Хакер - Досмотр файлов: как защитить свои данные на смартфоне при пересечении границы
nopaywall

https://t.me/nopaywall
Олег Афонин.

Содержание статьи

Мы часто пишем про абстрактные способы взлома и защиты мобильных устройств. При этом подразумевается, что защита должна быть, а противостоим мы некоему воображаемому злоумышленнику. Но что, если защищаться приходится не от сферического воришки в вакууме, а от вполне конкретного офицера-пограничника, который настойчиво требует предоставить ему полный доступ в устройство?
Вопрос далеко не праздный: количество подобных требований со стороны американских пограничников растет в геометрической прогрессии. Дурной пример заразителен, и практика проверок на границе может быть принята на вооружение в других странах (а в России в свете последних законодательных инициатив и вовсе сам бог велел).
Как себя вести в такой ситуации, как защитить свою информацию и стоит ли это делать вообще — тема сегодняшней статьи.

Что происходит на границе?

Несколько лет назад в Соединенных Штатах был принят закон, позволяющий пограничникам производить досмотр информации в устройствах путешественников, желающих пересечь американскую границу. Изначально этот закон использовался только для ноутбуков, флешек и прочих носителей информации. С появлением смартфонов действие закона распространили и на них.
Количество досмотров цифровых устройств быстро растет. Так, если в 2015 году было досмотрено порядка 8,5 тысячи устройств, то уже в 2016-м их число возросло до 19 тысяч. Прогноз на 2017 год — 29 тысяч досмотров. Цифра впечатляет, но вероятность попасть на такой досмотр у среднего путешественника все еще невелика и составляет лишь восемь шансов из 100 тысяч.

Что можно и что нельзя делать

Сразу определимся с тем, чего делать не стоит. Нельзя лгать и активно противодействовать пограничнику. В США это уголовное преступление, и последствия могут быть самыми печальными. (Вариант «забыл пароль от смартфона» не годится: будешь сидеть в камере, пока не вспомнишь.) Нельзя полагаться на то, что пограничник о чем-то не спросит (к примеру, если ты создал резервную копию устройства и сохранил ее на флешку с паролем, у тебя вполне могут попросить пароль от бэкапа). Нельзя полагаться на то, что пограничник чего-то не найдет: все эти скрытые контейнеры и приложения, шифрующие фотографии, — откровенный детский сад, относительно неплохо защищающий от родителей, которым в руки попал… надеюсь, что не твой смартфон. Опытного пограничника подобные трюки, наоборот, могут здорово насторожить и настроить против тебя, а твоя нервозность во время досмотра — вызвать дополнительные подозрения. Давай не будем играть в бирюльки и поговорим о том, что действительно можно сделать для защиты твоей персональной информации.

Переходим к защите

Самое важное в защите собственной информации — подготовиться заранее. Прохождение пограничного контроля всегда стресс, а стресс — не лучший советчик в принятии рациональных решений. Тебе нужно будет продумать следующие вещи.
Собираешься ли ты защищать свои данные в принципе? Многие вообще не используют пароли блокировки, игнорируют датчик отпечатков пальцев, отключают встроенное шифрование. Если ты один из таких пользователей, то, вероятно, скрывать тебе нечего и сопротивляться просьбам пограничника нет никакого смысла: на следующем шаге устройство будет конфисковано, разблокировано и исследовано, но уже без твоего участия. А вот на тебя упадут все возможные негативные последствия.
О последствиях. Если ты не собираешься разблокировать телефон по «просьбе» пограничника — насколько ты готов к возможным неприятностям (отказ во въезде в страну, задержание, пропуск трансфера)? Прими решение заранее.
Если ты все-таки ценишь свою частную жизнь, определи загодя, какие именно виды информации ты хотел бы защитить. Фотографии? Известен не один и не два случая, когда люди получали вполне реальные сроки за фото или видео купания младенца. Постинги в социальных сетях? Скорее всего, пограничников они заинтересуют лишь для того, чтобы убедиться, что ты не боевик, не камикадзе и не торгуешь спайсом. История поисковых запросов и браузера? Лично я не хотел бы, чтобы кто-то получил доступ к этой информации. А что насчет паролей? Готов ли ты к тому, что твои сохраненные в браузере логины и пароли ко всему на свете будут храниться неизвестно где неограниченное время, использоваться неизвестно кем и в неизвестных целях? Вспомним еще историю местоположения, список звонков, сообщений и контактов, доступ к фотографиям и документам, синхронизированным с твоим домашним компьютером через облачные сервисы OneDrive, Dropbox или Google Drive.
Отдельным абзацем пустим данные работодателя, особенно если у него есть собственные требования к безопасности. Здесь могут помочь политики безопасности, установленные на устройство через Exchange и другие подобные системы MDM.
Определившись с тем, что именно ты собираешься защищать, можно переходить собственно к техническим мерам.

Технические методы защиты

Прежде чем мы приступим к техническим методам защиты, разберемся сперва с устройством. Кстати, даже если у тебя смартфон на Android — не пропускай раздел про iPhone, там обсуждаются многие базовые вещи, общие для обеих платформ.

Защищаем iPhone

В целом защитить iPhone будет проще, чем смартфон на Android. Но обо всем по порядку.
Ты уже определился со стратегией? Если ты собираешься грудью стать на защиту своих данных, у тебя есть несколько вариантов.
Во-первых, ты можешь задать длинный (состоящий из шести цифр или буквенно-цифровой) пароль, после чего просто выключить телефон. Вскрыть его будет совершенно невозможно, пока ты не сообщишь этот пароль. А вот если твой iPhone оборудован датчиком отпечатков пальцев и ты забыл выключить телефон перед пересечением границы, то пограничнику будет достаточно приказать тебе приложить палец к сканеру, чтобы разблокировать устройство. Такой способ разблокирования устройств не требует каких-то особых ордеров или разрешений со стороны правоохранительных органов. Поэтому — выключи телефон.

Дотошные погранцы

Логичный вопрос: что мешает пограничникам запереть тебя и не выпускать, пока ты не выдашь (вспомнишь, введешь) пароль разблокировки? С одной стороны, вроде бы ничто не мешает: в известном случае сотрудника NASA, американского, кстати, гражданина, пограничники задержали и «прессовали» (цитата) до тех пор, пока он не выдал PIN-код от смартфона. С другой — такие случаи чрезвычайно редки, они скорее исключение, чем правило. Опять же, в законодательстве США на сегодняшний день есть широченная «серая зона», в рамках которой, с одной стороны, у пограничника есть широчайшие полномочия, но с другой — воспользоваться ими он может только при наличии «обоснованных подозрений».
Пограничник может «попросить» тебя разблокировать телефон паролем. Если это именно просьба (request в официальной терминологии), то у тебя есть право вежливо отказаться. Запирать тебя никто не станет (но могут возникнуть другие последствия, о них мы уже говорили). А вот если это приказ (order), то выбора у тебя не будет. Но именно приказать ввести или сообщить пароль пограничник может только при наличии «обоснованных подозрений», в исключительных случаях. В то же время разблокировку по отпечатку и пограничники, и полиция могут (тут снова «серая зона») проводить в оперативном порядке. Иными словами, врать нельзя, сопротивление тоже бесполезно.
Что остается?
Во-вторых, перед поездкой ты можешь сбросить устройство и настроить его заново, используя свежий Apple ID. Такое устройство не стыдно предъявить пограничнику. После пересечения границы просто подключишься к Wi-Fi, сбросишь телефон еще раз и восстановишься из облачного бэкапа (разумеется, такой бэкап у тебя должен в принципе иметься, а беспроводное соединение должно быть быстрым, стабильным и разрешать

передачу нескольких гигабайт данных). Обрати внимание на важный момент с двухфакторной аутентификацией: для авторизации в собственный Apple ID тебе придется иметь при себе второй фактор аутентификации (например, SIM-карту с доверенным телефонным номером, на который ты сможешь получить SMS с одноразовым кодом). Если ты не продумаешь это заранее, ты можешь оказаться отрезанным от собственной учетной записи и данных в iCloud.

Если ты берешь с собой компьютер, то бэкап можно создать и локально, на скрытом контейнере в формате TrueCrypt или одного из его «наследников». Сам контейнер можно спокойно предъявлять для анализа и даже сообщать пароль — определить наличие скрытого диска невозможно. Впрочем, тема вложенных криптоконтейнеров заслуживает отдельной статьи; развивать ее здесь мы не станем. (Пароль от бэкапа не забудь!)

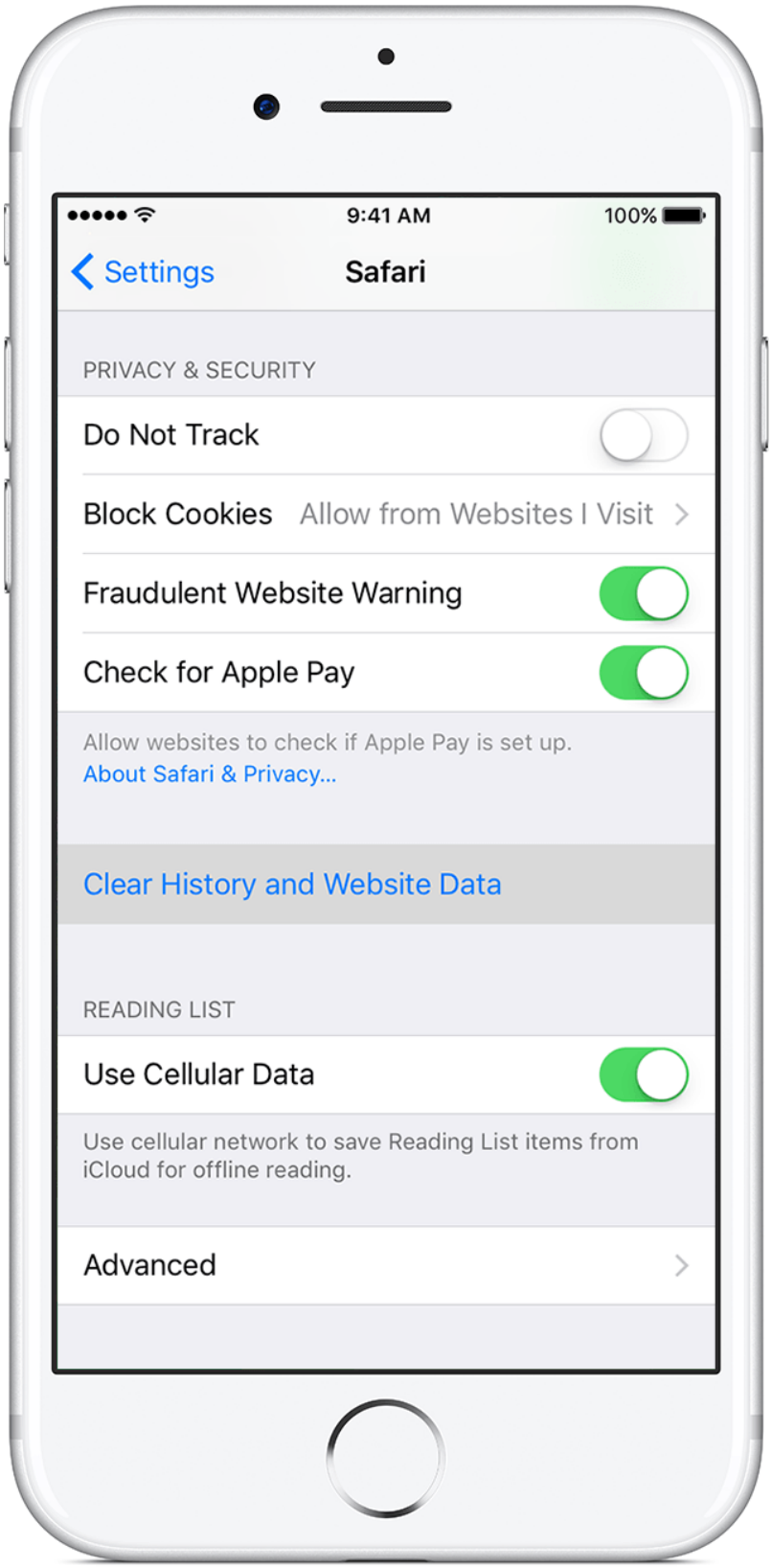
Если ты не хочешь идти на принцип или сбрасывать телефон из-за мизерного (0,08%) шанса его досмотра, рассмотри другие варианты.

Если у тебя iPhone с последней версией iOS, а jailbreak ты не ставил, то тебе повезло: снять физический образ устройства невозможно. Единственный способ анализа, доступный пограничникам, кроме запуска приложений на телефоне вручную, — снять резервную копию через iTunes или специализированное приложение (Elcomsoft iOS Forensic Toolkit или подобное). Противодействовать этому тоже очень легко: достаточно заранее озаботиться установкой пароля на резервные копии. Для этого запусти iTunes и активируй опцию Encrypt iPhone backup:

Далее нужно будет указать пароль:

Что указывать в качестве пароля? Рекомендуем сгенерировать длинный случайный пароль из 10–12 знаков, включающий в себя все возможные вариации букв, цифр и специальных символов. Сгенерируй, распечатай на бумажке, установи в телефон. Бумажку спрячь дома, с собой не бери. Если тебя попросят сообщить пароль от резервной копии, объясни, что офлайновыми бэкапами ты не пользуешься, поэтому в целях безопасности пароль был задан длинный и случайный, к запоминанию не предназначенный. Поскольку в повседневной жизни этот пароль не нужен, такой сценарий вполне вероятен.

Хочешь защитить свои пароли? Выключи keychain и iCloud Keychain на телефоне. Пароли будут удалены с устройства и не подтянутся из облака, пока ты в явном виде не активируешь iCloud Keychain. Аналогичным образом удаляется история браузера и поисковых запросов:



До недавних пор эти действия не защитили бы тебя в полной мере, так как Apple хранила удаленную историю браузера на своих серверах в течение неопределенного времени. После того как компания «Элкомсофт» выпустила приложение, извлекающее удаленные записи, в Apple спохватились и дыру закрыли.

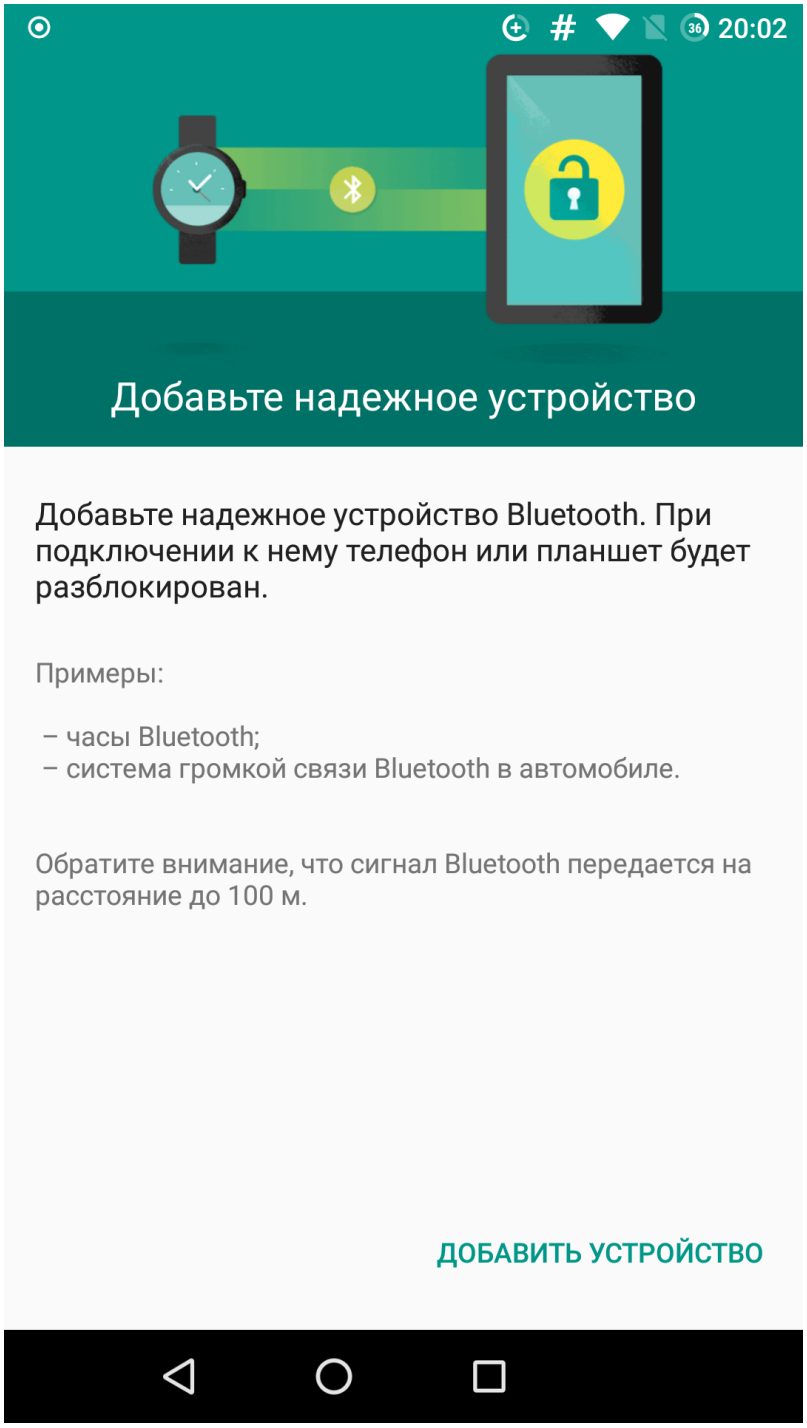
Впрочем, история браузера все равно будет храниться в iCloud как минимум две недели после удаления. Чтобы окончательно «прибить хвосты», потребуется отключить синхронизацию данных с облаком (ты всегда сможешь вновь ее подключить после пересечения границы). О том, как это сделать, — в официальном KB:

В облаке могут храниться и резервные копии устройства. Однако механизмы доступа к облачным данным регулируются уже другими законодательными актами, и в момент пересечения границы данные из облачных бэкапов сейчас не извлекаются. Успокоить внутренний голос и выключить облачные резервные копии (а также удалить уже созданные) ты можешь, но практического смысла в этом немного.

Наконец, ты можешь полностью отключить iCloud. Впрочем, делать это мы не рекомендуем — как минимум с выключением iCloud ты теряешь защиту от кражи iCloud Lock и Find My Phone.

Защищаем Android

Как ты можешь помнить из большой статьи, опубликованной в прошлом номере, Android мы признали наименее безопасной из распространенных систем. Соответственно, если у тебя смартфон на Android, для его защиты тебе придется серьезно поработать.
Первое и самое главное — защита от физического извлечения данных. Пограничник имеет полное право потребовать для досмотра любой предмет из твоего багажа или личных вещей. Получив в руки смартфон на Android, пограничники могут просто воспользоваться сервисным режимом (EDL, режимы 9006/9008 для Qualcomm, LG UP для смартфонов LG и так далее) для доступа к информации. И знаешь, что самое интересное? В 85% случаев этого будет вполне достаточно: согласно последним данным, всего около 15% устройств на Android использует шифрование раздела данных. Если у тебя возникла мысль, что на границе не найдется квалифицированного специалиста для извлечения информации из устройства, вынужден тебя огорчить: современные решения позволяют проделать все даже уборщице. Анимированные инструкции с картинками, что и в какой последовательности нажимать на телефоне и куда втыкать шнурок, появляются прямо на экране компьютера. Впрочем, устройство у тебя можно и конфисковать (прецеденты были), после чего данные извлекут уже в спокойной обстановке. Мораль? Включи, наконец, шифрование!
В Android доступны многочисленные небезопасные способы разблокировки, объединенные общим названием Smart Lock. Если, к примеру, ты пользуешься фитнес-трекером или часами и настроил разблокировку при наличии соединения Bluetooth с этим устройством — дальше можно не читать. Также нет никакой силы, которая могла бы помешать пограничнику сфотографировать твое лицо (очередной камень в сторону Smart Lock). Во многих моделях сомнения вызывает и надежность разблокировки с помощью датчика отпечатков пальцев. Вывод: отключи Smart Lock и убедись, что разблокировать телефон можно только PIN-кодом, желательно — сложным.



Никогда так не делай

В отличие от iOS, где в резервную копию попадает практически все, но сам бэкап можно раз и навсегда защитить паролем, в Android бэкапы создаются или в облаке, или через ADB. В резервные копии попадает довольно ограниченное количество данных; зашифровать их при этом нельзя. Впрочем, маркеры аутентификации (токены) от многих популярных мессенджеров и социальных сетей в бэкапы прекрасно попадают, так что этот момент необходимо иметь в виду. Сам бэкап в Android создается предельно просто: достаточно разблокировать телефон, включить режим разработчика, подключить телефон к компьютеру и выдать соответствующую команду. Скорее всего, если тебя убедят разблокировать телефон, будет проделана именно эта процедура.

Если с твоего телефона снимут резервную копию через ADB, в нее могут попасть:

- пароли от Wi-Fi-сетей, системные настройки;

- фотографии, видео и содержимое внутренней памяти;
- установленные приложения (APK-файлы);
- данные приложений, которые поддерживают резервное копирование (включая маркеры аутентификации).

Помимо прочего, в смартфонах Android царь и бог — компания Google. Google собирает огромное количество данных, которые передаются прямо на сервер. Если от тебя потребуют предоставить пароль от учетной записи и пограничнику в нее удастся войти (к примеру, если у тебя до сих пор не настроена двухфакторная аутентификация), сам телефон будет уже не нужен: в твоей учетке Google есть всё и даже немножко больше. Что с этим делать? Удалить учетную запись Google с телефона перед посадкой в самолет и залогиниться в свежесозданную. К счастью, в отличие от iPhone, это действие не потребует от тебя сбрасывать телефон. Да, и не забудь почистить данные приложений — как минимум контакты, фотографии, Google Maps и данные браузера Chrome. Хвосты, скорее всего, останутся, но если устройство не вызовет подозрений, то более подробного исследования может и не быть.
А что делать с фотографиями? Если тебе необходим в поездке доступ к твоей библиотеке фото и видео, но держать их в самом устройстве ты не хочешь, то тебе снова доступны варианты с облаком (подсказка: приложение Dropbox можно с телефона и удалить) или скрытым вложенным контейнером на компьютере. В конце концов, фотографии можно хранить и в Google Photos той учетной записи, которую ты собирался удалить с телефона перед поездкой (только имей в виду, по умолчанию туда попадают уменьшенные и «оптимизированные» файлы).
Наконец, пользователям с кастомным рекавери (TWRP) доступен вариант создания зашифрованной резервной копии раздела данных, который также можно сохранить во вложенном контейнере на компьютере. Его последующее восстановление — дело нескольких минут. Впрочем, и пересекать границу с «голым», ненастроенным устройством — плохая идея: в глазах пограничника ты будешь выглядеть очень подозрительно.

Слово редактора

Как это ни странно, смартфон без активированного шифрования может сильно облегчить пересечение границы. Все дело в том, что современные смартфоны, вышедшие с завода с Android 6.0+ на борту, обязаны шифровать данные и зачастую хранят ключ шифрования в хардварном модуле TEE (Trusted Execution Environment). С одной стороны, это хорошо, с другой — это препятствует возможности сделать/восстановить полный бэкап системы с помощью TWRP.

А вот если шифрование отключено и возможность сделать бэкап есть, у тебя появляется возможность очень ловко обвести досматривающих вокруг пальца. Суть метода: ты устанавливаешь на смартфон кастомный рекавери TWRP (о том, как это сделать, мы писали не раз и не два), перезагружаешься в него, делаешь nandroid-бэкап разделов system и data (они содержат саму ОС и твои данные/приложения соответственно), извлекаешь бэкап со смартфона (он хранится в каталоге TWRP на карте памяти) и сохраняешь его, ну, например, в Dropbox. Затем ты сбрасываешь смартфон до заводских настроек, привязываешь его к левому аккаунту, устанавливаешь несколько приложений, вводишь несколько неважных паролей в браузер — в общем, создаешь видимость активно используемого устройства. А затем вновь перезагружаешься в TWRP, и опять делаешь бэкап, и вновь сохраняешь его в облако.
В результате у тебя получится два бэкапа: в одном будет твоя основная система, во втором — потемкинская. Все, что тебе останется сделать, — восстановить второй, подставной бэкап перед поездкой, пройти через границу, а затем восстановить основной. При этом все твои настройки, софт и все остальное вплоть до расположения иконок на рабочем столе сохранится в первозданном виде.

Юридические методы противодействия

На сегодняшний день офицер-пограничник имеет право попросить соискателя на въезд в США разблокировать устройство и передать его для анализа. В некоторых случаях (обоснованные подозрения, попадание в список потенциально опасных или нежелательных лиц) офицер имеет право потребовать разблокировать устройство. Разницу между «просьбой» и «требованием» неподготовленному, уставшему от длительного перелета и, возможно, спешащему на пересадку пассажиру уловить трудно, но тем не менее она есть. Проигнорировать приказ не получится, последствия могут быть очень неприятными. А вот просьбу (request) можно вежливо отклонить; если получится аргументировать отказ — тем лучше. Да, тебя могут не впустить в страну, и да, тебя могут задержать на неопределенное время, но с точки зрения американского закона ты пока не совершил преступления.

Заключение

Смартфон — персональное устройство, которое всегда с нами. Смартфон знает о нас даже то, что мы можем не знать о себе сами. Пускать туда посторонних — хороший шанс получить длительную головную боль, заработать обострение паранойи или осложнения с законом. Мы искренне верим, что право на частную жизнь должно

оставаться неприкосновенным и может нарушаться в исключительных случаях и только по решению суда. Деловую или туристическую поездку за границу мы таким исключительным случаем не считаем. Защищать приватность частной жизни законными методами — твое полное и неотъемлемое право, но реализовывать его за тебя никто не будет. Если не хочешь, чтобы в твою личную жизнь лезли посторонние, тебе придется сориентироваться в законах и воспользоваться доступными легальными методами защиты от вторжения.

При этом нужно понимать, что на стороне пограничников если не право, то возможность интерпретации закона в свою пользу, грубая физическая сила и методы принуждения, которыми они не стесняются пользоваться. Применение методов принуждения год от года только растет. С точки зрения собственной безопасности возражать пограничникам не стоит. Не стоит лгать, хитрить и изворачиваться: все это приведет к дополнительным осложнениям и без того острой ситуации. Гораздо эффективнее будет воспользоваться комплексом технических методов защиты, которые мы описали в этой статье. Помни: нельзя извлечь из смартфона то, чего на нем физически нет, а любой пароль от тебя можно получить, было бы желание.