음악 애호가"라는 코호트를 형성할 수 있고, 해당 코호트 ID를 다른 웹사이트에 전달할 수 있다. 여기에는 Amazon.com도 포함이 된다. 이러한 경우 Amazon과 같은 거대 기업은 획득한 코호트 ID를 이용하여 폴카 음악 팬들을 탈취하듯 확보할 수 있게 된다. 광고 생태계에서 흔히 발생하는 소위 "audience stealing"이 발생하는 것이다. 이와 같은 유사사례는 여러 측면에서 발생할 수 있는데, 이는 결국 특정 사이트를 통해 획득한 '이용자에 관한 정보'를 다른 웹사이트에 공개하듯 전달(broadcast)하기 때문에 발생하는 현상이다. 코호트 ID를 전송받은 웹사이트는 해당 정보를 이용하여 가격 차별(price discrimination) 등 타 서비스 이용자를 획득하기 위한 공격적 마케팅을 활용할 가능성이 높아진다. 이와 같은 행태는 프로그래매틱 광고에서 오랜 기간동안 유지되어 왔으며, FLoC이 제거하려 시도하는 '제3자 쿠키 이후의 시대'에서도 FLoC으로 인해 여전히 유지될 가능성을 배제할 수 없다는 것이 Brave의 주장이다.[31)]

상기 내용을 종합해보면, FLoC을 주요 요소로 하는 Privacy Sandbox에 대해 제기되는 시장경쟁적 관점에서의 우려는 ① 기존에 Chrome 브라우저가 가지고 있는 시장 지배적 지위가 제3자 쿠키 지원 중단 및 FLoC 도입을 통해 더욱 강화될 것이라는 점, ② 제3자 쿠키에 대한 접근이 제한됨에 따라 웹사이트(publishers)들의 수익이 급감하며, 이로 인해 Google의 광고 생태계에 대한 의존이 증대될 것이라는 점, ③ 제3자 쿠키에 대한 접근이 제한됨에 따라 Google이 first party로 데이터를 수집할 수 있는 영역(예: analytics, Google login, Android OS)에서 수집한 데이터의 가치가 더욱 높아지게 되어 경쟁적 이익을 획득할 수 있게 될 점 ④ 기존 광고 생태계에 존재했던 audience stealing 등의 문제점을 지속적으로 유지할 가능성이 높은 점 등으로 추려볼 수 있을 것이다.[32)]

31) Brave Software INC, "Why Brave Disables FLoC", 2021. 4. 12., URL: https://brave.com/why-brave-disables-floc

32) ③에 대한 상세한 내용은 다음 링크를 참조할 수 있다. - Oracle (Blog), "Google's Privacy Sandbox-We're all FLoCed", 2021. 3. 7., URL: https://www.oracle.com/news/announcement/blog/google-privacy-sandbox-030721.html

33) Bird & Bird (Thomson Reuters Practical Law), "French Competition Authority: No interim measures against Apple regarding its App Tracking Transparency framework", 2021. 4. 1., https://uk.practicallaw.thomsonreuters.com/w-030-3276

34) 이진규, "iOS 14의 프라이버시 보호 정책 변화를 둘러싼 Facebook과 Apple의 대립, 그 속내는 - 프라이버시 보호와 반독점, 그리고 기업의 이익", 2021. 1., KISA Report Vol.01-5, 10면

2. Apple과의 비교

Apple은 iOS 14.5 업데이트를 통해 광고 식별자인 IDFA에 기반한 추적에 대한 옵트인을 요구하는 ATT(App Tracking Transparency)를 적용했다. 이에 관한 여러 설문 결과가 있으나, 대략 옵트인을 통해 광고 추적을 허용하는 이용자의 비율은 10~40% 이내로 확인되고 있다. IAB France, UDECAM, MMAF, SRI 등 4개 광고 사업자 단체는 '20. 10월, 프랑스 경쟁 감독당국(Autorité de la concurrence)으로 하여금 Apple이 ATT를 적용하는 것을 막아달라는 청원을 했다. 청원인들은 첫째, ATT의 적용이 이용자의 개인정보 보호에 비례하지 않거나, 필요하지 않은 불공정한 거래 조건을 부과할 것이며, 둘째, 유럽연합기능조약(TFEU) 102조 d항(계약의 주제(내용)와 관련 없는 의무(성질상 혹은 상관습 상의)를 타방 당사자가 수용하게 하고 계약을 체결하는 것을 금지하는 규정)에 반하는 부가적 조건을 부과할 것이라는 점을 고려해 달라면서, ATT 시스템을 통해 이용자의 동의를 받도록 하는 것을 조건으로 삼지 않을 것과 이용자 개인정보보호 및 건전한 경쟁상황 형성을 위해 연관된 관계자들과 건설적 대화에 나설 것을 요구했다. 감독당국은 추적에 대해 앱 이용자 동의를 받는 것이 남용적 행태는 아니라며(doesn't appear to be abusive) 주장을 받아들이지 않았다. 그러나, 당국은 Apple의 ATT 정책이 제3자 앱에 대해 보다 엄격한 조치를 적용하는 방식으로 '자사우대(self-preferencing)'를 한 것은 아닌지 심층 조사에 나서겠다고 밝혔다.[33)]

Facebook의 광고 및 비즈니스 제품 영역 부사장인 Dan Levy는 '20년 말에 "소기업을 위한 발언(Speaking Up for Small Business)"이라는 글을 통해 Apple이 iOS14에 적용한 변화가 '프라이버시 보호를 위한 것이라기 보다는 오히려 Apple의 이익을 위한 것(More about Profit than Privacy)'이라며 Apple을 강하게 비판했다. 그는 Apple의 정책 변화가 창작자들로 하여금 광고를 통해 돈을 벌 수 있는 기회를 제거하여 결국 구독이나 인 앱 구매(in-app purchase) 모델에 의존할 수밖에 없도록 내몰린다는 점을 강조했다. 이는 창작자들이 Apple에 지불하는 15% - 30%에 이르는 '애플 세(Apple Tax, 앱스토어 수수료를 의미함)'를 더 거둘 수 있게 되는 결과로 이어지는데, 결국 Apple은 이를 통해 더 많은 수익을 확보하게 되어 감소하는 하드웨어 사업부의 매출을 보충할 수 있지만, 사람들은 더 많은 '무료 서비스'를 잃게 될 것이라는 지적을 한 것이다. 또한, Apple은 스스로 만들어 놓은 iOS14의 변화로부터 '셀프 면제'를 적용하여 광고 사업에 부정적 영향을 받지 않을 것이지만, 다른 기업들은 정책을 차별적으로 적용 받아 경쟁력이 약화될 것이라고 주장했다.[34)]

여기에서 중요한 것은 Apple이 ATT를 적용하는 경우 앱스토어에서의 수익을 강화할 수 있다는 점이다. ATT에서의 옵트인 비율이 낮아지만, 광고에 의존하여 수익을 창출하던 중소 앱 개발자는 수익 모델을 광고에서 구독(subscription)으로 전환하게 되며, 이는 결국 Apple의 결제 수수료를 증대시키기 때문이다. 프랑스 감독 당국이 Apple의 ATT가 제3자 앱에 대해 보다 엄격한 조치를 적용하는 방식으로 자사우대를 한 것은 아닌지에 대한 조사를 하겠다 하였으나, 앱

개발자들의 수수료 방식으로의 사업모델 전환과 같은 '불투명한' 지점까지 확대될지 여부는 향후 조사 과정에서 지켜봐야 할 지점으로 판단된다. 또한, Google과 Apple 모두 이용자 프라이버시 보호를 위해 내세운 조치가 결과적으로 자사의 수익 구조를 강화하는 방식으로 광고 생태계를 재편한다는 점에서 프라이버시와 시장경쟁의 교집합을 확대하여 규제 방정식을 보다 다차원으로 만들고 있다고 평가할 수 있다. 이러한 점은 규제 관점에서 여러 도메인의 규제당국이 협력해야 할 지점이 점차 명확해지는 동시에 복잡해지고 있다고 바꾸어 말할 수 있다.

Ⅴ. 나가며

Google은 FLoC를 포함하는 Privacy Sandbox가 여전히 발전하고 있는 개념들의 집합이라며, 오픈 스탠다드 방식으로 다양한 참여자들의 의견을 반영하는 과정에서 지속적으로 변화하고 있다는 점을 강조한다. 그러면서, FLoC에 대한 origin trial(Chrome에 적용될 새롭거나 실험적 웹 플랫폼 기능을 테스트하는 것)을 3월 말에 개시했는데, GDPR이 적용되는 유럽연합은 테스트 대상에서 제외를 했다. Google 엔지니어인 Michael Kleber는 WWW 컨소시엄 미팅에서 "FLoC가 유럽연합 개인정보보호법제와 양립가능하지 않을 수 있다."고 발언한 사실이 알려졌다. 그는 "Google은 유럽에서 FLoC 테스트를 진행하지 않을 것인데, 코호트 생성에 있어 어느 주체가 data controller이고 어느 주체가 data processor인지에 대한 우려가 존재하기 때문이다."라고 설명했다고 한다.[35] 이는 코호트에 이용자를 배정하기 위해 웹 브라우저가 개인정보를 처리하는 것(=FLoC 모델의 알고리즘이 개인정보를 처리하는 것)이 유럽연합 개인정보보호법제의 적용을 받는 행위일 수 있다는 것이다. 따라서, 적절한 동의절차 없이는 위법에 해당할 수 있어 유럽연합에서는 이를 진행하지 않은 것으로 이해된다. 만약 FLoC를 본격적으로 Chrome 브라우저에 적용하는 시점에도 여전히 GDPR을 준수하는 방식으로 관련 기능을 제공할 수 있다는 확신이 없다면, Google은 유럽연합을 제외한 국가를 대상으로 FLoC를 적용할 가능성도 완전히 배제할 수는 없다. 그런 경우라면, '개인정보를 보호하기 위해 개발한 기능이 개인정보보호 법제로 인해 적용되지 못하는 상황'이 발생하는 것이며, 유럽연합 정보주체들은 그 결과 프라이버시 관점에서 보다 취약한 (이용자 추적 방식의) 제3자 쿠키 기반의 타게팅 광고에 노출될 가능성이 있다. 이는 매우 아이러니한 상황이 아닐 수 없다.

웹 서비스를 이용하는 이용자의 프라이버시를 보호하기 위한 기술적 고안이지만, FLoC이 프라이버시를 완벽하게 보장하는 방식은 아니다. 특히, 이용자의 웹 브라우징 활동 기록을 축적하여, 분석하고, 관심사를 코드화 하여 웹 사이트와 공유하는 것은 이용자 추적에 기반한 감시 자본주의 체제를 지속화할 수밖에 없다는 점에서 근본적인 결함이 있는(fundamentally flawed) 방식이라는 지적도 확인된다. 그렇다고 하여, Google이 광고 생태계에서 추적을 허용하는 유일한 빅테크 기업은 아니다. Apple도 ATT를 통해 동의를 받은 경우 IDFA 식별자에 기반한 추적 광고를 허용한다. 이용자의 선택에 추적 여부를 맡겨 둔 것이다. 어느 기업의 방식이 다른 기업의 방식보다 더 바람직하다고 평가하는 것도 쉽지 않은 이유가 여기에 있다.

이와 같은 논의에 있어 국내 광고 산업 생태계에 미치는 영향이 무엇이며, 글로벌 빅테크 기업의 정책 변화가 우리나라 규제에 미치는 영향 내지 우리나라 법을 준수하는 방식으로 진행이 되고 있는지에 대한 검토는 거의 확인되지 않는다. 프라이버시 보호를 내세운 글로벌 기업의 정책 변화가 국내 광고 산업의 경쟁 지형에 미치는 영향에 대한 실증적 분석은 매우 절실하다. 특정 디지털 서비스 시장에서 우월적 지위를 점하고 있는 글로벌 빅테크의 기술과 정책 변화를 제대로 이해하고, 이들의 활동이 우리 소비자들의 권익을 침해하지 않도록 공정한 경쟁의 장을 만들지 않는 경우 우리나라는 그저 빅테크에게 또 하나의 시장일 뿐이기 때문이다. "If you do not make the rules, you are ruled by their rules."라는 표현이 만들어질 수도 있을 것이다.

35) Search Engine Land, "Google's current FLoC tests aren't GDPR compliant", 2021. 3. 23., URL: https://searchengineland.com/googles-current-floc-tests-arent-gdpr-compliant-347168