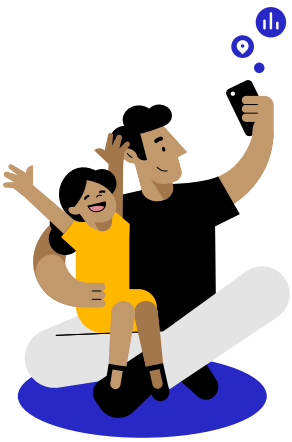


당신의 데이터는 어떤 하루를 보내는가

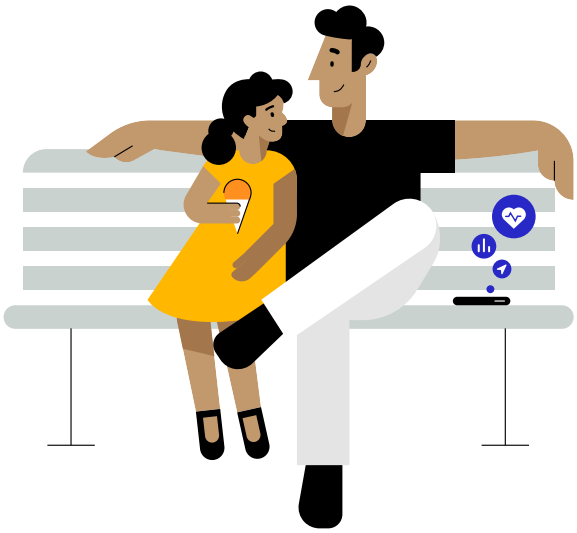
놀이터에서 함께 보낸 아빠와 딸의 어느 날 이야기

2021년 4월

"나는 인간의 판단력을 믿는 사람입니다. 저마다 차이는 있겠지만 자신의 정보를 더 많이 공유하고 싶은 사람도 있겠죠. 그렇더라도 지레짐작하지 말고 얼마큼의 개인 정보를 공유하고 싶은지 확인하세요. 매번 확인해야 합니다. 사용자들이 질려서 그만 좀 확인하라고 할 때까지 확인하세요. 그리고 사용자가 공유한 데이터를 어떻게 활용할 예정인지 역시 정확히 고지해야 합니다."

Steve Jobs

2010 All Things Digital 컨퍼런스



이 거대하고 불투명한 업계는 지난 10년간, 해가 거듭될수록 점점 더 많은 양의 개인 정보를 수집해왔습니다.[1,2] 웹사이트, 앱, 소셜 미디어 기업, 데이터 브로커, 에드 태크 기업들로 구성된 복잡한 생태계 속에서 사용자의 온라인 및 오프라인 활동이 추적되고, 사적인 데이터가 수집되었죠. 수집된 데이터는 짜깁기되고, 공유되고, 합쳐지고, 실시간 경매에 활용되어 업계에 연간 2,270억 달러에 달하는 수익을 안겨줍니다.[1] 사용자들이 일상을 살아가는 동안 매일같이 진행되는 이 작업은 종종 사용자의 동의나 허락 없이도 이루어지죠.[3,4] 아버지와 딸이 공원에서 즐거운 하루를 보내는 동안 이 업계가 부녀에 관해 얻을 수 있는 정보가 무엇인지 함께 알아볼까요?

알고 계셨나요?

당신이 매일 사용하는 대부분의 앱에는 개인 정보 추적기가 내장되어 있습니다. 평균적으로 한 앱당 6개의 추적기가 설치되어 있죠.[3] 대다수의 인기 안드로이드 및 iOS 앱에도 추적기가 내장되어 있습니다.[5,6,7]

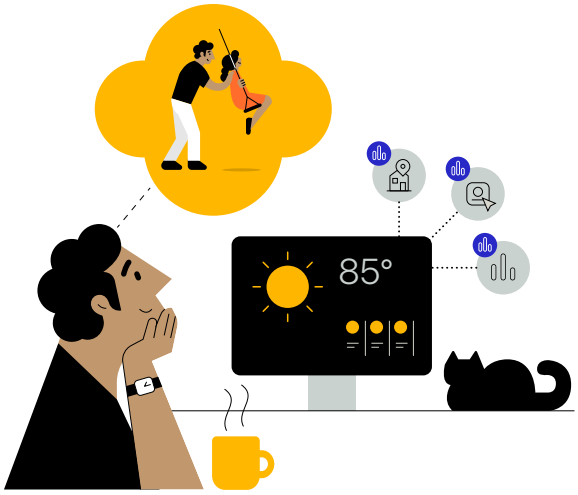
개발자의 앱 개발을 지원하는 SDK 및 API에 추적기가 내장되는 경우도 종종 있습니다. 추적기를 설치함으로써 개발자들은 당신이 개발자에게 공유한 데이터를 제3자가 수집할 수 있게 하기도, 이 데이터를 다양한 앱 및 당신에 관한 다른 데이터와 연결 지을 수 있게 하기도 하죠.

데이터 브로커는 개인 정보를 수집, 판매, 라이선싱하거나 제3자에게 공개합니다. 이 개인 정보는 보통 브로커와 직접적으로 관계없는 특정 개인들의 것이죠.[3]

수백 개의 데이터 브로커가 온라인 및 오프라인 경로를 통해 데이터를 수집합니다.[8] 보통 하나의 브로커가 전 세계 7억 명의 소비자 데이터를 수집하고, 이 데이터를 활용해 최대 5천 가지의 성향이 담긴 다양한 소비자 프로필을 완성하죠.[9]

한 연구에 따르면 약 20%의 아동용 앱에서 개발자에 의한 사용자의 개인 식별 정보 수집 및 공유가 이루어졌으며, 그 과정에서 그들은 아동의 부모로부터 유효한 동의를 구하지 않았습니다.[10]

온라인상에서는 매일, 매시간 수십억 건의 디지털 광고가 사용자들에게 노출됩니다.[11,12,13] 앱을 불러오는 데 걸리는 1,000분의 1초 동안 실시간 경매가 벌어지죠. 광고주들은 이 짧은 시간 동안 해당 광고 공간을 두고 입찰을 진행하며 이때 광고 대상 기기 사용자의 추적 데이터가 활용되기도 합니다.[14,15]



딸과 함께 공원에서 보낼 하루를 계획하는 존

존과 그의 일곱 살 난 딸 엠마는 하루를 함께 보내기로 합니다. 아침에 존은 컴퓨터로 날씨를 검색하고, 뉴스 기사를 읽고, 스마트폰 지도 앱으로 딸아이의 학교 옆 공원까지 가는 길의 교통 상황을 확인하죠. 차로 아이의 학교까지 가는 동안 존의 스마트폰에서는 네 개의 앱이 백그라운드에서 구동되며 주기적으로 그들의 위치 데이터를 수집하고 추적합니다.[16,17,18] 앱 개발자는 기기에서 추출된 데이터를 신원을 알 수 없고, 존이 들어본 적도 없는 다수의 제3자 데이터 브로커에 판매합니다.[16,17] 수집된 위치 데이터는 익명의 정보로 보관되는 것으로 알려져 있지만, 실제로 사용자 추적 기술은 데이터 브로커들이 해당 앱에서 얻은 존의 위치 이력을 그가 설치한 다른 앱의 사용 정보와 매치시킬 수 있게 해줍니다.[16,19] 즉, 다양한 앱 및 다수의 소스를 추적해 수집된 정보는 어느 기업, 어느 기관에나 팔려나갈 수 있고, 존의 상세한 하루 일과가 포함된 포괄적인 프로필을 만들어내는 데에도 쓰일 수 있다는 얘기죠.[3,16]

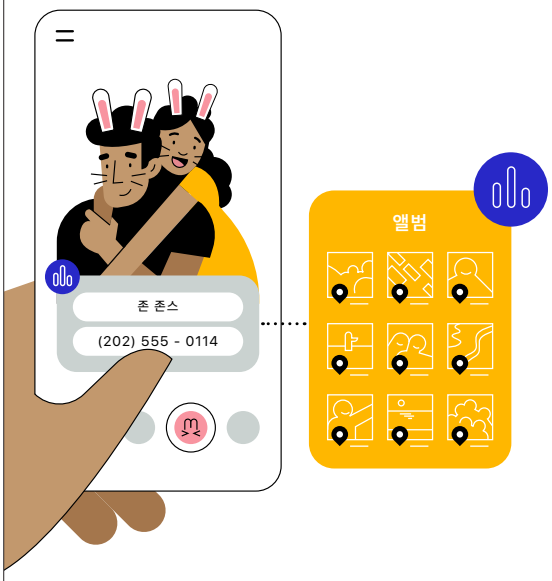
공원으로 향하는 차 안에서 게임을 즐기는 엠마

공원으로 가는 차 안에서 존은 딸이 자신의 태블릿으로 게임을 할 수 있게 허락해줍니다. 그리고 앱을 연 엠마는 킥보드 광고를 보게 되죠. 이건 우연히 일어난 일이 아닙니다. 앱을 불러오는 그 찰나의 시간 동안 해당 광고 공간에 대한 경매가 진행됩니다.[14] 사실 킥보드 회사를 대행하는 광고 회사들은 중개 업자를 통해 이 광고가 입찰 대상이 되었다는 사실을 미리 알고 있었습니다.[15] 그래서 수집된 존과 엠마의 개인 정보를 활용하여 광고 입찰에 참여할 수 있었던 거죠.[15] 킥보드 회사의 광고 파트너는 존과 엠마가 광고를 클릭했는지, 킥보드를 구매했는지 등을 확인하기 위해 이들이 광고를 본 이후의 행동 정보도 계속해서 수집합니다.[3] 광고주들은 앞으로도 존이 가지고 있는 모든 기기의 여러 앱 및 웹사이트를 통해 존과 엠마를 따라다니며 킥보드 광고를 노출시키기 위한 모든 방법을 동원할 것입니다.[3,20,21]

어떤 앱들은 서비스 제공에 필요한 것보다 더 많은 데이터에 대한 접근 권한을 요구합니다. 예를 들면 키보드 앱이 정확한 위치 정보 접근 권한을 요구하는 식이죠.[5]

광고 네트워크, 광고 퍼블리셔, 어트리뷰션 및 측정 제공업체, 데이터 브로커, 기타 사기업, 심지어 정부 기관까지도 정보 거래에 참여합니다.[3,15,40,41,42] 일부 소셜 미디어 및 에드 테크 기업들은 수백만 달러의 벌금형에 처해지거나 이미 벌금을 납부한 바 있습니다. 이들이 사용자에게 고지한 개인 정보 수집 목적과 실제로 데이터가 사용된 정황이 달랐기 때문이죠.[22,23,24,25]

데이터 브로커들은 수집한 데이터를 활용해 각 사용자에게 속성을 부여한 뒤, 대단히 세분화된 마켓 세그먼트에 따라 이들을 분류합니다. 예를 들어 '살은 빼고 싶지만 빵은 먹고 싶은' 소비자 그룹을 만드는 식이죠.[26] 하지만 이와 같은 프로필이 늘 정확한 건 아닙니다. 한 연구에서는 이와 같은 속성의 40% 이상이 부정확한 것으로 나타났습니다.[27,28]

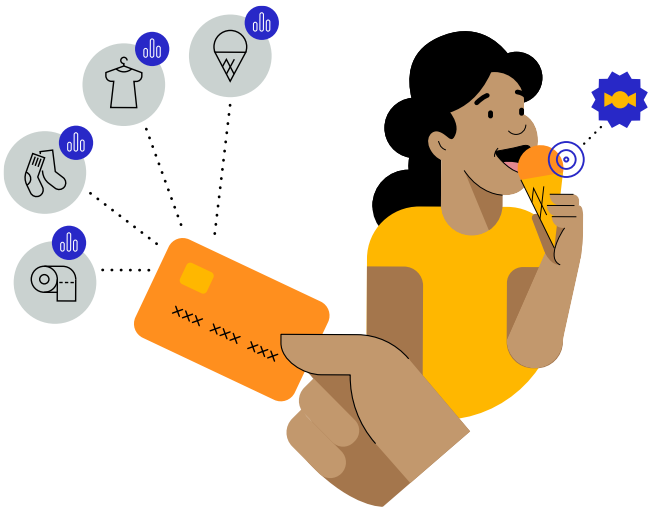


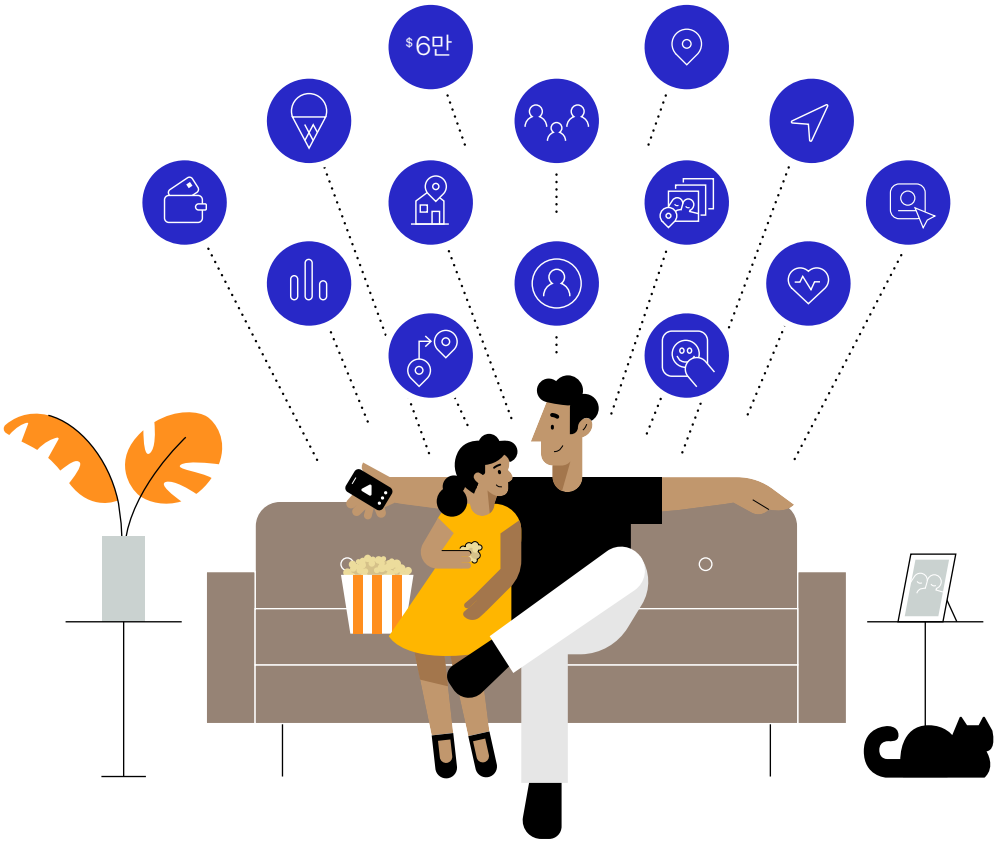
공원에서 셀피를 촬영하는 존과 엠마

공원에 도착한 존과 엠마는 얼마 뒤 셀피를 찍으며 놀기 시작합니다. 부녀는 사진 필터 앱으로 셀피를 촬영하다가, 촬영한 사진에 토끼 귀를 붙이는 설정을 추가합니다. 사실 이 필터 앱은 공원에서 찍은 셀피뿐만 아니라 기기에 저장된 모든 사진 및 사진의 메타 데이터에도 접근할 수 있습니다.[29,30] 이제 존은 딸과 함께 찍은 사진을 소셜 미디어 앱에 올립니다. 이 앱은 존의 현재 온라인 활동을 이메일 주소, 전화번호, 광고 식별자 등을 활용해 다른 앱에서 수집한 위치 정보, 구매 이력 등의 데이터와 연결 짓습니다.[3]

집으로 돌아가는 길에 아이스크림 가게에 들른 존과 엠마

집으로 돌아가는 길, 존과 엠마는 간식으로 먹을 아이스크림을 사러 가게에 들릅니다. 존이 아이스크림 값을 신용카드로 지불하자 그의 선호 성향에 관한 포괄적인 데이터 프로필에 가게의 위치, 소비한 금액 등의 정보가 추가됩니다.[31,32,33] 존의 위치를 추적하던 앱 중 하나가 존과 엠마가 장난감 가게에도 들렀다는 사실을 추적해냅니다.[3] 이 가족의 하루 동안의 쇼핑 위치 정보가 데이터 브로커에게 전달됩니다. 이들은 이 정보를 존에게 어린 자녀가 있다는 사실과 연관 지은 뒤, 달콤한 간식 및 부녀가 방문한 장난감 가게에 관한 타깃 광고를 존의 기기에 퍼붓습니다.[17]





결과적으로 존이 한 번도 거래해본 적 없는 전 세계 수많은 기업들이 존과 그의 딸에 관한 정보로 부녀의 프로필을 업데이트할 수 있게 된 겁니다. 이 기업들은 존의 거주지는 물론 부녀가 방문한 공원의 위치, 그들이 읽은 뉴스 기사 웹사이트, 검색한 제품, 시청한 광고, 구매 습관, 방문한 매장의 위치까지 알고 있습니다.[3,34] 이와 같은 데이터는 존과 엠마가 하루 종일 사용한 다양한 앱 및 기타 소스를 통해서 수집 및 추적되었죠. 존은 하루 동안 얼마큼의 개인 정보가 수집되었는지 전혀 알지 못했으며, 자신의 개인 정보를 관리할 수 있는 권한을 늘 가지고 있는 것도 아니었습니다. 게다가 이런 일이 일어날 것을 알고 개인 정보 제공을 승인한 것도 아니었죠.[3,4] 저녁에 쉬면서 볼 어린이 영화 한 편을 고르기 위해 스마트 TV에 설치된 앱을 검색하는 동안에도 추적, 데이터 교환, 경매, 리타기팅 사이클은 쉼 없이 이어집니다.[35,36]

Apple이 도입한 개인 정보 보호 기능 및 사용자의 개인 정보 보호를 위한 Apple의 노력에 대해 더 알아보려면 apple.com/kr/privacy를 방문하세요.

Safari가 사용자의 개인 정보를 어떻게 보호하고 있는지 더 알아보려면 Safari 백서를 읽어보세요.

Apple이 사용자의 위치 데이터를 어떻게 보호하고 있는지 더 알아보려면 위치 서비스 백서를 읽어보세요.

Apple의 개인 정보 보호 원칙

Apple은 개인 정보 보호가 모두가 누려야 할 기본적인 인권이라고 믿습니다. 그래서 우리는 네 가지 핵심 개인 정보 보호 원칙을 지침으로 삼아 제품과 서비스를 설계합니다.

데이터 수집 최소화
해당 서비스 제공에 꼭 필요한 최소한의 데이터만 수집합니다.

온디바이스 프로세싱
데이터를 Apple 서버로 보내는 대신 가능한 한 기기 자체에서 처리합니다. 이는 사용자의 개인 정보를 보호하고 데이터 수집을 최소화하기 위한 방법이죠.

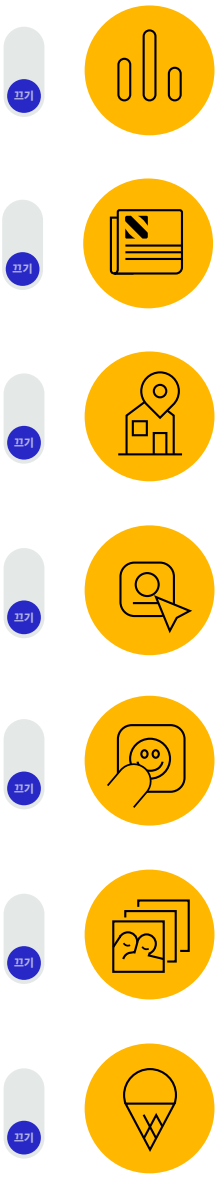
향상된 투명성 및 사용자 권한
어떤 데이터가 공유되었는지, 어디에 사용되었는지를 사용자에게 알리고, 사용자가 직접 자신의 개인 정보에 대한 권한을 행사할 수 있도록 합니다.

보안
데이터 보안 유지를 위해 하드웨어와 소프트웨어가 함께 구동됩니다.

Apple이 이 네 가지 원칙을 통해 이루고자 하는 목표는, 사용자가 자신이 원하는 데이터만을 안전하게 공유하고, 어떤 개인 정보가 공유되고 있는지 이해하고, 자신의 개인 정보를 직접 관리할 수 있도록 하는 것입니다. 지난 20년 동안 Apple이 우리의 모든 기기 및 서비스에 걸쳐 사용자 개인 정보 보호를 위한 혁신을 지속해온 이유가 바로 여기에 있죠. 우리는 기기 자체 인공지능을 포함한 여러 다양한 기능들을 도입함으로써 우리의 앱, 브라우저, 온라인 서비스가 수집하는 데이터의 양을 최소화했습니다. 또한 Apple의 앱 및 서비스 전반에 걸쳐 단 하나의 포괄적 사용자 데이터도 생성하지 않았죠.

Apple의 개인 정보 보호 기능은 존에게 더욱 높은 수준의 투명성 및 개인 데이터 제어 권한을 제공합니다

존과 엠마가 함께 보낸 하루의 이야기는 개인 정보 보호와 관련된 다양한 시사점과 이에 관한 Apple의 해결책을 보여줍니다.



딸과 함께 공원에서 보낼 하루를 계획하는 존

만약 존이 컴퓨터에서 날씨를 확인할 때 Safari를 사용했다면 기본 설정된 **'지능형 추적 방지' 기능이 이 활동에 대한 추적을 막을 수 있었을 겁니다.**

만약 존이 아침에 Apple News 앱을 사용해 뉴스 기사를 읽었다면 **Apple은 존이 누구인지, 무엇을 읽고 있는지 파악하지 않고, 그의 관심사만을 기반으로 기사를 제공했을 겁니다.**

만약 존이 'Apple 지도' 앱을 사용해 교통 정보를 확인했다면 **그의 위치 데이터는 존과는 관련 없는, 정기적으로 초기화되는 무작위 식별자와 연결되었을 겁니다.** 결과적으로 존 이외는 그 누구도 그의 위치를 알지 못했겠죠.

만약 존이 iPhone 사용자였다면 **어떤 앱이 백그라운드에서 그의 위치 정보에 접근하고 있는지 주기적으로 알림을 받았을 겁니다.** 앱에 위치 정보를 공유하기 전에 대략적인 위치 정보만을 공유할지 또는 위치 정보를 한 번만 공유할지도 선택할 수 있었겠죠.

공원으로 향하는 차 안에서 게임을 즐기는 엠마

iPad를 사용했다면 곧 출시될 **'앱 추적 투명성' 기능이 존에게 선택권을 주었을 겁니다.** 덕분에 존은 다른 기업 소유의 여러 앱 및 웹사이트를 넘나드는 엠마의 활동을 이 게임 앱이 추적하도록 허용할지 선택할 수 있었겠죠.

Apple의 SKAdNetwork API를 사용하는 광고 네트워크였다면 존의 기기 역추적에 활용될 수 있는 정보에 액세스하지 않고도 광고의 전반적인 효과를 측정할 수 있었을 겁니다.

공원에서 셀피를 촬영하는 존과 엠마

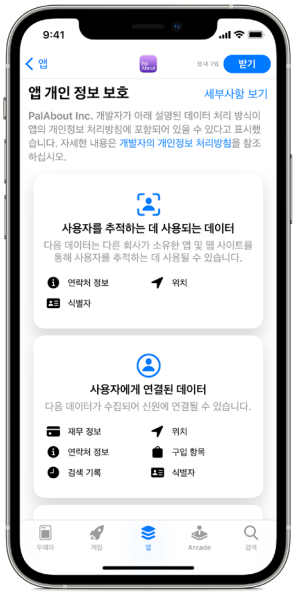
iPhone을 사용했다면 존은 필터 앱이 그의 전체 사진 앨범이 아니라 **앱을 사용해 촬영한 셀피에만 접근할 수 있도록 선택할 수 있었을 겁니다.**

집으로 돌아가는 길에 아이스크림 가게에 들른 존과 엠마

만약 존이 Apple Card로 아이스크림 값을 지불했다면 **은행이 그의 거래 정보를 마케팅 목적으로 사용하는 일은 없었을 겁니다.** 존이 Apple Pay를 사용했다면 Apple은 기기 자체 인공 지능을 활용해 그가 자신의 거래 이력을 iPhone으로 확인할 수 있도록 했을 겁니다. 그 과정에서 존이 어디에서 쇼핑을 했는지, 무엇을 구입했는지, 얼마를 썼는지 등의 정보가 Apple에 공유되는 일은 없죠.

Apple의 제품 및 개인 정보 보호 기능은 존에게 하루 동안 자신의 데이터가 얼마만큼 공유되었고 해당 정보가 어디에 사용되었는지에 관한 더 높은 수준의 투명성과 제어 권한을 제공할 수 있습니다.

App Store의 ‘앱 추적 투명성’ 기능 및 새로운 개인 정보 보호 관련 섹션



Apple은 앱 생태계 내 사용자의 개인 정보를 보호하기 위한 새로운 노력을 진행 중입니다. 점점 더 많은 다양한 주체들이 개인 소비자 데이터에 접근하고, 이를 추적하고, 거래 수단으로 삼음에 따라 Apple은 사용자들에게 향상된 투명성, 가시성, 선택권을 제공하는 것을 목표로 두 가지 기능을 새롭게 선보입니다. 이 기능들은 사용자가 정보에 기반한 의사 결정을 내리고, 자신의 개인 정보에 대한 더 커진 제어 권한을 가질 수 있게 해주죠.

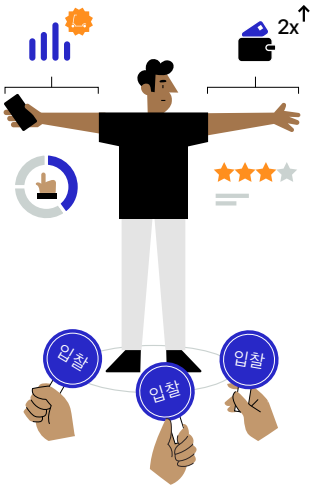
다음번 베타 업데이트와 함께 출시될 앱 추적 투명성 기능은, 앱이 다른 기업 소유의 앱 및 웹사이트에서 사용자의 데이터를 추적하려 할 때 추적 허용 여부를 사용자에게 먼저 승인받도록 하는 기능입니다. 사용자들은 ‘설정’의 하위 메뉴에서 추적 허용을 요청한 앱들을 확인할 수 있으며, 본인의 판단에 따라 허용 여부를 변경할 수 있죠. 이 기능은 올봄 초에 배포 예정인 다음 버전의 iOS 14, iPadOS 14, tvOS 14 전반에 적용될 예정이며, 벌써부터 전 세계 개인 정보 보호 옹호 단체들로부터 지지를 얻고 있습니다. 이 기능을 고안하는 과정에서 Apple은 사용자들에게 더 많은 투명성과 개인 정보 제어 권한을 제공하는 동시에, 광고를 앱 및 웹 콘텐츠 지원을 위한 유효하면서도 유용한 수단으로 유지하기 위한 방안을 고민했습니다. 우리는 Safari의 ‘지능형 추적 방지’ 기능 등 과거 개인 정보 보호 기능 도입 경험을 통해 사용자의 개인 정보 보호를 강화하면서도 광고의 높은 수익성을 유지하는 일이 충분히 가능함을 입증했습니다. 앱 추적 투명성 기능은, 사용자가 본인이 사용할 앱 및 해당 앱에 부여할 개인 정보 접근 승인 내용에 대해 충분한 정보를 기반으로 의사 결정을 내릴 수 있게 해줍니다. 이 기능을 통해 사용자들은 이제 앱에 개인 정보 추적 권한을 부여할지 직접 결정할 수 있죠. 사용자가 신뢰하고, 추적을 허용한 앱의 경우 개발자들은 앞으로도 개인 사용자들의 정보를 추적할 수 있습니다.

앱에 개인 정보 추적을 승인받도록 요구한 것 외에도, 최근 Apple은 투명성 강화를 위해 App Store 제품 페이지에 변화를 주었습니다. 새롭게 도입된 ‘앱이 수집하는 개인 정보’ 섹션을 통해 App Store는 사용자들이 각 앱의 개인 정보 정책을 보다 잘 이해할 수 있도록 돕습니다. 각 앱의 제품 페이지에는 개발자의 개인 정보 처리 방침이 사용자들이 이해하기 쉽도록 요약 제공되어야 합니다. 세부사항 페이지에는 사진, 위치, 연락처 정보 등 해당 앱이 수집하는 데이터의 종류에 관한 정보가 포함되어야 하죠. 이 페이지들은 또한 앱 개발자가 각각의 정보를 어떻게 활용하고 있는지에 대한 세부 정보까지 사용자에게 추가로 제공합니다. 그래서 사용자들은 앱이 자신의 활동을 추적하는 데 활용되고 있는지, 수집된 데이터가 사용자의 정보와 연결되어 있는지 등을 알 수 있죠. Apple을 포함한 모든 앱 개발자들은 자사의 개인 정보 처리 방침에 관한 정보를 직접 제공해야 합니다.

새로운 앱 추적 설정과 App Store 내 제품 페이지에 제공되는 투명성 및 개인 정보 보호 관련 정보는 자신의 사적인 데이터가 어떻게 사용되고 있는지에 대해 사용자가 더욱 쉽게 이해하는 데 도움을 줍니다. 또한 이전에는 음지에서 불투명하게 이루어지던 관행들을 양지로 끌어올리고, 사용자에게 자신의 데이터를 직접 제어할 수 있는 권한을 더 많이 제공하죠.

Apple은 앞으로도 개인 정보 보호를 위한 혁신적인 기술 개발에 매진하는 것은 물론, 당신의 개인 정보를 안전하게 보호할 새로운 방법들을 계속해서 마련해나갈 것입니다.

광고는 어떤 하루를 보내는가



광고 경매

엠마가 존의 태블릿 화면에서 킥보드 광고를 보게 된 것은 우연이 아닙니다. 광고주들은 해당 기기에 자사의 광고를 노출시키기 위해 경매에 참여합니다.[37] 다음은 1초도 안 되는 짧은 시간 동안 해당 기기의 화면에 표시될 광고가 선정되는 과정을 간단히 설명한 것입니다.

1.
엠마가 사용 중인 앱의 개발자가 에드 테크 기업을 고용해 경매를 통해 실시간으로 광고 공간을 확보합니다.[14]

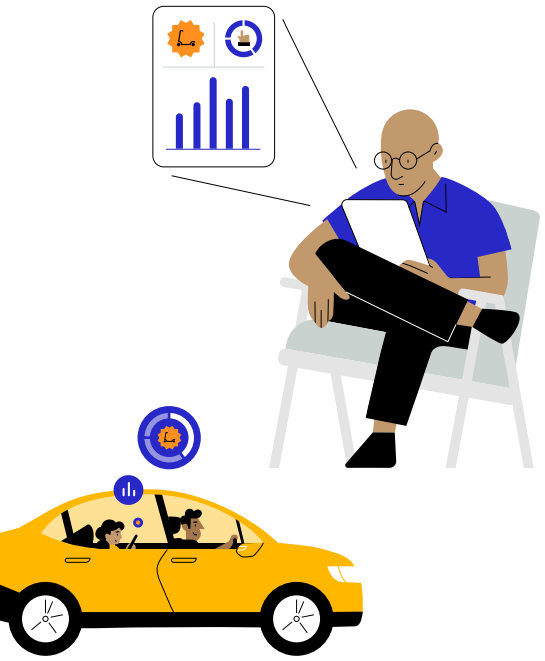
2.
엠마가 앱을 열면 광고 네트워크는 존의 기기가 사용되는 동안 생성된 데이터를 수집합니다. 여기에는 엠마가 사용 중인 앱의 종류, 현재 위치, 존의 광고 식별자가 포함되죠. 또한 존의 광고 식별자 및 사용자 추적을 가능하게 하는 기타 정보에 의존하는 제3자도 데이터 수집에 관여합니다.[3]

3.
광고 네트워크는 수집한 정보 중 일부, 특히 광고 식별자를 잠재 광고주들에게 공유합니다. 보통 광고주들은 입찰에 참여하기 전에 사용자에 관한 가능한 한 많은 정보를 파악하기 위해 애씁니다. 이 과정에서 광고주가 기존에 보유하고 있던 데이터는 물론 추적 및 프로파일링을 통해 수집 및 축적된 사용자 데이터 역시 활용되죠.[3,15]

4.
수집된 데이터가 보여주는 존과 엠마의 특징이 광고주들의 광고 타깃에 부합할수록 더 많은 광고주가 해당 광고 공간 입찰에 참여합니다.[15,38]

5.
최종 낙찰자의 킥보드 광고가 엠마가 사용 중인 기기에 표시됩니다.[14]

1초도 안 되는 시간 동안 경매가 벌어지기 때문에 광고 공간 입찰 및 광고 노출을 위해 구매자와 판매자 모두가 사용자의 개인 정보 수집, 교환 및 사용에 동시에 참여합니다.[14,15]



광고 어트리뷰션

광고가 사용자에게 노출된 이후에도 킥보드 회사의 광고 대행사는 광고가 엠마의 행동에 미친 영향을 측정하고 싶어 합니다. 그 측정 과정을 광고 어트리뷰션이라고 합니다.

어트리뷰션을 하기 위해 광고주는 엠마가 사용 중인 기기의 활동을 추적하여 웹에서, 앱에서, 심지어 오프라인일 때 엠마가 어떤 활동을 하는지 정보를 수집합니다.

- **제품에 관한 광고의 경우,** 광고주는 사용자가 광고 노출 이후 제품 구입을 위해 웹사이트 또는 오프라인 매장을 방문했는지 알아보기 위해 추적을 시도할 수 있습니다.[3]
- **앱에 관한 광고의 경우,** 광고주는 사용자가 해당 앱을 설치했는지 알아보기 위해 추적을 시도할 수 있습니다. 이를 앱 설치 어트리뷰션이라고 합니다.[39]

광고주는 광고의 효과가 더 높은 집단을 상대로 자사의 광고를 '최적화'하기 위해 광고 어트리뷰션을 활용하기도 합니다.[3]

하지만 꼭 광고 어트리뷰션이 필요한 건 아닙니다. 사용자를 추적하지 않고도 특정 집단을 타깃으로 한 광고 캠페인의 효과를 측정할 수 있는 방법도 있죠. Apple은 사용자의 개인 정보를 보호하면서, 동시에 광고 캠페인의 효과도 측정할 수 있는 도구 개발에 매진했습니다.

SKAdNetwork는 앱 관련 광고 노출 이후 해당 앱이 다운로드된 횟수를 광고주에게 알림으로써 광고주가 광고 캠페인의 효과를 측정할 수 있게 해줍니다. 하지만 이 정보에 포함된 사용자 또는 기기 관련 데이터는 공유가 불가능하도록 설계되었기 때문에 광고주가 사용자를 추적할 수 없죠.

Private Click Measurement는 광고주가 iOS 및 iPadOS 14.5용 앱에서 웹사이트 접속 유도 광고의 효과를 측정할 수 있게 해줍니다. 이 측정 과정은 기기 내에서 처리되기 때문에 수집되는 데이터의 양도 최소한으로 유지되죠. 사용자가 앱 내 제품 광고를 클릭하면 Private Click Measurement가 광고주에게 사용자가 해당 광고를 클릭했으며 이와 같은 활동이 웹사이트 방문 또는 웹사이트를 통한 구입 등 특정한 결과로 이어졌다는 사실을 알릴 수 있습니다. 이때에도 어떤 사용자가 해당 광고를 클릭했는지에 관한 정보는 광고주에게 제공되지 않죠.

자주 묻는 질문

'앱에 추적 금지 요청'을 선택한 사용자도 해당 앱의 전체 기능을 온전히 사용할 수 있나요?

그렇습니다. 앱 개발자는 앱의 전체 기능을 사용하려면 개인 정보 추적을 허용하라는 식의 요구를 사용자에게 할 수 없습니다.

식별자는 무엇이고 어떻게 사용되나요?

IDFA, 이메일 주소 등 식별자는 네트워크상에서 특정 기기를 식별하는 데 도움을 줍니다. 이와 같은 식별자들은 또한 광고주가 앱 및 웹사이트에 걸친 사용자 활동에 관한 자세한 프로필을 생성할 수 있게 해줍니다. 사용자의 기기 식별자를 발견하면 이를 사용자의 활동과 연결 지을 수 있도록 말이죠.

IDFA(Identifier For Advertisers)가 무엇인가요?

IDFA는 iOS가 각 기기에 부여하는, 사용자가 제어할 수 있는 식별자입니다. 하드웨어 자체 식별자가 아닌 소프트웨어 기반 식별자로, '앱 추적 투명성' 알림을 받은 사용자가 해당 앱에 대한 IDFA를 차단할 수 있죠. 덕분에 사용자는 IDFA를 기반으로 한 추적을 직접 제어할 수 있습니다.

'앱에 추적 금지 요청'을 선택하면 앱이 개인 정보를 추적하지 않는다고 Apple이 보장할 수 있나요?

IDFA는 종종 개인 정보 추적에 활용됩니다. 하지만 사용자가 '앱에 추적 금지 요청'을 선택할 경우 해당 앱의 개발자는 IDFA에 접근할 수 없죠. 우리는 또한 앱 개발자에게 광고 식별자 접근 권한 문제와는 별개로 사용자의 선택을 존중하도록 요구하고 있습니다. 이 사항은 개발자가 App Store 배포 목적으로 앱을 제출할 때 동의해야 하는 정책에 포함되어 있습니다. 추적을 허용하지 않은 사용자의 개인 정보를 추적하다가 적발될 경우, 우리는 해당 개발자에게 앱 운영 관행을 개선함으로써 사용자의 선택을 존중하도록 요구합니다. 이와 같은 요구를 받아들이지 않을 경우 해당 앱은 App Store에서 퇴출되죠.

개인 소셜 미디어 계정을 사용해 앱에 로그인할 경우 해당 소셜 미디어 기업이 앱 내에서의 나의 활동을 추적할 수 있나요?

해당 앱이 당신의 활동을 추적할 수 있는지 여부는 당신이 해당 앱에 정보 추적을 허용할지 여부에 달려있습니다.
'앱에 추적 금지 요청'을 선택할 경우 해당 앱은 다른 기업 소유의 앱 또는 웹사이트에서 광고를 목적으로 당신의 활동을 추적하거나, 데이터 브로커에게 당신의 정보를 공유해서는 안 됩니다. 즉, 위와 같은 목적으로 당신의 개인 정보가 사용될 경우 앱 개발자들은 당신의 개인 정보를 소셜 미디어 기업에 제공해서는 안 됩니다.

App Store 제품 페이지에 제공되는 개인 정보 보호 관련 정책의 정확성을 보장하기 위해 Apple은 어떤 노력을 하고 있나요?

App Store에 적용되는 '연령 등급' 정책과 마찬가지로, 개발자들은 자사의 개인 정보 처리 방침을 직접 보고합니다. 만일 개발자가 부정확한 정보를 제공한 것으로 파악된 경우, 우리는 해당 개발자와 협업을 통해 정보의 정확성이 지켜지도록 할 것입니다.

데이터 브로커가 무엇인가요?

일반적으로 데이터 브로커는 자사와 직접적인 관계를 맺지 않은 특정 최종 사용자의 개인 정보를 상시적으로 수집, 판매, 라이선싱하거나 제3자에게 제공하는 기업을 말하며, 일부 관할 구역에서는 데이터 브로커의 정의가 법으로 규정되어 있습니다.

Sources

1. Gröne, Florian, Pierre Péladeau, et al., "Tomorrow's data heroes," Strategy+Business, 2020년 2월 19일.

2. Reinsel, David, John Gantz, et al., "The Digitization of the World: From Edge to Core," IDC, 2018년 11월.

3. Competition & Markets Authority, "Online platforms and digital advertising," 2020년 1월 1일.

4. Hitlin, Paul, and Lee Rainie, "Facebook Algorithms and Personal Data," Pew Research Center, 2020년 1월 16일.

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," 2020년 9월 24일.

6. Binns, Reuben, Ulrik Lyngs, et al., "Third Party Track- ing in the Mobile Ecosystem," Proceedings of the 10th ACM Conference on Web Science, 2018년, pp. 23-31.

7. MightySignal, "Most Used SDKs in Top 200 Free iOS Apps," mightysignal.com/top-ios-sdks.

8. State of California Department of Justice, "Data Broker Registry," oag.ca.gov/data-brokers.

9. Acxiom Corporation, 2018 Form 10-K, 2018년 5월 25일 제출, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Reyes, Irwin, Primal Wijesekera, et al., "'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale," Proceedings on Privacy Enhanc- ing Technologies, Vol. 2018년, No. 3, 2018년, pp. 63-83.

11. Edwards, Jim, "Here's The Staggering Number of Ads Facebook Serves On Its Exchange Every Day," Business Insider, 2012년 11월 9일.

12. Kim, Larry, "How Many Ads Does Google Serve In A Day?," Business 2 Community, 2012년 11월 2일.

13. Deighton, John, and Leora Kornfeld, "The Socio- economic Impact of Internet Tracking," Interactive Advertising Bureau, 2020년 2월.

14. Hwang, Tim, Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet, FSG Originals, 2020년 10월 13일.

15. Australian Competition and Consumer Commission, "Digital advertising services inquiry - Interim report," 2020년 12월.

16. Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," The New York Times, 2020년 12월 19일.

17. Nanos, Janelle, "Every step you take: How compa- nies use geolocation data to target you – and everyone around – in ways you're not even aware of," The Boston Globe, 2018년 7월 21일.

18. Vitaldevara, Krish, "Safer and More Transparent Access to User Location," Android Developers Blog, 2020년 2월 19일.

19. Schechner, Sam, and Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook," The Wall Street Journal, 2020년 2월 22일.

20. Facebook for Business, "Measuring Conversions on Facebook, Across Devices and in Mobile Apps," 2014년 8월 14일.

21. Bender, Brad, "New digital innovations to close the loop for advertisers," Google Ads & Commerce Blog, 2016년 9월 26일.

22. Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," 2019년 7월 24일.

23. Chin, Kimberly, "Twitter Could Pay FTC Fine Over Alleged Privacy Violations," The Wall Street Journal, 2020년 8월 3일.

24. Satariano, Adam, "Google Is Fined $57 Million Un- der Europe's Data Privacy Law," The New York Times, 2019년 1월 21일.

25. Schiffer, Zoe, "Period tracking app settles charges it lied to users about privacy," The Verge, 2021년 1월 13일.

26. Thompson, Stuart A., "These Ads Think They Know You," The New York Times, 2020년 4월 30일.

27. Venkatadri, Giridhari, Piotr Sapiezynski, et al., "Au- diting Offline Data Brokers via Facebook's Advertising Platform," The World Wide Web Conference, 2020년, pp. 1920-1930.

28. Leetaru, Kalev, "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong," Forbes, 2018년 4월 5일.

29. Grothaus, Michael, "The top 7 iOS 14 privacy features: What you need to know," Fast Company, 2020년 9월 16일.

30. Germain, Thomas, "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information," Consumer Reports, 2020년 12월 6일.

31. Helm, Burt, "Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism," Fast Company, 2020년 5월 12일.

32. Ramirez, Edith, Julie Brill, et al., "Data Brokers: A Call for Transparency and Accountability," Federal Trade Commission, 2014년 5월.

33. Oracle, "12 Must-Ask Questions to Separate Fact from Fiction," www.oracle.com/a/ocom/docs/idg-12- must-ask-questions-for-identity-vendors.pdf.

34. Hern, Alex, "'Anonymous' browsing data can be easily exposed, researchers reveal," The Guardian, 2017년 8월 1일.

35. Fowler, Geoffrey A., "You watch TV. Your TV watch- es back," The Washington Post2020년 9월 18일.

36. X-Mode, "Data Licensing," xmode.io/data-licensing/.

37. 기기에 등록된 Apple ID 사용자의 연령이 18세 미만인 경우, IDFA 접근이 기본으로 비활성화되며, 해당 기기에 대한 IDFA 접근은 어떤 개발자에게도 승인되지 않습니다.

38. Google Ads Help, "About Smart Bidding," 지원. google.com/google-ads/answer/7065882?hl=en.

39. Litfin, Marne, "What is Mobile ad attribution? An intro- duction to app tracking," Adjust, 2019년 2월 4일.

40. Cox, Joseph, "The IRS Is Being Investigated for Using Location Data Without a Warrant," Vice, 2020년 10월 6일.

41. Cox, Joseph, "How the U.S. Military Buys Location Data from Ordinary Apps," Vice, 2020년 11월 16일.

42. Cox, Joseph, "CBP Bought 'Global' Location Data from Weather and Game Apps," Vice, 2020년 10월 6일.