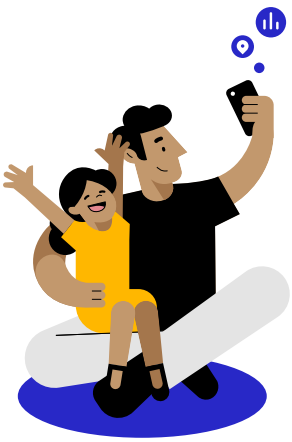


Один день из жизни ваших данных

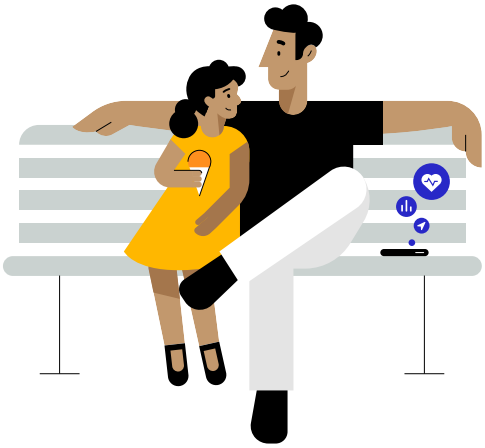
Семейная поездка на детскую площадку

Апрель 2021 г.

«Люди сами знают, какими данными
они готовы делиться. Просто спросите
их об этом. И спрашивайте каждый раз.
Пусть они сами попросят вас прекратить,
если устанут от ваших вопросов. Они должны
точно понимать, что вы собираетесь делать
с их личной информацией».

Стив Джобс

Конференция All Things Digital, 2010 г.



Последние десять лет мы наблюдаем, как крупная и сложно устроенная отрасль собирает всё больше личных данных.[1,2] Сайты, приложения, социальные сети, информационные брокеры и рекламные аналитики объединяются в сложную экосистему, чтобы отслеживать пользователей онлайн и офлайн. Собранные данные анализируются, передаются между участниками этой сети, объединяются и используются в режиме реального времени на аукционах, поддерживая отрасль с доходностью 227 миллиардов долларов в год.[1] Всё это происходит каждый день, а пользователи живут своей жизнью и даже не замечают, что кто-то использует их личные данные.[3,4] Давайте представим, что эта отрасль может узнать про обычного человека, который приятным летним днём отправился на прогулку с дочкой.

Знаете ли вы?

Трекеры встроены в приложения, которыми вы привыкли пользоваться ежедневно: в среднем их шесть на приложение.[3] В большинстве популярных приложений для Android и iOS есть встроенные трекеры.[5,6,7]

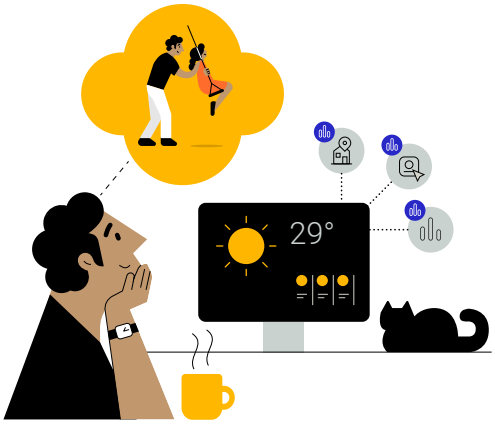
Трекеры часто встраиваются во фрагменты стороннего кода, который разработчики используют для создания нового приложения. Добавляя трекеры, разработчики позволяют сторонним компаниям отслеживать связь между данными, которые собраны из разных приложений, а также между новыми и старыми данными пользователя.

Информационные брокеры собирают, а затем продают, предоставляют по лицензии или передают на других условиях личные данные пользователей, с которыми компания-получатель не взаимодействовала напрямую.[3]

Сотни информационных брокеров собирают данные онлайн и офлайн.[8] Один брокер способен собрать информацию о 700 миллионах человек со всего мира и составить потребительские профили, включающие до 5000 характеристик.[9]

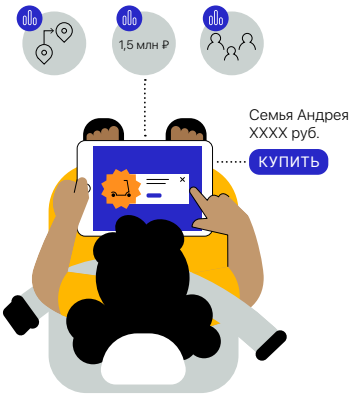
Исследование показало, что почти 20% детских приложений собирают и передают идентифицирующие данные без подтверждённого согласия родителей ребёнка.[10]

Каждый час пользователям показывают миллиарды цифровых объявлений.[11,12,13] За те доли секунды, пока загружается объявление, проводится аукцион, в ходе которого рекламодатели борются за право показать объявление, и чаще всего при этом учитываются личные данные пользователя.[14,15]



Андрей решил сходить с дочкой в парк

Дочке Андрея 7 лет. Её зовут Катя. Сегодня они договорились сходить на прогулку. Утром Андрей включил компьютер, посмотрел погоду, прочитал новости. Проверил пробки в навигаторе на смартфоне и узнал, как проще доехать до детской площадки возле школы, где учится дочка. Пока Андрей с Катей в пути, четыре приложения на телефоне Андрея в фоновом режиме периодически собирают данные о его местоположении.[16,17,18] Затем разработчики извлекают данные с устройства и продают их различным информационным брокерам, о которых Андрей не имеет ни малейшего представления.[16,17] Хотя в приложениях заявлено, что данные о местоположении собираются анонимно, средства отслеживания пользователя позволяют брокерам сопоставить информацию из разных источников.[16,19] Это значит, что любая компания или организация может купить личные данные, собранные в приложениях и на сайтах, и использовать их для создания полного личного профиля, в котором будет, например, информация о том, куда человек ездит каждый день.[3,16]



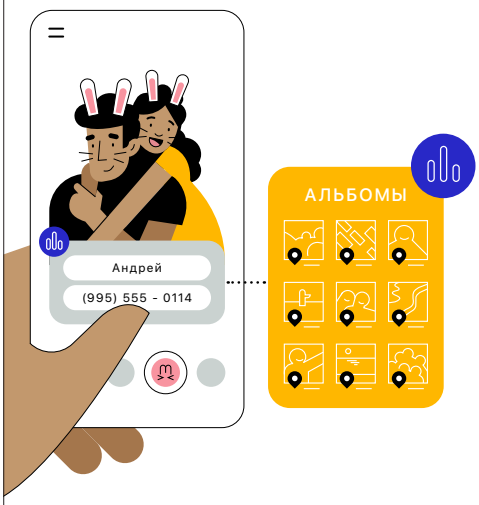
Катя играет по дороге на детскую площадку

По дороге на детскую площадку Андрей разрешил Кате поиграть на планшете. Открыв приложение, Катя видит рекламу самокатов — и это неслучайно. За доли секунды, пока загружалось приложение, был проведён аукцион за право показать рекламное объявление.[14] Через посредников рекламные партнёры компании, торгующей самокатами, узнали, что появилось свободное рекламное место.[15] Используя личные данные Андрея и Кати, они назначили свои ставки за показ объявления.[15] После аукциона рекламные компании продолжили собирать данные. Их интересовало, как Андрей и Катя отреагировали на объявление: нажали на него или нет, решились ли на покупку самоката.[3] Теперь реклама самокатов будет преследовать Андрея и Катю в самых разных приложениях и на сайтах на всех устройствах Андрея.[3,20,21]

Некоторые приложения запрашивают доступ к большему количеству данных, чем им требуется для работы. К примеру, экранной клавиатуре совершенно незачем знать, где вы сейчас находитесь.[5]

Собранные данные могут передаваться в рекламные сети, использоваться для размещения объявлений, атрибуции и измерения показателей. Эти данные могут получить информационные брокеры, частные компании и государственные организации.[3,15,40,41,42] Социальные сети и компании, занимающиеся аналитикой рекламы, уже либо получили, либо уплатили штрафы на миллионы долларов за то, что использовали личные данные не в тех целях, которые были раскрыты пользователю.[22,23,24,25]

Информационные брокеры, используя собранные данные, присваивают пользователям атрибуты и распределяют всех пользователей по крайне узким группам. Например: «хотят похудеть, но всё равно любят выпечку».[26] Впрочем, подобные профили часто оказываются неточными: исследование показало, что более 40% атрибутов присваивается неверно.[27,28]

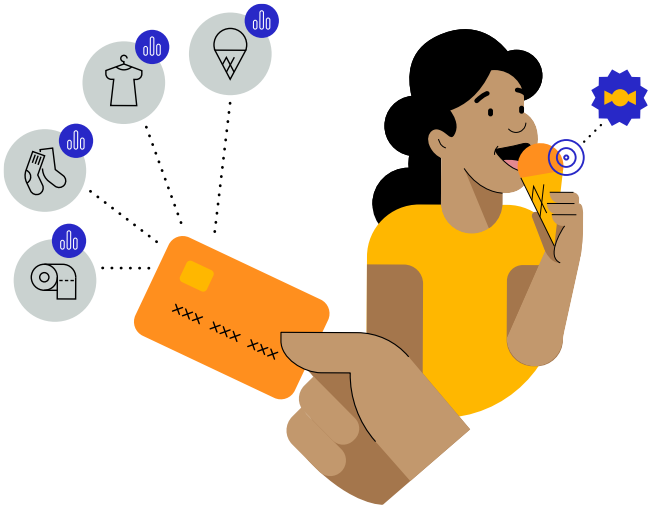


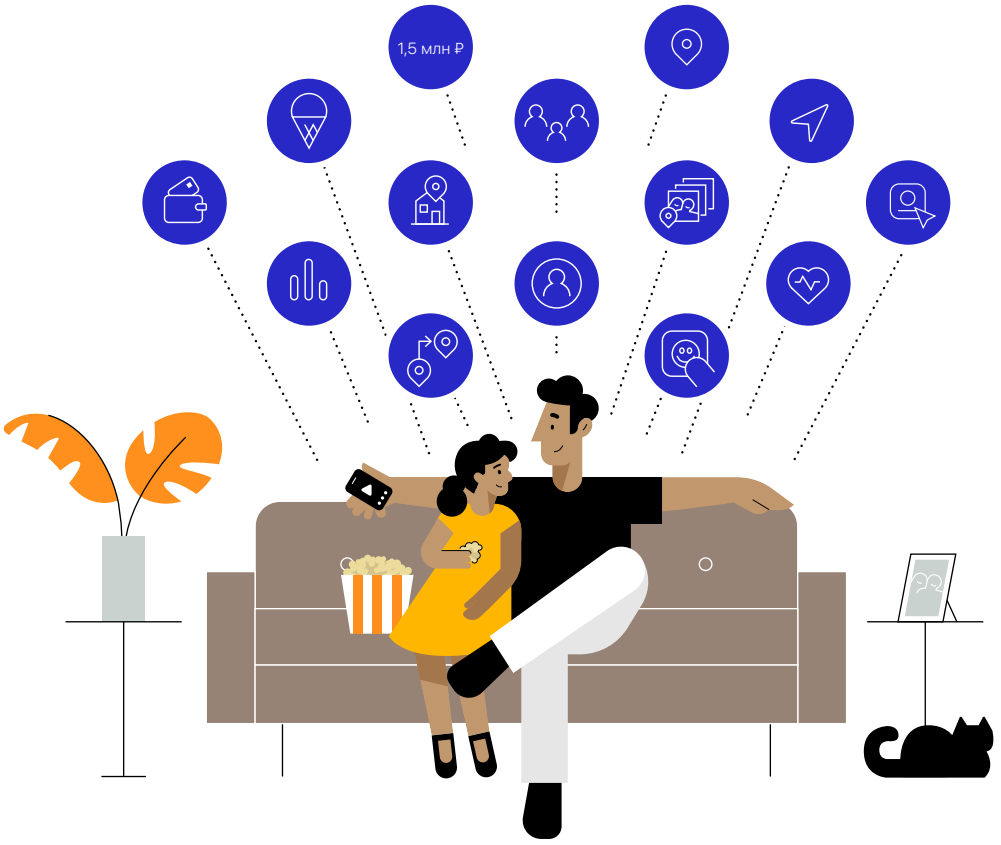
Андрей и Катя делают селфи на детской площадке

На детской площадке Андрей решил сфотографироваться с Катей и сделал селфи. Потом они немного поиграли с фильтрами и остановились на славных кроличьих ушках. Между тем фоторедактор, которым пользовались Андрей и Катя, имеет доступ ко всем фотографиям на устройстве и ко всем метаданным, а не только к последнему селфи.[29,30] Андрей разместил фотографию в социальной сети через приложение, установленное на смартфоне. Приложение сопоставило действия Андрея с уже собранными данными из других приложений — например, с демографической информацией, потребительскими привычками, адресом электронной почты, номером телефона и рекламным идентификатором.[3]

Мороженое по дороге домой

На обратном пути Андрей и Катя завернули в кафе, чтобы съесть по мороженому. Андрей расплатился кредитной картой — и тут же новые данные (адрес кафе и стоимость покупки) попали в его профиль.[31,32,33] Одно из приложений, следящих за перемещениями Андрея, определило, что ещё он заезжал в магазин игрушек.[3] Данные о том, где побывали Андрей и Катя, передаются информационным брокерам. Зная, что в семье есть ребёнок, они показывают на устройствах Андрея персонализированную рекламу сладостей и игрушек из магазина.[17]





В итоге сразу несколько компаний, о которых Андрей никогда не слышал, обновили у себя потребительские профили, добавив в них новую информацию об Андрее и его дочке. Теперь они знают, где живёт Андрей, в какой парк он ездил, на каких сайтах читал новости, какие товары искал, какие рекламные объявления просматривал, что он обычно покупает и в каких магазинах.[3,34] Эти данные были собраны из разных источников, в том числе из приложений, которыми Андрей и Катя пользовались в течение дня. Андрей даже не подозревает, сколько данных о нём было собрано за день. Он не контролирует отслеживание и не давал разрешения на сбор подобных сведений.[3,4] И пока семья выбирает, какое кино они будут смотреть вечером, весь цикл отслеживания, передачи данных, проведения аукционов и изменения настроек таргетинга повторяется снова.[35,36]

Принципы конфиденциальности Apple

Компания Apple считает, что неприкосновенность частной жизни — это фундаментальное право человека. При создании своих продуктов и сервисов мы придерживаемся четырёх основных принципов.

О функциях обеспечения конфиденциальности и о том, что Apple делает для защиты частной жизни, можно узнать на странице apple.com/ru/privacy.

Минимизация сбора данных
Собирается минимум информации — только те данные, которые действительно необходимы для работы приложения или сервиса.

Обработка информации на устройствах
Когда это возможно, данные обрабатываются на устройствах, а не передаются на серверы Apple. Это помогает обеспечивать конфиденциальность и минимизировать сбор данных.

О защите личных данных в Safari подробно рассказано в технической документации к браузеру.

Прозрачность и контроль
Пользователь должен знать, какие данные о нём собираются. Он должен иметь возможность контролировать использование своей личной информации.

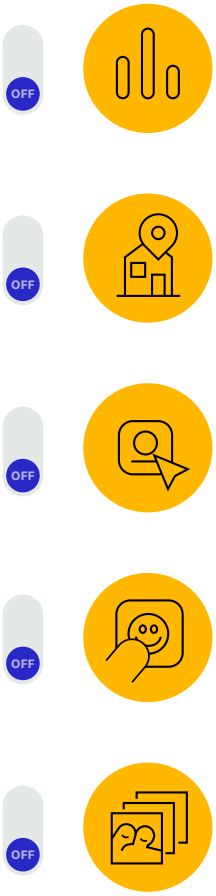
О том, как Apple защищает данные о местоположении пользователя, рассказано в технической документации к службам геолокации.

Безопасность
Устройства и программное обеспечение, работая в тандеме, обеспечивают защиту данных.

Компания Apple сформулировала эти принципы, чтобы у пользователей всегда была возможность самим решать, какие данные предоставлять, и чтобы все процессы были безопасными, понятными и подконтрольными пользователю. Вот почему последние двадцать лет Apple непрерывно совершенствует инструменты защиты личных данных во всех своих продуктах и сервисах. Например, мы используем средства аналитики, которые работают непосредственно на устройствах, и применяем другие способы минимизации сбора данных в наших приложениях, браузерах и онлайн-сервисах. Мы не объединяем данные из разных приложений в общий профиль пользователя.

Функции обеспечения конфиденциальности, встроенные в продукты Apple, позволяют Андрею контролировать свои данные

История Андрея и Кати наглядно указала на проблемы с конфиденциальностью, и Apple работает над их решением.



Андрей решил сходить с дочкой в парк

Если бы Андрей посмотрел погоду в Safari, функция интеллектуальной защиты от сбора данных не позволила бы отследить его действия.

Если бы Андрей проверял пробки в приложении «Карты», данные о его местоположении были бы привязаны к случайному идентификатору, который регулярно обновляется и не связан с личными данными Андрея. И никто, кроме Андрея, не знал бы, где он находится.

iPhone бы периодически напоминал Андрею, какие приложения отслеживают его местоположение в фоновом режиме. И Андрей мог бы решить, какие данные предоставить тому или иному приложению: можно сообщить приблизительное место, а можно разрешить посмотреть данные геолокации только один раз.

Катя играет по дороге на детскую площадку

На iPad скоро будет добавлена функция контроля отслеживания в приложениях. Она позволит Андрею указать, можно ли приложению, в которое играет Катя, отслеживать её действия в приложениях и на сайтах, принадлежащих другим компаниям.

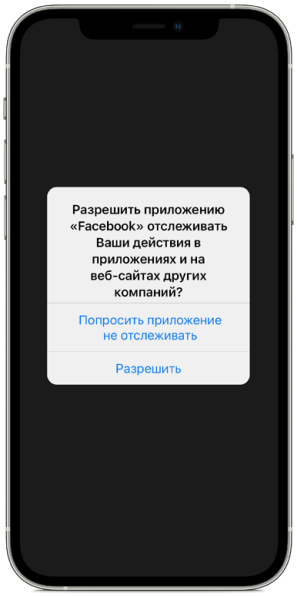
Рекламные сети, использующие SKAdNetwork API от Apple, измеряли бы только общую эффективность объявлений и не имели бы доступа к данным, позволяющим отследить устройство Андрея.

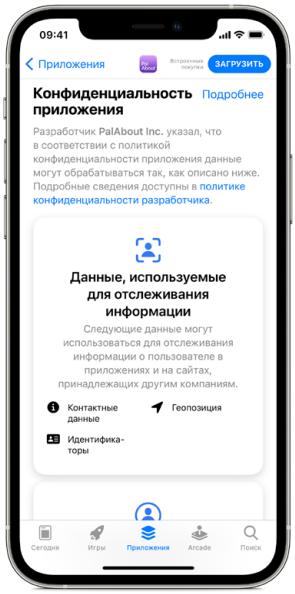
Андрей и Катя делают селфи на детской площадке

На iPhone Андрей мог бы предоставить фоторедактору доступ только к одному селфи, а не ко всей медиатеке.

Продукты Apple со встроенными функциями обеспечения конфиденциальности позволяют Андрею понять и проконтролировать, сколько информации о нём было собрано и как она будет использоваться.

Прозрачность отслеживания в приложениях и новый раздел о конфиденциальности на продуктовых страницах в App Store





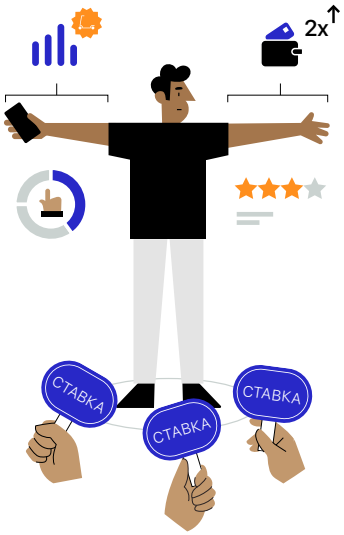
Apple переводит защиту личных данных в экосистеме приложений на новый уровень. Число компаний, которые просматривают, отслеживают и монетизируют личные данные, постоянно растёт. Поэтому Apple вводит две новые функции, с которыми пользователю будет проще понять, кто и для чего собирает его личные данные, и управлять доступом к этой важной информации.

Совсем скоро, с выходом обновлённой бета-версии, вступит в силу требование к прозрачности отслеживания в приложениях. Разработчики смогут собирать информацию о пользователе в сторонних приложениях и на сторонних сайтах, только если он даст на это согласие. В Настройках будет указано, какие приложения запросили разрешение на отслеживание. Отменить разрешение можно будет в любой момент. Требование вступит в силу в начале весны с выпуском обновлений iOS 14, iPadOS 14 и tvOS 14. Его введение уже поддержали защитники неприкосновенности частной жизни по всему миру. Разрабатывая эту функцию, Apple ставила перед собой цель сделать сбор данных более прозрачным и дать пользователям дополнительные средства контроля, при этом не лишая разработчиков возможности получать доход от рекламы. Опыт внедрения других инструментов в этой области, например интеллектуальной защиты от сбора данных в Safari, показал, что они не мешают показу рекламы, но при этом помогают обеспечивать конфиденциальность пользователей. Функция контроля отслеживания в приложениях позволит пользователям более осознанно предоставлять доступ к своим личным данным и выбирать приложения. Теперь пользователь сам будет определять, разрешать приложениям отслеживать его действия или нет. Если пользователь доверяет приложению и даёт ему разрешение на отслеживание, то разработчик сможет продолжить собирать данные пользователя.

В дополнение к требованию запрашивать разрешение на отслеживание, Apple недавно добавила новый раздел на продуктовых страницах в App Store. В нём указываются сведения об обеспечении конфиденциальности в приложениях. На продуктовой странице приложения разработчик должен простым и понятным языком объяснить свою политику в отношении личных данных пользователей. В этом разделе указывается, какие данные собирает приложение (фото, сведения о местоположении, контакты и так далее). И описывается, как именно разработчик будет использовать собранные сведения: например, будут ли отслеживаться действия пользователя и будет ли эта информация привязана к личности пользователя. Все разработчики, включая Apple, обязаны самостоятельно заполнять раздел с информацией о мерах обеспечения конфиденциальности.

Требование к прозрачности отслеживания в приложениях и раздел с информацией о мерах обеспечения конфиденциальности помогут пользователям понять, как используются их личные данные (эта информация долгое время была от них скрыта), и позволят более эффективно контролировать их использование. Apple продолжит разрабатывать технологии для защиты данных и новые способы обеспечения конфиденциальности.

Один день из жизни рекламного объявления



Аукционы

Катя неслучайно увидела рекламу самокатов. Рекламодатели участвуют в аукционах, соревнуясь за право показать своё объявление на том или ином устройстве.[37] Объявление выбирается за долю секунды. Вот как это происходит.

1.
Разработчик приложения, которым пользуется Катя, заключил договор с рекламной компанией, и та выставляет рекламное место в приложении на аукцион, проводящийся в реальном времени.[14]

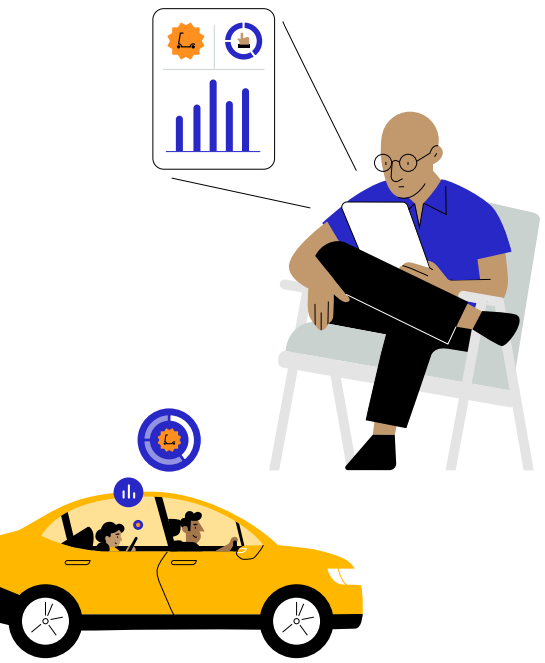
2.
Как только Катя открыла приложение, в рекламную сеть поступили данные об устройстве Андрея (например, о том, какое приложение использует Катя, где она находится, какой рекламный идентификатор присвоен Андрею), сведения из сторонних источников, привязанных к этому рекламному идентификатору, и другая информация, которую можно использовать для отслеживания.[3]

3.
Рекламная сеть передаёт часть полученной информации, в том числе рекламный идентификатор, потенциальным рекламодателям. Перед назначением ставки рекламодатели стараются узнать о пользователе как можно больше: изучают информацию, которую получили сами, а также данные, собранные и агрегированные в ходе отслеживания и составления профиля.[3,15]

4.
Чем точнее Андрей и Катя соответствуют критериям целевой аудитории рекламодателя (это определяется на основе их личных данных), тем выше будет ставка рекламодателя за рекламное место на устройстве Андрея.[15,38]

5.
Объявление, победившее в аукционе (в нашем случае — реклама самокатов), появляется на устройстве, которым пользуется Катя.[14]

Поскольку аукцион проводится за долю секунды, и покупатели, и продавцы собирают, передают друг другу и используют личные данные пользователей для расчёта ставки за показ объявления.[14,15]



Атрибуция

После показа объявления рекламные компании стараются узнать, насколько сильно оно повлияло на поведение пользователя. Этот процесс называется атрибуцией.

С этой целью рекламодатель отслеживает, что происходит на устройстве, которым пользуется Катя: собирает информацию о её действиях в интернете, в приложениях и даже в реальной жизни.

- **В случае с продвижением реального товара рекламодатель выясняет, перешёл ли пользователь на сайт продавца или, может быть, зашёл в магазин, принадлежащий этой компании, и купил там что-то.**[3]
- **Если продвигается приложение, рекламодателя интересует, установил ли пользователь данное приложение.** Это называется атрибуцией установки приложения.[39]

Рекламодатели также используют атрибуцию для оптимизации рекламных кампаний, подбирая группы пользователей, среди которых та или иная реклама будет работать наиболее эффективно.[3]

Но на самом деле необязательно действовать именно так. Рекламодатели могут оценивать эффективность рекламных кампаний для разных аудиторий, не отслеживая отдельных пользователей. Apple разработала инструменты, которые позволяют получить те же результаты без нарушения конфиденциальности.

С SKAdNetwork рекламодателю доступна информация о том, сколько раз приложение было установлено после показа рекламы. Такая статистика вполне позволяет оценить результативность рекламной кампании. При этом данные об отдельных пользователях или их устройствах никуда не передаются, то есть рекламодатель не отслеживает пользователей.

Метод конфиденциального подсчёта кликов, реализованный для приложений в iOS и iPadOS 14.5, позволяет рекламодателям оценивать эффективность объявлений, собирая минимальный необходимый объём данных. Основная информация при этом обрабатывается на устройстве пользователя. Когда пользователь нажимает на рекламу в приложении, браузер, используя метод конфиденциального подсчёта, сообщает об этом рекламодателю и показывает, что именно пользователь сделал на сайте продавца (посмотрел продуктовую страницу, купил товар и так далее). Никакие личные данные рекламодателю не передаются.

Часто задаваемые вопросы

Смогу ли я пользоваться всеми функциями приложения, если попрошу его не отслеживать мои действия?

Да. Разработчик не может ограничить работу приложения на основании того, что пользователь запретил отслеживание.

Что такое идентификаторы и как они используются?

Идентификаторы бывают разными — например, рекламный идентификатор (IDFA) или адрес электронной почты. Они используются, чтобы различать устройства в сети. Они же позволяют рекламодателям составлять подробные профили с перечнем ваших действий в разных приложениях или на сайтах. Данные заносятся в профиль, когда рекламодатель видит ваш идентификатор и может привязать к нему то, что вы делаете.

Что такое рекламный идентификатор (IDFA)?

Это уникальный номер, который система iOS присваивает устройству. Пользователь может контролировать использование IDFA. Поскольку этот идентификатор создаётся программными методами, а не привязывается к устройству, пользователь может запретить определённым приложениям доступ к IDFA. Таким образом, пользователь сам определяет, какие данные будут отслеживаться через рекламный идентификатор.

Может ли Apple гарантировать, что приложение не будет отслеживать мои действия, если я не дам согласия на отслеживание?

Если вы попросите приложение не отслеживать ваши действия, разработчик не узнает рекламный идентификатор устройства (IDFA) — именно он чаще всего используется для отслеживания. Разработчик должен будет уважать ваш выбор и в отношении всех остальных ваших данных. Это требование прописано в правилах, которые разработчики принимают перед публикацией приложений в App Store. Если мы узнаем о нарушениях, мы потребуем их исправить или удалим приложение из нашего магазина.

Если я использую для входа в приложение учётную запись социальной сети, сможет ли она отслеживать мои действия в приложении?

Это зависит от того, разрешили вы приложению отслеживать ваши действия или нет. Если вы выберете вариант «Попросить приложение не отслеживать», то приложение не будет помогать сторонним компаниям отслеживать ваши действия в рекламных целях, а также не будет передавать ваши данные информационным брокерам. То есть приложение не будет делиться вашей личной информацией с социальными сетями, если они намерены использовать её для отслеживания.

Как Apple проверяет достоверность информации о конфиденциальности, размещённой на продуктовых страницах в App Store?

Разработчики сами заполняют раздел о конфиденциальности, так же как и выбирают возрастной рейтинг. Если у нас возникают подозрения, что информация указана некорректно, мы связываемся с разработчиком и просим обновить сведения.

Кто такие информационные брокеры?

Информационный брокер — это компания, которая регулярно собирает, а затем продаёт, предоставляет по лицензии или передаёт на других условиях личные данные пользователей, с которыми компания-получатель не взаимодействовала напрямую. В законодательстве некоторых стран есть официальное определение информационного брокера.

Список источников

1. Gröne, Florian, Pierre Péladeau, et al., "Tomorrow's data heroes," *Strategy+Business*, February 19, 2019.

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

3. Competition & Markets Authority, "Online platforms and digital advertising," July 1, 2020.

4. Hitlin, Paul, and Lee Rainie, "Facebook Algorithms and Personal Data," *Pew Research Center*, January 16, 2019.

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020.

6. Binns, Reuben, Ulrik Lyngs, et al., "Third Party Tracking in the Mobile Ecosystem," *Proceedings of the 10th ACM Conference on Web Science*, 2018, 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, filed May 25, 2018, 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 Enhancing Technologies*, Vol. 2018, No. 3, 2018, pp. 63-83.

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

12. Kim, Larry, "How Many Ads Does Google Serve In A Day?," *Business 2 Community*, November 2, 2012.

13. Deighton, John, and Leora Kornfeld, "The Socioeconomic Impact of Internet Tracking," *Interactive Advertising Bureau*, February 2020.

14. Hwang, Tim, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*, FSG Originals, October 13, 2020.

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

16. Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, December 19, 2019.

17. Nanos, Janelle, "Every step you take: How companies use geolocation data to target you – and everyone around – in ways you're not even aware of," *The Boston Globe*, July 21, 2018.

18. Vitaldevara, Krish, "Safer and More Transparent Access to User Location," *Android Developers Blog*, February 19, 2020.

19. Schechner, Sam, and Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook," *The Wall Street Journal*, February 22, 2019.

20. Facebook for Business, "Measuring Conversions on Facebook, Across Devices and in Mobile Apps," August 14, 2014.

21. Bender, Brad, "New digital innovations to close the loop for advertisers," *Google Ads & Commerce Blog*, September 26, 2016.

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

23. Chin, Kimberly, "Twitter Could Pay FTC Fine Over Alleged Privacy Violations," *The Wall Street Journal*, August 3, 2020.

24. Satariano, Adam, "Google Is Fined $57 Million Under Europe's Data Privacy Law," *The New York Times*, January 21, 2019.

25. Schiffer, Zoe, "Period tracking app settles charges it lied to users about privacy," *The Verge*, January 13, 2021.

26. Thompson, Stuart A., "These Ads Think They Know You," *The New York Times*, April 30, 2019.

27. Venkatadri, Giridhari, Piotr Sapiezynski, et al., "Auditing Offline Data Brokers via Facebook's Advertising Platform," *The World Wide Web Conference*, 2019, pp. 1920-1930.

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

29. Grothaus, Michael, "The top 7 iOS 14 privacy features: What you need to know," *Fast Company*, September 16, 2020.

30. Germain, Thomas, "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information," *Consumer Reports*, December 6, 2019.

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

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

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*, August 1, 2017.

35. Fowler, Geoffrey A., "You watch TV. Your TV watches back," *The Washington Post*, September 18, 2019.

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

37. If the user age associated with the Apple ID registered to a device is under 18, IDFA access is disabled by default, and cannot be granted to any developer.

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

39. Litfin, Marne, "What is Mobile ad attribution? An introduction to app tracking," *Adjust*, February 4, 2019.

40. Cox, Joseph, "The IRS Is Being Investigated for Using Location Data Without a Warrant," *Vice*, October 6, 2020.

41. Cox, Joseph, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020.

42. Cox, Joseph, "CBP Bought 'Global' Location Data from Weather and Game Apps," *Vice*, October 6, 2020.