من سلسلة تدوينات التوثيق أثناء حجب الإنترنت

هذه التدوينة جزء من سلسلة التوثيق أثناء حجب الإنترنت، أيضاً سنقوم بإصدار بيان به مقارنة للعديد من تطبيقات التوثيق قريباً

بمشاركات من أرول باركاش

تمت مراجعته في *31* يناير *2020*

هناك العديد من التطبيقات التي يمكن أن يستخدمها الموثقين لتصوير الفيديو، بدءًا من تطبيق الكاميرا الأصلي لهاتفك، إلى تطبيقات أكثر تخصصا مثل ProofMood أو Tella أو Eyewitness to Atrocities.

تحتوي بعض التطبيقات على مميزات تعتمد على الاتصال بالإنترنت، لذلك ضع في اعتبارك أن هذه الميزات قد لا تكون متاحة في حالة حجب الانترنت أو إيقاف تشغيله.

لا يمكننا إخبارك إي تطبيق بيعنه هو الأنسب لك، حيث يعتمد ذلك على موقفك واحتياجاتك ومخاطرك . ولكن يمكن أن تساعدك هذه الأسئلة الإرشادية أدناه في تقييم التطبيق الأنسب لك.

من قام بصنع هذا التطبيق وهل أثق به؟

يجب أن تفكر دائمًا في مصدر أي تطبيق تقوم بتنزيله وتثبيته على جهازك، وما إذا كان بإمكانك الوثوق بالمطورين الذين قامو بتطويره أو لا حتى لا تتعرض بسببه للخطر ، عن قصد أو عن غير قصد.

بعض الأشياء التي يجب البحث عنها:

ما هي سمعة مطور التطبيق ماذا يقول الناس في مجتمعك عنهم وعن أدواتهم؟

هل مطور التطبيق ضعيف؟ فكر في سياقها ومدى احتمال إجبارهم على تسليم بياناتك أو الرضوخ للسلطات (أو ما إذا كانوا قد فعلوا ذلك بالفعل في الماضي). ما هي الدولة التي يتم تخزين البيانات فيها وما هي القوانين المتعلقة بأوامر المحكمة في تلك الدولة؟

هل يحافظ مطور التطبيق على التطبيق؟ ويحدثه باستمرار ويؤمن ثغراته؟ يمكنك الكشف عن ذلك من خلال صفحة التطبيق على سوق جوجل.

ما حجم مطور التطبيق ، وهل يبدو أنه سيكون بإمكانه الحفاظ على التطبيق مع مرور الوقت؟

هل التطبيق مفتوح المصدر؟ من الأرجح أن تعالج التطبيقات التي تكون مفتوحة للتدقيق أو يتم تحديدها على الأقل. هل المطور قام بتطوير التطبيق والتأكد من أمانه؟

ما هي الدوافع أو الحوافز التي تدفع عمل مطور التطبيق ، وكيف يمكن أن يؤثر ذلك على جدارته بالثقة؟ على سبيل المثال ، هل هي للربح أو برعاية ممول معين؟

على الرغم من عدم كونه مؤشرًا مباشرًا للثقة أو لا ، إلا أن تكلفة التطبيق قد تكون أحد الاعتبارات المهمة. تحتوي بعض التطبيقات على رسوم اشتراك شهرية عالية أو رسوم لكل فيديو.

حول اختيار التطبيقات للمزيد EFF (تحقق من دليل الدفاع عن النفس للمراقبة (؟؟؟

أين يمكن تحميل البرنامج؟

يجب عليك دائمًا تنزيل التطبيقات وتثبيتها فقط المتاجر الرسمية (متجر جوجل مثلا) أو مواقع الويب ذات السمعة الطيبة. حتى إذا كنت قد قمت بإجراء بحثًا شاملاً لتحديد مدى مصداقية أحد التطبيقات ، فإن التحميل من المواقع سيئة السمعة قد تضرك أو تؤدي بك إلى تنزيل مخادع غير شرعي تم إنشاؤه لأغراض ضارة. على سبيل المثال ، أصدرت مؤسسة الحقوق الرقمية SMEX في العام الماضي تحذيراً حول العديد من مواقع الويب التي تقوم بتسويق تطبيق يسمى "WhatsApp Plus" (للتوضيح ، هذا ليس WhatsApp!) ، مما قد يؤدي إلى حفظ بيانات المستخدمين وبيعها ، أو تجهيز الهواتف التي تثبيته ليتم اختراقها.

يوفر بعض مطوري البرامج الواعين للأمان تشفيرات تتيح لك التحقق من صحتها. سيقدمون عادة شرحًا لكيفية التحقق من هذه التشفيرات.

أين سيتم تخزين الداتا ؟

تخزن بعض التطبيقات بياناتك ووثائقك محليًا على جهازك فقط ، بينما يقوم البعض الآخر بإرسال بياناتك وتخزينها في مكان آخر. في كثير من الحالات ، يكون هذا متأصلًا في تصميم التطبيق والغرض منه ، مثل تطبيق Eyewitness to Atrocities ، الذي يرسل نسخة غير قابلة للتغيير من مستنداتك إلى مرفق تخزين Lexis Nexis حتى يتسنى لشاهد Eyewitness أن يشاهد المادة. لا يمكنك تصدير الوسائط الخاصة بك إلا من المعرض المشفر داخل تطبيق Eyewitness بعد.

الأمر متروك لك لتحديد ما إذا كنت بحاجة إلى الاحتفاظ بمستنداتك على جهازك فقط، أو ما إذا كنت بحاجة إلى إرسالها وتخزينها إلى موقع بعيد تتحكم فيه (كما هو الحال مع Tella) ، أو ما إذا كنت بحاجة لإرساله إلى خارج النظام الأساسي التي تسمح بالوصول إلى وثائقك واستخدامها. ضع في اعتبارك أنه أثناء إيقاف تشغيل الإنترنت، لن تتمكن من إرسال مستنداتك عبر الإنترنت على الفور ، لذلك ستحتاج إلى تطبيق تسطيع من خلاله مؤقتًا تخزين مستنداتك محليًا (راجع النسخ الاحتياطي للوسائط الهاتف دون الإنترنت أو الكمبيوتر).

إذا تم إرسال بياناتك إلى موقع بعيد ، فاحرص على تحديد البلدان التي ستتواجد بها البيانات. ما مدى تعرض البيانات للكشف في تلك البلدان ، سواء بأمر من المحكمة أو بوسائل أخرى؟ ما هي المخاطر التي من الممكن أن تواجهل من خلال كشف بياناتك؟

هل يقوم التطبيق بتشفير المادة الموثقة؟

توفر بعض التطبيقات ، مثل Tella و Eyewitness to Atrocities ، تشفير الملفات و / أو التخزين المشفر لوثائقك ، منفصلة عن معرض هاتفك الرئيسي وتشفير هاتفك ، بحيث لا يتم تشفير الوسائط والبيانات الوصفية على جهازك ما لم يتم الوصول إليها من خلال التطبيق مع رمز المرور. هذا يعني أنه حتى لو كان هاتفك غير مؤمّن ، فإن وثائقك تظل مشفرة. يمكن أن يوفر هذا مستوى إضافيًا من الحماية لمستنداتك.

إذا كان التطبيق يرسل ويخزن الوسائط الخاصة بك إلى موقع بعيد بعد عودة الاتصال بالإنترنت، ففكر أيضًا في ما إذا كنت بحاجة إلى تشفير الوسائط الخاصة بك أثناء النقل، كما يفعل تطبيق EyeWitness ، على سبيل المثال.

ضع في اعتبارك أنه على الرغم من أن التشفير قانوني في معظم البلدان، فقد يكون لدى البعض منهن قوانين تقيد استخدامه أو تجرّمه.

هل يقوم التطبيق بتخزين البيانات الوصفية (metadataa) أثناء عدم الاتصال بالإنترنت

البيانات الوصفية أو ال metadata هي بيانات تصف الفيديو أو الصورة ، مثل الوقت والتاريخ أو الموقع. تعتبر هذه المعلومات ذات قيمة لتحديد الفيديو أو الصورة وفهمها والمصادقة عليها والتحقق منها كوثائق لحدث معين. في سياق حجب الإنترنت ، تعد قدرة التطبيق على جمع بيانات وصفية معينة تلقائيًا و / أو السماح لك بإدخال معلومات وصفية مفيدة على الفور مفيدة بشكل خاص ، حيث قد تكون

هناك فترة طويلة من الوقت قبل أن تتمكن من مشاركة الوثائق مع أي شخص (الوقت الذي يمكن فيه نسيان التفاصيل ، قد تتغير الظروف ، وما إلى ذلك).

تحتوي معظم تطبيقات الوثائق المتخصصة ، مثل ProofMode ، على ميزات بيانات وصفية محسّنة ، وتجمع بيانات وصفية أكثر من تطبيقات الكاميرا المضمنة النموذجية. قد تشمل البيانات الوصفية المحسّنة بيانات استشعار مختلفة ، وإشارات WiFi أو Bluetooth قريبة ، وبيانات الجهاز، والمعلومات التي يوفرها المستخدم ، وكل ذلك يمكن أن يسهل التأكد من مصداقية المادة والتحقق من الوسائط في وقت لاحق.

ضع في اعتبارك أنه أثناء إيقاف تشغيل الإنترنت، ستحتاج إلى تطبيق لا يتطلب إرسال البيانات من أجل إنشاء البيانات الأولية أو تسجيلها. قد تعتمد بعض التطبيقات على الإنترنت ، بدلاً من أجهزة استشعار الأجهزة ، لجمع بيانات تعريف معينة. على سبيل المثال قد تعكس البيانات التعريفية الموقع الأخير حيث كان الجهاز متصل بالانترنت، بدلاً من الموضع الفعلي للجهاز. يجب أن يسمح لك التطبيق أيضًا بتخزين البيانات الوصفية محليًا بدون الإنترنت ، بما في ذلك حفظ أي النماذج التي تملأها (على سبيل المثال ، "الوضع غير المتصل لـ Tella").

هل استطيع إخراج المادة من التطبيق؟

اعتمادًا على نواياك فيما يتعلق بالتوثيق والوثائق، قد يكون من الضروري أن تكون قادرًا على نقل وثائق الفيديو وبيانات التعريف الخاصة به من التطبيق ، بتنسيق لا يمتلكه التطبيق فقط لتتمكن أنت والآخرين من عرض المادة بدون الحاجه للتطبيق. ويمنحك مهلة أكبر في العمل مع المضي قدمًا في المحتوى. ضع في اعتبارك أن بعض البيانات الوصفية - ***metadata*** - قد لا تكون مفهومة.

لاحظ أن بعض التطبيقات قد يكون لديها حراسة مغلقة المتعمدة ولا تسمح للمستخدمين بنقل المادة أو إخراجها من التطبيق، بينما قد لا يتم تصميم بعض التطبيقات مع مراعاة إخراج المادة بالشكل المراد. عليك أيضًا أن تدرك أن بعض التطبيقات ، مثل ***Eyewitness to Atrocities*** ، قد لا تسمح لك بإخراج المادة حتى تقوم بتحميلها إلى خادم - سيرفر - *(*والتي تحتاج إلى الإتصال بالإنترنت للقيام بها*)* ، وقد تسمح لك بعض التطبيقات بتصدير الوسائط، ولكن ليس البيانات التعريفية *(*بخلاف البيانات التعريفية الموجودة في الملف نفسه*)*. إذا كنت تحتاج إلى إخراج المادة، فمن الأفضل أن يسمح لك التطبيق بتصدير نسخة من الوسائط دون أي تغييرات أو تحويلات ونسخة من البيانات الوصفية - الـ ***metadata*** - بتنسيق نصي مقروء موحد. على سبيل المثال ، يتم تخزين بيانات ***Tella*** الوصفية في تشفير معرض ***Tella*** ، ولكن يمكن إخراجها بتنسيق ***CSV***. بالإضافة إلى ذلك، أثناء عدم الاتصال الإنترنت، من الضروري وجود خيارات للنقل إلى التطبيقات غير المتصلة بالإنترنت أو الخدمات التي لا تعتمد على الإنترنت. تحتوي معظم التطبيقات التي تسمح لك بالتصدير على "زر" المشاركة الذي يقوم بتشغيل قائمة مشاركة، والتي يسجلها ***Android*** من قائمة من التطبيقات على هاتفك قادرة على التعامل مع هذا النوع من المحتوى. للأسف، يمكن لمطوري التطبيقات تخصيص قوائم مشاركتهم ولا يوجد تناسق بين التطبيقات.

أما إذا كانت كمية أكبر من الملفات، قد يكون الوصول إلى الملفات المخزنة أكثر فعالية من خلال تطبيق مدير الملفات ونسخ الملفات من هناك، على الرغم من أنك قد لا تتمكن من الوصول إلى البيانات الوصفية - الـ***metadata*** - المخزنة في قاعدة بيانات التطبيق بهذه الطريقة. هذا الخيار غير متاح أيضًا للتطبيقات التي توفر معارض آمنة خاصة بها، حيث سيتم تشفير الملفات أثناء التخزين. وبالنسبة لهذه التطبيقات ، من الضروري وجود خيار للمشاركة داخل التطبيق.

اطلع على التدوينة التالية في هذه السلسلة ، "الحفاظ على الوسائط القابلة للتحقق أثناء إيقاف تشغيل الإنترنت" ومخططنا المقبل للوثائق