CIS / № 1 (11) / 2020 / www.cismag.ru

Сервисы Google и Privacy

«...знаете ли: лучше быть живым параноиком, чем мертвецом, который ждал от жизни только приятных неожиданностей...»

Макс Фрай

В современном мире всё чаще и чаще мы сталкиваемся с тем, что наша информация нам не принадлежит. Увы, но стоит признать, что понятия «тайна личной жизни» больше не существует. Можно ли всё же что-то защитить? Думаю, нет, но стоит попробовать. В данной статье мы рассмотрим можно ли что-то предпринять, чтобы сделать ваши данные всё же более защищёнными.

О том, что компания Google собирает данные о нас, мы давно знаем и свыклись с этим. Стоит отметить, что то, что о вас знает Google, – намного больше, чем то, что собирает о вас Android. Почему? А всё просто. Ведь мы используем сервисы Google не только на смартфонах под управлением Android, но и на ПК под управлением Windows, и на смартфонах под управлением iOS. Вспомните: карты Google, браузер Google Chrome и так далее.

Но всё же, что собирает о вас Google? Для того чтобы увидеть это, следует зайти по адресу https://myaccount.google.com. При этом вам потребуется войти в свой аккаунт (рис. 1).

На данной странице вы можете не только настроить конфиденциальность ваших данных, но и узнать какие данные хранятся в аккаунте.

Конфиденциальность и персонализация

Проверка настроек конфиденциальности

Настройки конфиденциальности мы начнём с **Проверки настроек конфиденциальности (рис. 2).**

Если вы включите функцию «История приложений и веб-поиска» – в аккаунте Google будут сохраняться сведения о ваших поисковых запросах и действиях в других сервисах Google. Эти данные позволяют быстрее находить актуальный контент и получать более точные рекомендации.

Учтите, данная опция включена по умолчанию. Но стоит отметить, что вы всегда можете отключить историю приложений и веб-поиска или удалить информацию о своих действиях.

Примечание. Если вы используете **корпоративный аккаунт или выданный вам в учебном заведении, то** включить историю приложений и веб-поиска может только администратор.

История местоположений

В Истории местоположений хранятся данные о том, где вы были со своими устройствами, на которых:

- Выполнен вход в аккаунт Google
- Включена история местоположений
- Разрешена отправка геоданных

С одной стороны, если история включена – вы можете получать дополнительные возможности в следующих сервисах:

- Персонализированные карты
- Рекомендации с учётом тех мест, которые вы уже посетили
- Помощь в розыске своего смартфона
- Сведения о пробках на дороге
- Актуальные рекламные объявления

Вместе с тем необходимо понимать, что в случае хищения вашего смартфона или получения доступа к данным о местоположении все ваши передвижения станут доступными сторонним лицам. А если учесть, что люди в большинстве случаев используют один и тот же маршрут…

По умолчанию история местоположений отключена. Кроме того, запись маршрутов можно приостановить в разделе **Отслеживание действий**.

Однако если вы думаете, что, отключив историю местоположений, вы сумеете сохранить приватность, то, увы, это не правда.

Как говорится в сообщении Associated Press (AP), Google записывает местоположения пользователей, даже когда они не просят об этом.

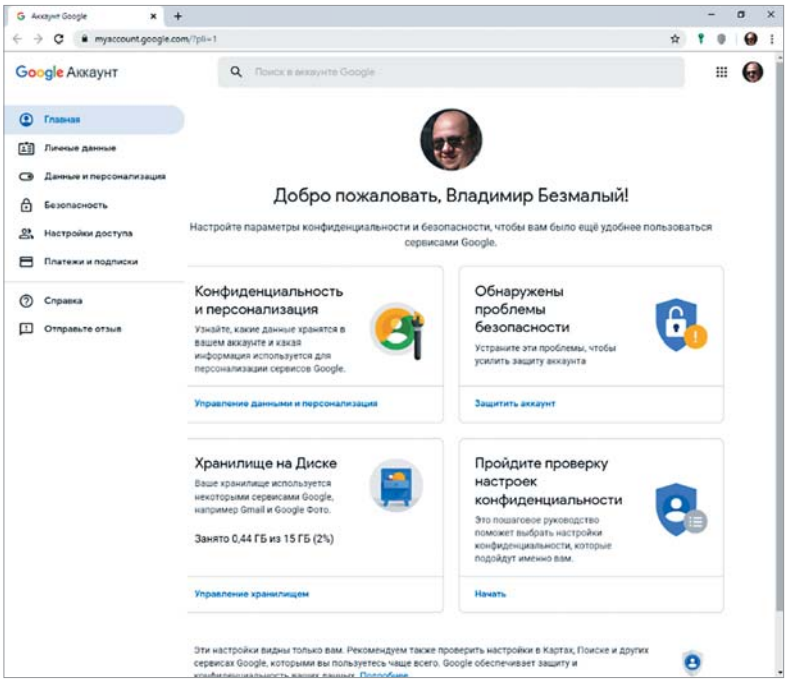

Рисунок 1. Настройка конфиденциальности

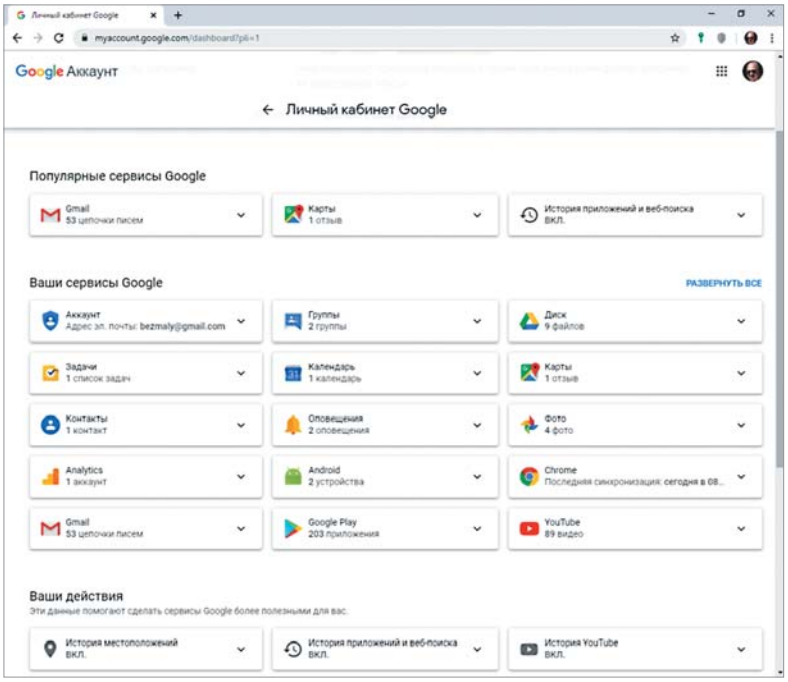

Рисунок 2. Личный кабинет

Эта проблема может затронуть до двух миллиардов устройств Android и Apple, которые используют Google для карт или поиска.

Исследование, проведённое научными сотрудниками из Принстонского университета, показало, что местонахождение пользователей регистрируется даже тогда, когда история местоположений была отключена.

Например:

- Google хранит снимок вашего местоположения при открытии приложения Карты

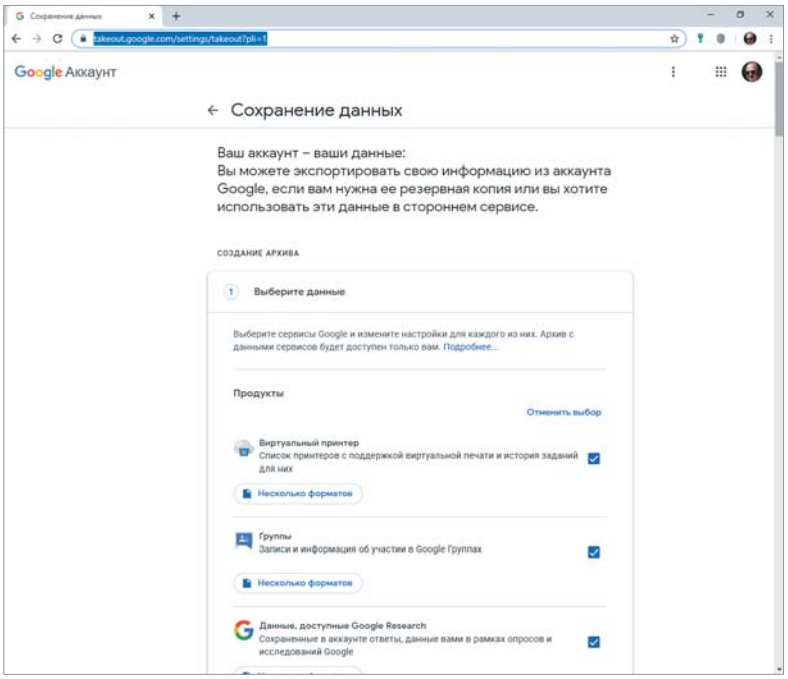

Рисунок 3. Сохранение данных

- Автоматические обновления погоды на телефонах Android точно указывают, где находится пользователь
- Поиски, которые не имеют никакого отношения к местоположению, точно определяют долготу и широту пользователей

Чтобы проиллюстрировать влияние этих маркеров местоположения, AP создала визуальную карту, показывающую движения исследователя из Принстона Гунеса Акара, который использовал телефон Android с отключённой историей местоположений.

Карта показала, что его поезд ездит по Нью-Йорку, а также он сам посещает парк Хай Лайн, рынок Челси, Центральный парк и Гарлем. Это также показало его домашний адрес.

Чтобы Google не сохранял эти маркеры местоположения, пользователи должны отключить другой параметр, который называется «Активность в Интернете и приложениях», который включён по умолчанию и не содержит данных о местоположении.

«Можно подумать, что, если вы скажете Google, что не хотите отслеживать своё местоположение, отключив опцию «История местоположений», это помешает интернет-гиганту хранить данные о вашем местоположении», – пишет исследователь блога Грэм Клули в своём блоге.

После своего исследования **AP создала руководство,** чтобы показать пользователям, как удалять данные о местоположении.

Следует учесть, что с 2014 года Google позволяет рекламодателям отслеживать эффективность онлайн-рекламы с помощью функции, основанной на данных о результатах, которая опирается на историю местоположений.

Независимое тестирование AP подтвердило, что iPhone работает аналогично при использовании приложений Google.

Данные о местоположении, собранные Google, можно найти на myactivity.google.com, но, как указывает точка *доступа,* эта информация разбросана по разным заголовкам, часто не связанным с местоположением.

Чтобы было ясно, Google не занимается незаконным сбором данных о местоположении, но запутывает свои политики в отношении данных о местоположении и собирает данные с помощью функций, которые не содержат информацию о местоположении. Многие люди могут не знать, что эти функции Google вообще включены, так как это настройка по умолчанию.

Единственное упоминание Google о том, что он может продолжать сохранять некоторые данные о местоположении, появляется во всплывающем окне, которое отображается, когда история местоположений отключена в настройках учётной записи Google. В этом всплывающем окне указывается, что «некоторые данные о местоположении могут быть сохранены как часть вашей деятельности в других службах Google, таких как Поиск и Карты».

На iPhone, когда «Журнал местоположений» отключён с помощью настроек в приложениях Google, говорится следующее: «Ни одно из ваших приложений Google не сможет сохранять данные о местоположении в Журнале местоположений». Как указывает AP, это утверждение верно, но вводит в заблуждение, потому что, хотя данные о местоположении не хранятся в истории местоположений, они всё ещё хранятся в разделе «Моя активность».

Информация о местоположении, хранящаяся в разделе «Моя активность», используется для таргетинга объявлений.

Чтобы запретить Google собирать какие-либо данные о местоположении, необходимо отключить «Активность в Интернете и приложениях» и «История местоположений», что можно сделать через пользовательские настройки учётной записи Google. На устройствах iOS неиспользование приложений Google и отключение служб определения местоположения для приложений Google также является эффективным способом предотвращения сбора данных о местоположении.

Для чего Google отслеживает ваше местоположение?

Чтобы лучше вас обслуживать:

- Google / Apple Maps, навигация
- Гораздо более релевантные результаты поиска

• Найти мой телефон / Найти моё устройство

Удобство:

• Знаете, как работает этот ресторан в это время дня или прямо сейчас
• Внутренняя навигация
• Чтобы продать рекламу

Основной источник дохода Google – объявления на основе местоположения (рис. 3).

Кроме того, не стоит забывать о таком сервисе, как Sensorvault.

Sensorvault

В процессе расследования различных преступлений полиция обращается к базе Sensorvault, принадлежащей Google, чтобы отследить местоположение и перемещение смартфонов.

Sensorvault содержит записи геолокации сотен миллионов мобильных устройств по всему миру. Она собирает соответствующую информацию, которую передают продукты Google, чтобы лучше понимать, какую рекламу отображать пользователям и как эта реклама работает.

Как передаёт The New York Times, за последние шесть месяцев подобные запросы резко увечились в количестве – стало приходить по 180 запросов за одну неделю. Сама Google отказалась предоставить развёрнутые данные относительно Sensorvault, однако заявила, что ограничила количество информации, которую предоставляет правоохранительным органам.

Благодаря Sensorvault полиция может отследить местоположение смартфона в определнной местности, а также получить информацию о том, в течение какого времени устройство находилось в этом месте.

Google: источники данных о местоположении

История местоположения: извлечение из облака, online интерфейс. Стоит отметить, что данных о местоположении чрезвычайно много.

Где они хранятся?

Хранятся в облаке (Google Account). При этом нужно учесть, что облако содержит намного больше информации, чем устройство.

Откуда их извлекают?

• Google Maps и My Places
• Фотографии: локальные (извлекаемые из устройства), извлекаемые из Google Photos
• Системные журналы: local (требуется root)
• Данные приложений: local (требуется root), cloud backups (ограниченно)

Как остановить отслеживание вашего местоположения

• Для любого устройства:
  - откройте веб-браузер, перейдите на myactivity.google.com, выберите «Элементы управления активностью» в раскрывающемся меню вверху слева и отключите «Активность в Интернете и приложениях» и «История местоположений»
• Для устройств Android:
  - Перейдите прямо к настройке «Безопасность и местоположение», прокрутите вниз до «Конфиденциальность» и нажмите «Местоположение». Теперь вы можете отключить его для всего устройства
  - Вы также можете использовать «Разрешения на уровне приложений», чтобы отключить доступ к различным приложениям
• Для устройств iOS:
  - если вы используете Карты Google, перейдите в *«Настройки»* → *«Конфиденциальность»* и установите для своего местоположения значение «Во время использования» приложения. Это предотвратит доступ приложения к вашему местоположению, когда оно не активно

История поиска YouTube

Используется как YouTube, так и другими сервисами. Вы можете как удалять историю вручную, так и автоматически через 3 месяца или 18 месяцев (по выбору).

История просмотров YouTube

Вы можете как удалять историю вручную, так и автоматически через 3 месяца или 18 месяцев (по выбору).

Однако если вы думаете, что это всё, вы ошибаетесь. На самом деле следить за вами можно с помощью использования идентификаторов устройств на Android. Поговорим о том, как ими злоупотребляют приложения, чтобы больше зарабатывать на рекламе.

Как приложения зарабатывают на рекламе

Для того, чтобы маркетологи могли составить на вас детальное досье и показать вам персонализированную рекламу, они собирают информацию о вас с помощью мобильных приложений. При этом отправляется даже та информация, использовать которую в рекламных целях Google не разрешает.

Какая информация позволяет отследить ваше Android-устройство

Что могут рассказать приложения рекламной сети о вашем устройстве? В первую очередь то, что они там установлены. Фактически, получив подобную информацию, можно сделать вывод о том, чем вы интересуетесь и какие объявления могут быть вам интересны. Например, если вы пользуетесь селфи-камерой, Instagram и Snapchat – вам покажут приложения с фильтрами и эффектами для фото.

Как убедиться, что то или иное приложение установлено именно на вашем устройстве? Для этого используются специальные коды-

идентификаторы. Как правило, их у смартфона, планшета и любого другого гаджета несколько, и большинство из них придуманы не для рекламы.

Например, уникальный номер IMEI нужен, чтобы распознавать ваш телефон в сотовых сетях и, например, блокировать краденые устройства. А при помощи серийного номера можно определить все гаджеты серии, в которых обнаружен брак, и отозвать их из магазинов.

Ещё один уникальный идентификатор – MAC-адрес – нужен для подключения устройства к сети, а заодно может быть использован, чтобы ограничить набор гаджетов, которые имеют право подключаться к вашему домашнему Wi-Fi. Наконец, Android ID (он же SSAID) разработчики приложений используют, чтобы продавать лицензии на ограниченное количество копий для платных версий своих продуктов.

Теоретически изменить эти номера можно, но стоит помнить, что для этого нужны root-права. А в некоторых странах смена IMEI запрещена законом.

Сменить Android ID проще – достаточно сбросить смартфон или планшет до заводских настроек. Но ведь потом придётся заново задавать все параметры, устанавливать приложения… Желающих это делать совсем не много.

Есть ли выход?

Ещё в 2013 году компания Google ввела специальный рекламный идентификатор. Его задают сервисы Google Play, и пользователь в любой момент может его сбросить и создать новый. Делается это в меню *Настройки → Google → Реклама → Сброс рекламного идентификатора*. С одной стороны, такой идентификатор позволяет рекламным сетям отслеживать привычки и увлечения владельцев устройств. С другой – если же хочется избавиться от слежки рекламщиков, вы можете в любой момент без лишних трудностей его сбросить.

По правилам магазина Google Play, в рекламных целях можно использовать только этот идентификатор. Площадка не запрещает связывать его с другими ID, но для этого приложению нужно получить согласие пользователя.

В теории это должно работать так: если вам нравится реклама по интересам, то вы не трогаете рекламный идентификатор и можете даже разрешить приложениям объединять его с чем угодно. Если же нет, то вы запрещаете связывать эту метку с другими и периодически сбрасываете её, таким образом отвязывая своё устройство от собранного на него досье.

Увы, в действительности всё несколько иначе. По правилам Google Play, в рекламных целях можно использовать только этот идентификатор. Приложение может связывать его с другими ID, но только с явного согласия пользователя.

Рекламный идентификатор – реальность

Как обнаружил исследователь Серж Эгельман (Serge Egelman), более 70% приложений в Google Play используют хотя бы один дополнительный идентификатор без предупреждения. Некоторые из них, например 3D Bowling, Clean Master и CamScanner, скачали многие миллионы человек.

Чаще всего в ход идёт Android ID, хотя IMEI, MAC-адреса и серийные номера разработчики тоже задействуют. Некоторые приложения отправляют партнёрам сразу три идентификатора и более. Так, игра 3D Bowling (видимо, для верности) использует и рекламный идентификатор, и IMEI, и Android ID.

Такой подход делает саму идею специального рекламного идентификатора бессмысленной. Даже если вы против слежки и регулярно сбрасываете его, маркетологи при помощи более стабильной метки легко привяжут к существующему профилю новый идентификатор.

Вместе с тем, начиная с Android Oreo, для каждого приложения задаётся свой Android ID. Однако для IMEI, серийных номеров и MAC-адресов ввести такую защиту нельзя.

Что же делать?

- Регулярно удаляйте программы, которыми вы не пользуетесь: чем меньше на устройстве приложений, тем меньше данных получат рекламные сети
- Не давайте оставшимся программам лишних разрешений. Это не избавит вас от слежки полностью, но не позволит тем же играм отправлять IMEI кому попало. На всякий случай: за этот идентификатор отвечает разрешение «Телефон». Оно же позволит приложению узнать ваш мобильный номер, посмотреть историю вызовов, позвонить (за ваш счёт, разумеется) и многое другое, так что выдавать его в принципе не рекомендуется.

Заключение

Как видно из приведённого в статье материала, вы можете настроить удаление хранимых данных, однако никто не может гарантировать что ваши данные не будут храниться или удаляться. Ведь основной бизнес Google – это торговля данными для показа рекламы.

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности