Оглавление:

Введение в Документирование при отключении интернета

В июне 2019 года, когда в Мьянме происходил гуманитарный кризис, и продолжались нарушения прав человека, Министерство Транспорта и Связи страны приказало телекоммуникационным компаниям отключить мобильный интернет в некоторых областях штата Ракхайн и соседнего штата Чин. Ссылаясь на статьи «нарушение общественного порядка» и «незаконная деятельность», правительство Мьянмы утверждает, что отключение было предпринято «в интересах народа». На деле же блокировка интернета лишила более миллиона человек доступа к важной информации и средствам связи, а также нарушила гуманитарную деятельность. Как заявил Мэтью Смит из Fortify Rights: «Это отключение происходит в контексте продолжающегося геноцида против народности Рохинджа и военных преступлений против народа Ракхайна, но даже если бы эта мера была направлена против боевиков, она вопиюще несоразмерна».

В сентябре 2019 блокировку частично сняли в пяти округах, но в целом она продолжается. В том же месяце в соседнем Бангладеше, куда бежали многие рохинджа, власти приказали операторам мобильной связи заблокировать услуги 3G и 4G в лагерях беженцев рохинджа и прекратить продажу им SIM-карт. На момент начала 2020 года четыре округа в штате Ракхайн по-прежнему отрезаны от мира, а Бангладеш продолжает ограничивать обслуживание в лагерях беженцев.

Документирование при отключении интернета

По всему миру растет число случаев блокировки интернета. Согласно данным кампании #KeepItOn, проводимой AccessNow, в период с января по июль 2019 года зафиксировано 128 преднамеренных отключений, на фоне 196 блокировок за весь 2018 год, что говорит о резком росте - с 106 в 2017 году и 75 в 2016 году. Во всем мире правительства в

сотрудничестве с телекоммуникационными компаниями все чаще обращаются к блокировке интернета как к стратегии для подавления сообществ, предотвращения мобилизации и предотвращения документирования и распространения информации о нарушениях прав человека.

«Блокировка интернета и нарушения прав человека идут рука об руку».

- Берхан Тай, AccessNow

Отключение может принимать различные формы, в том числе блокировки конкретных платформ, нацеленные на популярные приложения и сайты; отключение передачи мобильных данных; ограничение трафика или полное отключение интернета. Все эти виды отключений предназначены для нарушения возможности передачи информации и выявления нарушений в режиме реального времени. Они часто происходят во время протестов, выборов и в периоды политической нестабильности и часто сопровождаются усилением репрессий со стороны государства, военными наступательными операциями и насилием. Хотя правительства иногда оправдываются тем, что отключения предпринимались ради «общественной безопасности» или по другим причинам, блокировки применяются тогда, когда репрессивные государства боятся потерять хрупкий контроль над своими людьми, информацией или политической линией. Блокировка интернета нарушает права человека, серьезно подрывает жизнедеятельность и источники заработка людей, а также имеет глобальные экономические последствия.

Документировать нарушения прав человека в периоды отключения интернета как никогда важно. Даже если в данный момент информация не может быть передана, документация может стать способом сохранить голоса, которые власти пытаются заставить замолчать, и собрать доказательства злоупотреблений, чтобы позже призвать нарушителей к ответу. Конечно, репрессивный контекст и технологические препятствия, связанные с блокировкой интернета, делают документирование нарушений (и безопасное хранение этих материалов) гораздо более сложным и рискованным. **Как активисты могут снимать и сохранять свои видео в период блокировки и даже публиковать их в автономном режиме, причем делать это более безопасным способом?**

Об этом курсе

Работая с активистами, которые сталкивались с отключениями интернета, мы узнали несколько полезных советов и техник для **записи и сохранения видеодокументации во время блокировки интернета**; мы поделимся ими в данном курсе. Мы описали техники для устройств Android, но эти же советы можно применить и к iPhone. Некоторые подходы требуют заблаговременной подготовки (и зачастую доступа к интернету), поэтому мы рекомендуем изучить их и предпринять необходимые шаги еще *до* того, как вы окажетесь

в ситуации, когда требуется что-то задокументировать, а интернета уже нет. Сохраняйте копии любых инструкций, чтобы вы могли пользоваться ими или распространять их в период блокировки. И, наконец, начните практиковать рекомендуемые приемы и методы в своей повседневной работе, чтобы выработать привычку, прежде чем окажетесь в кризисной ситуации.

- Подготовьтесь
  - Настройка телефона для документирования офлайн
- Снимайте
  - Стоит ли использовать это приложение для документирования?
- Храните
  - Хранение достоверных материалов при отключении интернета
  - Резервное копирование с телефонных носителей без интернета или компьютера
- Делитесь и Сообщайте
  - Обмен файлами и коммуникация при отключении интернета

И последнее замечание: хотя эти советы могут помочь вам с документированием даже в условиях блокировки, мы хотим подчеркнуть, что коренным решением проблемы должно быть восстановление доступа в интернет и эффективная защита прав людей на запись, а также свободу слова, информации и собраний. К счастью, существует глобальное движение, возглавляемое такими организациями, как NetBlocks, AccessNow и многими другими, которые активно отслеживают блокировки и обмениваются информацией об отключениях. Адвокаты по всему миру участвуют в стратегических судебных процессах против блокировки Инернета. Мы солидарны с их работой по защите прав человека.
****

Настройка телефона для Документирования офлайн

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Несмотря на отключение интернета, документалисты по-прежнему могут записывать важные видеодоказательства, которыми можно делиться в автономном режиме или сразу после подключения к сети.

Вот несколько советов от активистов и других деятелей о том, как настроить телефон для автономной документации. Обратите внимание, что для некоторых шагов **требуется доступ в интернет**, поэтому их необходимо выполнить заранее, до наступления блокировки, или после возобновления работы интернета. Кроме того, не ждите

наступления стрессовой ситуации, чтобы выполнить эти шаги; сделайте это сейчас и потратьте время на то, чтобы **попрактиковаться в использовании телефона,** прежде чем вам придется использовать его в кризисной ситуации.

Блокировки интернета часто сопровождаются усилением контроля над информацией и ограничениями свободы слова и собраний. Если вы документатор, примите дополнительные меры предосторожности для защиты себя и своей информации в эти периоды. Если есть риск, что власти конфискуют ваш телефон или заставят вас разблокировать его и раскрыть содержимое (в период блокировки или в иных условиях), подумайте о возможности использования отдельного телефона для документирования, вместо вашего основного личного устройства. Это может помочь минимизировать объем информации, которая может быть скомпрометирована (например, ваши контакты, аккаунты, сообщения и т.д.). Если вы не можете использовать другое устройство, все равно следуйте этому руководству, чтобы уменьшить объем конфиденциальных данных и повысить безопасность своего основного телефона.

Если используете старый телефон, сначала "почистите" его

Чтобы стереть все данные с телефона, вернитесь к заводским настройкам.

Примечание: Исследования показали, что восстановление на телефоне заводских настроек не обязательно приводит к стиранию всех данных. Фактически, единственный 100% безопасный способ стереть данные - это уничтожить сам телефон, но такой метод не подходит тем, кто хочет повторно использовать имеющееся устройство! В этой статье инженер-разработчик Android предлагает перед возвратом к заводским настройкам убедиться, что содержимое вашего устройства зашифровано. Так или иначе, шифрование используется по умолчанию на большинстве современных телефонов; в противном случае перед сбросом настроек перейдите в «Настройки»> «Безопасность»> «Зашифровать телефон». Таким образом, при возврате телефона к заводским настройкам ключ шифрования будет утерян, и все неудаленные данные станут недоступными.

Практикуйте базовую защиту телефона

Существуют общие практики защиты телефона, которые актуальны в любой ситуации, независимо от того, занимаетесь вы документированием при отключении интернета или нет. Вот некоторые полезные ресурсы от ряда других организаций. Хотя никакие методы не дают 100% гарантию безопасности, некоторые ключевые советы подразумевают следующее:

- Убедитесь, что ваш телефон зашифрован. В новых телефонах шифрование включено по умолчанию. Если вы не уверены насчет своего телефона, проверьте его настройки безопасности.

- Регулярно запускайте обновления операционной системы (ОС), так как они часто устраняют уязвимости системы безопасности.
- Регулярно обновляйте важные приложения (например, мессенджеры).
- Установите на телефоне надежный код доступа, состоящий как минимум из 6 цифр и не использующий отпечатки пальцев (touch ID) или идентификацию лица (face ID).
- Установите блокировку экрана и таймер блокировки.
- Отключите службы геолокации, если они вам не нужны (включая службу экстренного определения местоположения, точность определения местоположения, историю локаций и функции "поделиться местоположением", а также опции сканирования Wi-Fi и Bluetooth). Также проверьте разрешения на доступ к местоположению для отдельных приложений.
- Чтобы избежать отслеживания устройств, выключайте Bluetooth и Wi-Fi, когда они вам не нужны.
- Выключайте телефон, когда вы им не пользуетесь.

Установите полезные приложения для документирования

Для фото- или видеодокументации вы можете использовать встроенную камеру на своем телефоне или специализированное приложение для документирования, например ProofMode или его аналоги, которые обеспечивают более надежные запись и экспорт метаданных, идентификацию и аутентификацию, шифрование, безопасные галереи или другие функции.

Полезным приложением для документирования *самой* блокировки является OONI Probe, приложение с открытым исходным кодом, которое запускает тесты с вашего телефона, чтобы определить, блокируются ли сайты или платформы. Оно может показать вам, как, когда, где и кем блокируются сайты. Перед использованием этого приложения обязательно осознайте потенциальные риски.

Не уверены, какое приложение использовать для документирования? Мы освещаем некоторые наводящие вопросы в нашем руководстве «Стоит ли использовать это приложение для документирования?».

Установите несколько обычных приложений

Наличие на телефоне минимального объема данных и нескольких специализированных приложений может вызвать подозрение. Чтобы устройство выглядело, как обычный телефон, установите несколько повседневных приложений, которые популярны в регионе, где вы документируете (но которые загружаются из авторитетных источников), и сделайте несколько безобидных фотографий для своей галереи.

Для приложений социальных сетей вы можете создать альтернативные аккаунты и войти в них, однако имейте в виду, что фальшивые аккаунты нарушают Условия Обслуживания

большинства платформ, а требования проверки личности на ряде платформ могут усложнить создание поддельных аккаунтов. Кроме того, вам нужно будет потратить некоторое время на наполнение аккаунта контентом и добавление друзей, что может быть довольно трудоемко.

Установка приложений при отсутствии интернета

Очевидно, что скачивание и установка приложений без доступа к интернету является проблемой. Если вы допускаете возможность отключения интернета, вам необходимо заранее скачать приложения.

Одна из стратегий, которая может помочь вам и другим в дальнейшем, - это скачать и сохранить установочный файл приложения формата Android Package (.apk) (**скачивается из надежного источника**, например, непосредственно у разработчика) в памяти вашего телефона или на диске. Наличие этих APK-файлов офлайн позволит вам или другим пользователям делиться приложениями в условиях отсутствия интернета.

Хотя у нас не было возможности попробовать этот сервис, приложение F-Droid предоставляет интерфейс для обмена APK-файлами офлайн. Вот их руководство.

Храните реальную личную или частную / конфиденциальную информацию вне устройства

Постарайтесь использовать устройство только для документирования. Не используйте его для электронной почты, телефонных звонков или обмена сообщениями с личными контактами или активистами, которые могут быть подвергнуты риску, и не подключайте это устройство к вашим реальным, основным аккаунтам.

Используйте функции сокрытия контента

В случае, если ваш телефон досматривается, будет полезно сделать ваши намерения менее очевидными, а контент - менее обнаруживаемым. Если ожидается, что ваш телефон будет *досмотрен бегло и поверхностно*, вы можете использовать такие простые приемы, как:

- Изменить названия и иконки ваших приложений с помощью лаунчер приложений (например, Nova Launcher, но их много), чтобы было не так очевидно, что представляют собой определенные приложения.
- Использовать встроенную функцию конфиденциальности, если она поддерживается на вашем телефоне, например "Режим конфиденциальности" (Private Mode) (для Samsung) или "Блокировка контента" (на LG).

- Поместить пустой файл с именем «.nomedia» в любую папку, чтобы медиафайлы из папки не показывались в вашей галерее. Примечание: Если медиа все еще отображаются, возможно, вам нужно почистить кэш галереи. Это может сработать не на всех устройствах.
- Создавайте скрытые папки (папки, название которых начинается с «.») с помощью приложения для управления файлами. Вы можете переместить файлы в скрытую папку вручную, либо, если пользуетесь приложением для камеры типа Open Camera, можете указать, где сохранять записанные вами медиафайлы. Обязательно отключите в настройках параметр «Показывать скрытые файлы», чтобы скрытые файлы не отображались.
- Некоторые специализированные приложения для документирования, такие как Tella или Eyewitness to Atrocities, хранят материалы в отдельных зашифрованных галереях, содержимое которых доступно только через приложение, так что при досмотре вашего телефона наличие подобных файлов будет не так очевидно. Для документации в этих защищенных галереях устанавливается отдельный код доступа в приложении, поэтому контент остается зашифрованным, даже когда ваш телефон разблокирован.

Важное примечание о сокрытии контента

Важно отметить: описанных выше техник может быть достаточно, чтобы сбить с толку того, кто бегло просматривает ваш телефон, но **они не смогут эффективно скрыть ваш контент от тех, кто действительно ищет.**

Также имейте в виду, что в некоторых странах могут действовать законы, которые ограничивают или криминализируют использование приложений для безопасности, которые шифруют или стирают ваши данные. Их использование для предотвращения доступа властей к вашим данным может рассматриваться как уничтожение улик или препятствование расследованию и может наказываться как преступление. Эта карта (всеобъемлющая, но 2017 года) служит хорошей отправной точкой, если у вас есть вопросы о действующих в вашей стране законах.

Настройте офлайн-доступ

В ситуации, когда вы записали контент, но у вас нет интернета, вы все равно можете перекинуть материал со своего телефона чтобы освободить место, поделиться им с другими или из соображений безопасности. Регулярная выгрузка материалов с вашего телефона также поможет свести к минимуму объем информации, которая может быть скомпрометирована, если ваш телефон будет конфискован и разблокирован.

Даже если вы не можете подключиться к интернету, вы все равно можете подключиться к локальным устройствам с Wi-Fi или Bluetooth, например к другому телефону или USB-накопителю с Wi-Fi. Ваши телефоны обычно снабжены приложением / интерфейсом для

подключения и передачи файлов. Если ваш телефон поддерживает эту функцию, вы также можете подключить USB-флешку или переходник, чтобы выгрузить материалы на флешку или другое устройство.

Эти методы более подробно обсуждаются в нашем Руководстве по обмену файлами и коммуникации при блокировке интернета и в нашем пособии «Видео в качестве доказательства: Технические инструменты - Передача файлов».

Практикуйтесь до того, как окажетесь в кризисной ситуации

Настройте телефон сейчас, если и пока у вас есть доступ в интернет. Начните практиковать использование приложений в повседневных ситуациях (когда нет проблем с безопасностью), чтобы привыкнуть к работе с ними. Сделайте хорошую базовую защиту телефона своей стандартной практикой. Тогда, если вы окажетесь в кризисной ситуации, эти методы вспомнятся по привычке, и вы сможете сфокусироваться на других не менее важных вещах.

Прочтите следующую статью этого курса: «Стоит ли использовать это приложение для документирования?»

****

Стоит ли использовать это приложение для документирования?

Этот раздел является частью курса, посвященного Документированию при отключении интернета. Сравнительная таблица по различным приложениям для документирования доступна ~~здесь~~ (готовится).

Последний пересмотр: 31 января 2020 г.

Существует множество приложений, которые документалисты могут использовать для записи видео, от встроенного приложения камеры на вашем телефоне до более специализированных приложений для документирования типа ProofMode, Tella или Eyewitness to Atrocities. Некоторые приложения имеют функции, требующие доступа в интернет, так что имейте в виду - они могут быть недоступны в случае отключения интернета.

Мы не можем сказать, какое конкретное приложение подойдет вам больше всего, поскольку это зависит от вашей ситуации, потребностей и рисков (ознакомьтесь с этой статьей в блоге, чтобы узнать больше о том, как оценивать свои риски и угрозы). Проведенная вами оценка рисков и приведенные ниже наводящие вопросы помогут вам выбрать оптимальное приложение для видеодокументации.

Кто создал это приложение, и вызывают ли они доверие?

Вы всегда должны задумываться о том, кто разработал скачиваемое и устанавливаемое вами приложение; а также можно ли доверять разработчику и быть уверенным в том, что он не подвергнет вас риску, намеренно или непреднамеренно.

На что следует обратить внимание:

- Надежен ли разработчик приложения? Что говорят о нем и его инструментах люди из вашего сообщества и в более широком кругу?
- Уязвим ли разработчик приложения? Подумайте о его контексте и вероятности того, что он может быть вынужден передать ваши данные или создать доступ для властей (а также делал ли он это в прошлом). В какой стране хранятся данные, и каковы законы о постановлениях суда в этой юрисдикции?
- Поддержка приложения осуществляется разработчиком? Необслуживаемые инструменты уязвимы для атак хакеров, которые используют обнаруженные изъяны. Проверьте сайт разработчика или страницу приложения в Google Play, чтобы узнать дату «последнего обновления».
- Насколько авторитетен разработчик приложения, и сможет ли он поддерживать приложение в дальнейшем?
- Это приложение с открытым исходным кодом? Приложения, которые открыты для проверки, с большей вероятностью устраняют или, по крайней мере, идентифицируют свои проблемы с безопасностью. Прозрачен ли разработчик в вопросе эффективности и безопасности своего приложения?
- Какие мотивы или стимулы движут разработчиком приложения, и как это может повлиять на его надежность? Например, они руководствуются миссией? Или нацелены на получение прибыли? Финансируются конкретным спонсором?
- Стоимость приложения тоже может быть важным фактором, хотя он не является прямым показателем надежности. Некоторые приложения работают с высокой ежемесячной подпиской или берут плату за видео.

Чтобы узнать больше, ознакомьтесь с руководством EFF по выбору приложений для защиты себя от слежки.

Откуда скачивается приложение?

Вы всегда должны скачивать и устанавливать приложения только из авторитетных магазинов приложений или сайтов. Даже если вы тщательно изучили надежность тех или иных приложений, недобросовестные магазины приложений могут искажать информацию о своих товарах и побудить вас скачать нелегальный аналог нужного вам приложения, созданный с сомнительными целями. Например, в прошлом году организация по цифровым правам SMEX выпустила предупреждение о том, что различные сайты предлагают приложение под названием «WhatsApp Plus» (для ясности подчеркнем, что

это не WhatsApp!), которое, вероятно, сохраняет и продает данные пользователей или даже способствует взлому телефонов, на которых оно установлено.

Некоторые разработчики, которые серьезно относятся к вопросу безопасности, даже предоставляют криптографические ключи, позволяющие проверить их подлинность. Обычно они объясняют, как проверить эти подписи.

Где будут храниться данные?

Некоторые приложения для документирования хранят ваши данные и материалы только локально на вашем устройстве, а другие - отправляют и хранят ваши данные в другом месте (это может быть единственный вариант или дополнительная функция). Во многих случаях это связано с конфигурацией и назначением приложения; например, приложение Eyewitness to Atrocities отправляет неизмененную копию вашего материала в хранилище Lexis Nexis, чтобы Eyewitness могли поручиться за цепочку хранения и целостность материала. Вы можете экспортировать свои медиафайлы из зашифрованной галереи в приложении Eyewitness только *после* того, как они были отправлены в хранилище безопасным способом.

Вам решать, нужно ли оставлять материалы только на вашем устройстве, отправлять и хранить их в удаленном месте, которое вы контролируете (опция, доступная в приложении Tella), или же отправить их внешним организациям / платформам, которым вы разрешаете доступ и использование вашей документации. Имейте в виду, что во время блокировки интернета вы не сможете сразу переслать свои материалы через интернет, поэтому вам понадобится приложение, которое позволит вам по крайней мере временно хранить (а в идеале обеспечит резервное копирование) вашу документацию локально (см. Резервное копирование данных с телефона без интернета или компьютера).

Если ваши данные будут отправлены в удаленное хранилище, вам следует знать, в каких странах они будут находиться. Насколько в этих странах данные уязвимы для раскрытия по постановлению суда или другим способом? С какими рисками вы сталкиваетесь, размещая там свои данные?

Шифрует ли приложение мои медиафайлы?

Некоторые приложения, такие как Tella и Eyewitness to Atrocities, предоставляют шифрование файлов и / или зашифрованное хранилище для вашей документации, отдельно от основной галереи вашего телефона и шифрования вашего устройства, так что ваши медиафайлы и метаданные будут всегда зашифрованы на вашем устройстве, если только не войти в них через приложение с паролем. Это означает, что даже если ваш телефон разблокирован, ваша документация останется зашифрованной. Так обеспечивается дополнительный уровень защиты ваших материалов.

Если приложение отправляет и хранит ваши медиафайлы в удаленном месте после восстановления интернета, подумайте, нужно ли вам шифровать медиафайлы во время

передачи и на период хранения в удаленном месте, как это делает, например, приложение EyeWitness.

Имейте в виду, что, хотя шифрование законно в большинстве стран, в некоторых странах могут действовать законы, ограничивающие или криминализирующие его использование. Эта карта (всеобъемлющая, но 2017 года) служит хорошей отправной точкой, если у вас есть вопросы о действующих в вашей стране законах.

Фиксирует ли приложение важные метаданные (без интернета)?

Метаданные - это данные, которые описывают ваше видео или фото, например время и дата или место съемки. Эта информация важна для идентификации, понимания, аутентификации и проверки вашего видео или фотографии в качестве документации определенного события. В контексте отключения интернета особенно важна способность приложения автоматически собирать определенные метаданные и / или позволять вам быстро вводить полезную описательную информацию на месте, поскольку может пройти много времени, прежде чем вы сможете с кем-то поделиться своими материалами (за это время детали могут забыться, обстоятельства могут измениться и т.д. и т.п.).

Большинство специализированных приложений для документации, таких как ProofMode, имеют расширенные функции метаданных и собирают больше метаданных, чем обычные встроенные приложения для камер. Расширенные метаданные могут включать в себя данные различных датчиков, ближайшие сигналы Wi-Fi или Bluetooth, данные устройства, криптографический хэш и предоставленную пользователем информацию, - все это может в дальнейшем облегчить аутентификацию и проверку материалов.

Имейте в виду, что во время отключения интернета вам понадобится приложение, которое не требует передачи данных для генерации или записи метаданных. Некоторые приложения могут использовать для сбора определенных метаданных интернет, а не датчики устройств. Например, если данные о местоположении фиксируются в результате поиска на устройстве, метаданные могут отражать последнее местоположение, где устройство было подключено для передачи данных, вместо фактической локации устройства. В идеале приложение также должно позволять хранить метаданные локально без интернета, включая сохранение любых заполняемых вами форм (например, «автономный режим» в приложении Tella).

Могу ли я экспортировать данные из приложения?

В зависимости от ваших намерений в отношении материалов вам может потребоваться экспортировать видеодокументацию и ее метаданные из приложения в формате, который не является собственностью приложения, чтобы иметь возможность открывать, просматривать и использовать мультимедиа и метаданные вне приложения. Возможность экспорта означает, что вы и другие пользователи не зависите от одного приложения или

поставщика услуг для доступа к вашим материалам, и дает вам больше свободы действий в работе с контентом в будущем. Имейте в виду, что некоторые метаданные могут быть непонятными, если у вас нет доступа к определенным базам данных или переводным таблицам для интерпретации чисел (например, в случае с ID вышек сотовой связи или сетями Wi-Fi).

Обратите внимание, что некоторые приложения могут иметь преднамеренно закрытую цепочку сохранности и не разрешать пользователям экспортировать файлы, а другие приложения могут просто не предлагать функции экспорта. Также имейте в виду, что некоторые приложения, такие как Eyewitness to Atrocities, могут не разрешать экспорт, пока вы не загрузите медиафайлы на удаленный сервер (а для этого вам нужен доступ в интернет), а другие могут позволить вам экспортировать медиафайлы, но не метаданные (за исключением метаданных, хранящихся в самом файле).

Если вам нужно экспортировать файлы, в идеале ваше приложение должно позволять экспортировать неизмененную копию мультимедиа, а также копию метаданных в стандартизированном читаемом текстовом формате. Например, метаданные из приложения Tella хранятся в зашифрованном виде в галерее Tella, но могут быть экспортированы в формате CSV. Кроме того, во время отключения интернета необходимо иметь возможности для экспорта в автономные приложения или сервисы, не зависящие от интернета. В большинстве приложений, позволяющих экспорт данных, есть своего рода кнопка «Поделиться»; она открывает меню, где Android перечисляет приложения на вашем телефоне, способные обрабатывать этот тип контента. К сожалению, разработчики приложений могут настраивать свои меню "поделиться" индивидуально, и между приложениями нет согласованности.

При работе с большим количеством файлов может быть эффективнее заходить в сохраненные файлы через приложение файлового менеджера и копировать файлы оттуда, хотя в таком случае вам могут быть недоступны метаданные, хранящиеся в базе данных приложения. Эта опция также недоступна в приложениях, которые предоставляют свои собственные безопасные галереи, поскольку файлы будут зашифрованы в хранилище. В таких приложениях должна иметься функция "поделиться".

Ознакомьтесь с нашей сравнительной таблицей приложений для документирования и следующей статьей курса «Сохранение достоверных материалов при отключении интернета».

****

Хранение достоверных материалов при отключении интернета

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Правозащитники, эксперты, исследователи и журналисты часто полагаются на документацию из первых рук, снятую свидетелями, чтобы отслеживать нарушения прав человека, сообщать о них и бороться с ними. Чтобы убедиться, что они действуют на основе достоверной информации, эти пользователи предпринимают шаги для аутентификации и проверки получаемой документации, - этот процесс может быть кропотливым и трудоемким.

Как документатор, вы можете предпринять простые шаги, которые облегчат другим проверку и подтверждение ваших материалов, чтобы они могли использоваться своевременно и эффективно. Выполнять эти дополнительные шаги при блокировке интернета еще важнее, учитывая следующее:

- Если вы не сможете загрузить файл сразу, дата публикации и информация о местоположении из социальных сетей будут не так полезны для доказательства того, что ваше видео было снято не ранее определенной даты или в конкретном месте.
- Если другие пользователи тоже не могут загрузить свои файлы, тогда в целом может быть доступно меньше материалов, которые могли бы использоваться для подтверждения вашего видео.
- Если, чтобы доставить видео по назначению, вам приходится передавать его через несколько рук в автономном режиме, другим лицам может быть сложнее отследить источник видео.
- Если вы вынуждены удалить исходное видео с телефона из соображений безопасности или из-за ограниченной емкости хранилища без резервного копирования в облако, или если вы вынуждены избавиться от телефона, в таких случаях подтвердить подлинность видео может быть сложнее.
- Если вы забыли подробности о конкретном видео, а используемое вами приложение не фиксирует / не записывает метаданные без доступа к интернету, последующая идентификация видео может быть невозможна.

Следующие советы помогут вам сохранить ваше видео во время отключения интернета, чтобы обеспечить в дальнейшем его максимальную проверяемость и пригодность в качестве документации.

Снимайте или поместите в видео идентифицирующие данные

Постарайтесь включить в свое видео детали, которые в дальнейшем позволят исследователю или журналисту определить время и место съемки, например, уникальные достопримечательности, панорама, уличные знаки, витрины магазинов, номерные знаки, флаги, часы, первые полосы газет и т.д. Вы также можете озвучить в видео основную информацию, такую как ваше имя и контактную информацию (если это

безопасно), время, дату и местоположение /координаты GPS (или записать их на листе бумаги и снять на видео). Чем больше подробностей вы укажете, тем проще будет потом кому-то исследовать и проверить ваше видео, даже не зная вас или происхождение видео. Чтобы узнать больше, ознакомьтесь с нашими советами по Основным методам Съемки, Хранения и Распространения видео.

Добавить описание / метаданные

Воспользуйтесь одним из множества специализированных приложений для документирования, которые извлекают расширенные метаданные или техническую информацию с вашего телефона, а также позволяют вводить дополнительную описательную информацию вручную. Имейте в виду, что во время блокировки для записи или хранения этих метаданных вам понадобится приложение, которое может работать без доступа в интернет. Чтобы узнать больше о том, как выбрать подходящее приложение, ознакомьтесь с разделом «Стоит ли использовать это приложение для документирования?».

Даже если вы не используете специализированное приложение для документирования, вы все равно можете создавать дополнительную информацию в виде заметок, карт или фотографий на своем телефоне. Вы можете организовать ваше видео с помощью этой дополнительной информации, используя удобно вам приложение - файловый менеджер. В видео следует включить такую ключевую дополнительную информацию, как время, дата, место записанного на видео инцидента, а также источник записи (т.е. ваше имя и контактная информация), если это безопасно. Экспортируйте метаданные и включите их в видео (вы можете поместить все это в папку и заархивировать ее), когда делитесь им.

Делайте резервные копии

Регулярно выполняйте резервное копирование медиафайлов с телефона, в идеале на 2 разных накопителя. Например, вы можете подключить к телефону флэшки или беспроводные накопители даже без компьютера. Для получения более подробной информации ознакомьтесь с нашими советами по «Резервному копированию мультимедиа с телефона без интернета или компьютера». Резервное копирование гарантирует, что вы сохраните копию своего видео на случай, если телефон потеряется или сломается, или вам придется удалить видео с телефона. Наличие защищенной копии вашего исходного видео также позволит исследователю или журналисту, просматривающему ваше видео каким-то другим способом, позже получить видео от вас напрямую (при условии, что они смогут выйти на вас), что способствует более короткой и цельной цепочке сохранности.

Ознакомьтесь со следующей статьей этой серии «Резервное копирование мультимедиа с телефона без интернета или компьютера».

****

Резервное копирование с телефонных носителей без интернета или компьютера

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Резервное копирование - ключ к тому, чтобы ваши данные и материалы не были случайно удалены, повреждены или утеряны, если ваше устройство будет конфисковано. Во время отключения или замедления интернета вы не сможете запустить обычное резервное копирование в облако или отправить свои материалы в безопасное удаленное хранилище. Выгрузка на настольный компьютер или ноутбук - это один из способов резервного копирования, но поскольку у людей часто нет доступа к компьютеру, существует несколько вариантов и советов по резервному копированию мультимедиа с телефона без компьютера в период блокировки интернета.

Используйте флешку или беспроводной диск

Флэш-накопитель для смартфона (или OTG) - это тип USB-накопителя, совместимый со многими (но не всеми) Android-устройствами. Вы можете подключить флэшку для смартфона непосредственно к своему телефону или использовать соответствующий адаптер для подключения телефона к обычному жесткому диску USB. В случае флэшки для смартфона (OTG) диск питается от вашего телефона.

К популярным брендам флэш-накопителей для смартфонов (или OTG) относятся SanDisk, Kingston, Samsung и множество других. Обычно они стоят в диапазоне от 8 до 25 долларов США в зависимости от емкости.
Беспроводные флэш-накопители / жесткие диски похожи на обычные жесткие диски, но не используют кабели. Это позволяет подключать устройства, которые обычно не подключаются к жестким дискам, такие как, например, ваш телефон. Преимущество беспроводного накопителя перед флэш-накопителем для смартфона заключается в том, что вы сможете подключить к одному беспроводному диску одновременно несколько пользователей. Это может быть полезно, например, в ситуации протеста, когда вы снимаете материал командой - отснятые видео каждого участника можно скопировать на жесткий диск, который находится у одного из членов команды. Обратите внимание: беспроводные накопители не потребляют энергию от подключаемого к нему устройства; их питание обеспечивается собственным аккумулятором, который нужно заряжать.

SanDisk, пожалуй, самый популярный бренд беспроводных флэш-накопителей, хотя есть и другие. Беспроводные флэш-накопители обычно дороже, чем флэшки для смартфона;

цены на них варьируются в диапазоне от 25 до 100 долларов США в зависимости от емкости. Цены на более крупные беспроводные внешние жесткие диски начинаются от 150 долларов США в зависимости от емкости.

Альтернатива: старый неиспользуемый телефон

Если у вас нет флэшки для смартфона или беспроводного накопителя, но есть старый неиспользуемый телефон в рабочем состоянии, его тоже можно задействовать для резервного копирования. Пока оба телефона находятся в физической близости, вы можете подключить устройства и копировать мультимедиа с одного на другое через Bluetooth, WiFi Direct или Near Field Communication (NFC) / Android Beam. Bluetooth и Wifi Direct - это беспроводные технологии, которые могут «связать» два устройства без участия роутера или точки доступа. WiFi Direct обеспечивает более широкий диапазон и более быструю передачу данных, чем Bluetooth, но потребляет гораздо больше энергии. Между тем, NFC имеет гораздо более короткий радиус (~ 4 см) и значительно более медленную скорость передачи, чем Bluetooth или WiFi Direct, но подключается быстрее и потребляет меньше энергии, поэтому может быть полезен для быстрой передачи небольших объемов данных, когда оба устройства находятся у вас в руках.

Ваш телефон, вероятно, имеет встроенные приложения / функции Bluetooth, WiFi Direct или NFC, позволяющие выбрать ближайшие устройства для обмена данными. Если на обоих телефонах установлена программа Files By Google, вы также сможете обмениваться файлами в автономном режиме, используя эти технологии в приложении.

Важно: помимо преимущества в виде простоты подключения, эти сервисы имеют и недостаток они небезопасны. Маяки / сканеры Bluetooth и Wi-Fi могут использоваться для отслеживания вашего местоположения или "прощупывания" вашего устройства на предмет информации. Злоумышленники могут попытаться подключиться к вашему устройству, отправить вам нежелательные файлы или даже получить контроль над вашим устройством, если оно уязвимо. **Для большей безопасности отключайте эти сервисы, когда не пользуетесь ими, и включайте только находясь в безопасных местах; ограничьте разрешения приложений только тем, что вам действительно нужно, и применяйте стандартные практики безопасности телефона, такие как установка обновлений и использование надежных паролей.**

Добавляйте любые отдельные описания / метаданные

При копировании медиаданных на флешку, беспроводной накопитель или старый телефон полезно добавлять любую описательную информацию или метаданные, которые могут существовать отделено от носителя. Например, многие приложения для документирования создают текстовые документы CSV или JSON, которые включают извлеченные с устройства метаданные (такие как геолокация, время, дата) и любое

другое описание, введенное пользователем вручную. Обязательно экспортируйте и добавляйте эти документы с метаданными в свои резервные копии.

Защищайте жесткие диски паролями

Многие беспроводные накопители можно защитить паролем с помощью мобильного приложения, которое поставляется вместе с накопителем. Обратите внимание, что защита паролем - это не то же самое, что шифрование (см. ниже). Большинство беспроводных накопителей или флешек не позволяют полное шифрование диска с использованием только мобильного телефона, хотя поддерживают полное шифрование с компьютера.

Подумайте о возможности шифрования файлов

Если для хранения файлов вам нужна большая безопасность, вы можете рассмотреть возможность шифрования резервных копий. Хотя вы, вероятно, не сможете зашифровать большинство беспроводных накопителей или флешек с мобильного телефона, вы можете зашифровать сами файлы перед выгрузкой их на накопитель. Среди приложений, которые шифруют файлы на Android, ZArchiver и RAR. Имейте в виду, что вам нужно помнить свои пароли шифрования. В случае потери пароля восстановить зашифрованные файлы будет невозможно.

Имейте в виду, что в некоторых странах могут действовать законы, ограничивающие или криминализирующие использование шифрования. Их использование для предотвращения доступа властей к вашим данным может рассматриваться как уничтожение улик или препятствование расследованию и может наказываться как преступление. Эта карта 2017 года, возможно, немного устарела, но она служит хорошей отправной точкой, если у вас есть вопросы о действующих в вашей стране законах.

Держите 2 резервные копии в разных местах

Одна резервная копия не всегда надежна. Например, вы можете потерять устройство резервного копирования, повредить его, или оно может просто вдруг выйти из строя. IT-специалисты обычно советуют иметь 2 резервные копии (т.е. всего 3 копии) на отдельных устройствах, хранящихся в разных местах. Это помогает снизить различные риски для каждой копии.

Прочтите последнюю статью этой серии «Обмен файлами и коммуникация при отключении интернета».

****

Обмен файлами и Коммуникация при отключении интернета

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Продолжающееся отключение интернета и репрессии в Кашмире (а это была самая длительная блокировка интернета, когда-либо примененная в условиях демократии) катастрофически сказались на жизни людей в регионе. Более того, в декабре 2019 года в соответствии с политикой компании WhatsApp начал аннулировать аккаунты кашмирцев из-за 120-дневного бездействия пользователей.

На момент написания этой статьи в январе 2020 года Верховный суд Индии постановил, что блокировка интернета на неопределенный срок в Кашмире является незаконной и трактуется как злоупотребление властью. Ограниченный широкополосный и мобильный интернет был восстановлен в некоторых областях, но только для разрешенных сайтов из «белого списка».

Отключение интернета предпринимается для того, чтобы люди не могли обмениваться информацией и общаться (а также чтобы подтолкнуть людей использовать менее безопасные формы связи, такие как мобильный телефон и SMS, которые властям легче контролировать и перехватывать). При полном отключении интернета не всегда есть эффективные обходные пути. Например, в самые строгие периоды отключения интернета в Кашмире для передачи сообщений своим близким люди прибегали к рукописным заметкам и курьерам.

У нас нет гарантированных способов обойти все блокировки, но в ходе бесед с активистами и коллегами мы узнали некоторые методы и подходы для автономного обмена материалами и общения, которые могут быть вам полезны в зависимости от обстоятельств. Обратите внимание, что некоторые из этих опций подразумевают подключение к интернету для первоначальной настройки (например, для скачивания приложений и т.д.).

Обменивайтесь файлами напрямую через Bluetooth, Wi-Fi Direct или NFC

Вам не нужен интернет, чтобы подключить свой телефон к другому устройству, находящемуся поблизости, через Bluetooth, Wifi Direct или Near Field Communication (NFC) (иногда на более старых устройствах эта функция называется Android Beam). Bluetooth и Wifi Direct - это беспроводные технологии, которые могут «связать» два устройства без участия роутера или точки доступа. WiFi Direct обеспечивает более широкий радиус и более быструю передачу данных, чем Bluetooth, но потребляет гораздо больше энергии. Между тем, NFC работает в более коротком радиусе (~ 4 см) и с более низкой скоростью передачи, чем Bluetooth или WiFi Direct, но подключается быстрее и потребляет меньше

энергии, поэтому такой вариант может быть полезен для быстрой передачи небольших объемов данных, когда оба устройства находятся у вас в руках.

Скорее всего, в ваш телефон встроены функции Bluetooth, WiFi Direct и NFC, которые отображаются в меню "поделиться". Кроме того, эти технологии интегрированы в приложения с функцией обмена файлами, такие как Files By Google.

Важно: помимо преимущества в видео простоты подключения, эти сервисы имеют и недостаток - они небезопасны. Маяки / сканеры Bluetooth и Wi-Fi могут использоваться для отслеживания вашего местоположения или "прощупывания" вашего устройства на предмет информации. Злоумышленники могут попытаться подключиться к вашему устройству, отправить вам нежелательные файлы или даже получить контроль над вашим устройством, если оно уязвимо. **Для большей безопасности отключайте эти сервисы, когда не пользуетесь ими, и включайте только находясь в безопасных местах, ограничьте разрешения приложений только тем, что вам действительно нужно, и применяйте стандартные практики безопасности телефона, такие как установка обновлений и использование надежных паролей.**

Обменивайтесь файлами с помощью беспроводных накопителей или через беспроводную локальную сеть (WLAN).

Беспроводной жесткий диск или флэшка могут использоваться для одновременного обмена файлами между командой или несколькими людьми. Жёсткий диск с Wi-Fi обычно сопровождается инструкциями и / или приложением для подключения к телефону, и достаточно прост в использовании. Не забудьте для безопасности установить на диске пароль.

Если у вас нет беспроводного накопителя, вы также можете обмениваться файлами с помощью обычного USB-накопителя, подключив его к беспроводному роутеру. Например, дорожный роутер с USB-портом относительно недорог и очень портативен. Пользователи могут подключаться к USB-накопителю через локальную сеть (интернет для этого не требуется). Чтобы иметь доступ с вашего телефона к файлам на подключенном USB-накопителе, вам потребуется приложение для управления файлами, способное подключаться к сетевому хранилищу, например Solid Explorer. IP-адрес вашего роутера обычно можно найти в расширенных настройках Wi-Fi вашего телефона.

Между тем, еще одним решением является PirateBox - независимый проект, предоставляющий бесплатное лицензированное программное обеспечение. Пользователи этого сервиса могут обмениваться файлами аналогичным образом, но Piratebox позволяет это делать анонимно, а также предлагает дополнительные функции чата и мессенджера. Для настройки работы Piratebox необходимо скачать, установить и настроить несколько программ. Инструкции есть на сайте Piratebox.

Общайтесь с коллегами в специализированных чатах

Два новых приложения для обмена сообщениями с коллегами, о которых мы узнали от активистов, - это Briar и Bridgefy. Мы еще не пробовали эти приложения, но мы знаем людей, которые тестируют их.

Briar - это приложение для обмена сообщениями со сквозным шифрованием и открытым исходным кодом, которое не использует центральный сервер, а вместо этого синхронизирует сообщения между устройствами пользователей (так что контент сохраняется на устройстве каждого пользователя). Оно способно синхронизироваться даже без интернета, через Bluetooth или Wi-Fi (при наличии интернета приложение синхронизирует устройства с помощью сети Tor). В Briar также есть закрытые группы, общедоступные форумы и блоги. При использовании в автономном режиме ваш радиус охвата ограничен диапазоном Bluetooth или Wi-Fi (максимум ~100 метров).

Bridgefy - это приложение для обмена сообщениями со сквозным шифрованием (за исключением случаев использования функции «трансляции»), которое для отправки сообщений использует Bluetooth. В отличие от Briar, сообщения могут пересылаться на бóльшие расстояния, перемещаясь по сотовой сети других пользователей Bridgefy (но только предполагаемый получатель сможет прочитать сообщение). У Bridgefy, в отличие от Briar, нет закрытых групп, форумов и блогов, но есть режим Трансляции, с помощью которого вы можете отправить сообщение сразу до 7 пользователей Bridgefy в пределах досягаемости, которые при этом не обязательно должны быть в ваших контактах (сообщения типа "трансляция" в силу необходимости не шифруются).

Общайтесь через зашифрованные SMS

Текстовые SMS-сообщения отправляются по сотовым сетям и не привязаны к интернету, поэтому могут работать даже в периоды отключения интернета. Однако SMS считаются очень небезопасным средством коммуникации. В отличие от приложений, использующих интернет, таких как WhatsApp или Signal, SMS не шифруется сквозным шифрованием. Это означает, что текстовые сообщения (и их метаданные) могут быть прочитаны правительствами и операторами мобильной связи или перехвачены хакерами. SMS также можно «сфабриковать»; это значит, что отправитель может манипулировать своей контактной информацией и выдавать себя за другого пользователя.

Если вам нужно использовать SMS, Silence - это приложение, которое обеспечивает сквозное шифрование SMS-сообщений. Это приложение с открытым исходным кодом использует протокол шифрования Signal. Хотя мы сами не пробовали работать с ним, мы слышали отзывы других пользователей. Это приложение должны установить и отправитель, и получатель, после чего они обмениваются друг с другом ключами. Поскольку SMS-сообщения обязательно проходят через серверы вашей телекоммуникационной компании, даже при использовании Silence телекоммуникационной компании будет известно, что вы отправляете зашифрованное сообщение, и доступны метаданные о вашем сообщении.

Частичное отключение: обход заблокированных сайтов

«Отключение интернета» зачастую означает не полное отключение интернета, а скорее блокирование доступа к определенным сайтам или платформам социальных сетей. Правительства через интернет-провайдеров (ISP) могут блокировать сайты на основе IP-адреса, контента или по DNS-запросам. Не уверены, заблокирован ли сайт? Такие организации, как Open Observatory of Network Interference и Netblocks, отслеживают и измеряют сбои в работе интернета и цензуру по всему миру.

К счастью, пока у вас есть доступ в интернет, есть несколько способов попробовать обойти частичные блокировки. Как и в случае с шифрованием, имейте в виду, что обход заблокированных сайтов может быть уголовно наказуем в вашей стране.

VPN

Один из способов обойти блокировку по IP и контенту - использовать виртуальную частную сеть или VPN, например ProtonVPN или TunnelBear. Когда вы подключаетесь через VPN, ваш интернет-трафик зашифровывается и маршрутизируется через VPN-сервер в другой локации, например, в другой стране, таким образом истинный адресат информации и содержимое вашего трафика скрываются от интернет-провайдера.

Имейте в виду, что некоторые правительства запрещают использование VPN или пытаются обнаружить и блокировать VPN-соединения. Также важно использовать надежный VPN-сервис, желательно такой, который не хранит данные или журналы посещений, иначе сервис сможет видеть вашу активность в интернете. Вы должны знать, в какой стране базируется VPN-сервис, и какие юридические процедуры могут к нему применяться в зависимости от юрисдикции. Также учтите, что VPN, одобренные правительством, могут фактически допускать слежку и проверку ваших данных.

DNS-серверы

Серверы DNS («система доменных имен») работают путем преобразования доменных имен или URL-адресов, которые пользователь вводит в браузер, в числовые IP-адреса, которые интернет использует для идентификации веб-страниц. Интернет-провайдер может изменить подконтрольные ему DNS-серверы, чтобы блокировать определенные запросы или выдавать неверную страницу, сообщающую, что сайт не существует. В 2014 году во время выборов в Турции с помощью этой техники премьер-министр Турции Реджеп Тайип Эрдоган пытался заблокировать Twitter. Запрет был быстро пресечен активистами, которые делились пошаговыми советами по использованию VPN и смене DNS-серверов.

Вы можете изменить DNS-сервер по умолчанию в настройках сети или Wi-Fi на вашем телефоне. Чтобы обойти блокировки на основе DNS, вместо DNS-сервера по умолчанию

вы можете использовать альтернативные DNS-серверы, такие как Google Public DNS или CloudFlare. У Cloudflare также есть приложение под названием 1.1.1.1, которое позволяет пользователям переключаться на DNS-сервер Cloudflare в приложении с простым интерфейсом.

Это всего лишь два способа обойти наиболее распространенные методы блокировки. Для получения более подробной информации ознакомьтесь с полезными руководствами от Internet Society, Access Now, Security-in-a-Box и EFF.

****