Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?

Seri Mendokumentasikan selama Pemadaman Internet

Oleh Yvonne Ng

Dengan kontribusi dari Arul Prakkash

*Artikel ini adalah bagian dari Seri Pendokumentasian Selama Pemadaman Internet.*Nantikan bagan perbandingan berbagai aplikasi dokumentasi kami yang akan datang!

Ulasan terakhir: 31 Januari 2020

Ada banyak aplikasi yang dapat digunakan oleh para pembuat dokumentasi untuk mengambil video, mulai dari aplikasi kamera bawaan ponsel kamu, hingga aplikasi dokumentasi yang lebih khusus seperti ProofMode, Tella, atau Eyewitness to Atrocities. Beberapa aplikasi memiliki fitur yang membutuhkan akses internet, jadi perlu diingat bahwa fitur tersebut mungkin tidak tersedia jika terjadi pemadaman internet.

Kami tidak dapat memberi tahu aplikasi spesifik mana yang paling tepat untukmu, karena tergantung dari situasi, kebutuhan, dan risiko (lihat posting blog ini untuk informasi lebih lanjut tentang cara menilai risiko dan ancamanmu). Dengan penilaian risiko, pertanyaan panduan di bawah ini dapat membantu untuk mengevaluasi aplikasi dokumentasi video mana yang paling cocok untuk kamu.

Siapa pengembang aplikasi dan apakah saya mempercayai mereka?

Kamu harus selalu mempertimbangkan sisi pembuat aplikasi apa pun yang kamu unduh dan instal di perangkat kamu, dan apakah kamu dapat mempercayai mereka untuk tidak menempatkanmu dalam risiko, baik secara sengaja atau tidak sengaja.

Beberapa hal yang harus diperhatikan adalah:

- Apakah pengembang aplikasi memiliki reputasi yang baik? Apa yang dikatakan sejawat di komunitasmu dan jaringan komunitas yang lebih luas tentang pembuat aplikasi dan aplikasi mereka?
- Apakah pengembang aplikasi tersebut rentan? Pertimbangkan konteks mereka mengembangkan aplikasi dan seberapa besar kemungkinan mereka dapat dipaksa untuk menyerahkan datamu atau membuat pintu belakang (*backdoor*) bagi pihak berwenang (atau apakah mereka pernah melakukannya di masa lalu). Di negara mana data disimpan dan apa hukum terkait perintah pengadilan di yurisdiksi itu?
- Apakah pengembang aplikasi mengelola terus-menerus memperbaharui aplikasi? Aplikasi yang tidak dikelola rentan terhadap peretasan yang mengeksploitasi kerentanan yang ditemukan. Periksa situs web pengembang atau halaman Google Play aplikasi untuk mengetahui tanggal "terakhir diperbarui".
- Seberapa mapan pengembang aplikasi, dan apakah mereka akan dapat mempertahankan

aplikasi dari waktu ke waktu?
- Apakah aplikasi tersebut *open-source*? Aplikasi yang terbuka untuk diteliti lebih cenderung untuk mengatasi masalah keamanan mereka atau setidaknya dapat diidentifikasi. Apakah pengembang bersikap transparan tentang kemanjuran dan keamanan aplikasi?
- Motivasi atau insentif apa yang mendorong kerja pengembang aplikasi, dan bagaimana hal itu mempengaruhi kepercayaan mereka? Sebagai contoh, apakah mereka digerakkan oleh misi tertentu? Untuk mengambil keuntungan? Disponsori oleh pendonor tertentu?
- Meskipun bukan indikator langsung dari kepercayaan atau tidak, biaya aplikasi mungkin menjadi pertimbangan penting. Beberapa aplikasi memiliki biaya berlangganan bulanan yang tinggi atau biaya per-video.

Lihatlah panduan EFF tentang pertahanan diri dari pengawasan untuk memilih aplikasi lebih lanjut.

Dari mana aplikasi tersebut diunduh?

Kamu harus selalu mengunduh dan menginstal aplikasi dari toko aplikasi (app store) atau situs web terkemuka. Bahkan jika kamu telah melakukan penelitian menyeluruh untuk menentukan kepercayaan terhadap suatu aplikasi, toko aplikasi yang tidak jelas dapat salah menggambarkan barang dagangan mereka dan membuat kamu mengunduh penipu ilegal yang dibuat untuk tujuan jahat. Misalnya, tahun lalu organisasi hak digital SMEX mengeluarkan peringatan tentang berbagai situs web yang memasarkan aplikasi yang disebut "WhatsApp Plus" (untuk lebih jelasnya, ini bukan produk WhatsApp!), yang berpotensi menyimpan dan menjual data pengguna, atau memungkinkan ponsel yang meng-*install*-nya diretas.

Beberapa pengembang yang sadar keamanan bahkan menyediakan kunci kriptografi yang memungkinkan kamu memverifikasi keasliannya. Mereka biasanya akan memberikan penjelasan tentang cara memverifikasi tanda tangan digital tersebut.

Di mana Data akan disimpan?

Beberapa aplikasi untuk dokumentasi hanya menyimpan data dan dokumentasi kamu secara lokal di perangkat kamu, sementara beberapa aplikasi hanya atau dengan tambahan mengirim dan menyimpan data kamu di tempat lain. Dalam banyak kasus, hal ini melekat pada desain dan tujuan dari aplikasi, seperti aplikasi Eyewitness to Atrocities, yang mengirimkan salinan dokumentasi kamu yang tidak diubah ke fasilitas penyimpanan Lexis Nexis sehingga Eyewitness dapat menjamin rantai penjagaan dan integritas bahan. kamu hanya dapat mengekspor media dari galeri terenkripsi di dalam aplikasi Eyewitness setelah dikirim untuk dijaga.

Kamu bebas untuk menentukan apakah kamu memerlukan dokumentasimu untuk tetap tersimpan pada perangkat kamu saja, atau apakah kamu memerlukannya dikirim dan disimpan ke lokasi terisolir yang kamu kontrol (seperti pilihan dengan Tella), atau apakah perlu mengirimnya ke *platform*/organisasi luar yang kamu izinkan untuk mengakses dan menggunakan dokumentasi kamu.

Ingat bahwa selama *internet shutdown*, kamu tidak dapat mengirimkan dokumentasi melalui internet dengan segera. Jadi kamu akan memerlukan aplikasi yang setidaknya untuk sementara waktu

memungkinkan kamu menyimpan (dan idealnya membuat cadangan) dokumentasi kamu secara lokal (Lihat Mencadangkan media ponsel tanpa internet atau komputer).

Jika data kamu akan dikirim ke lokasi yang jauh, waspadalah dengan negara mana tempat data akan tersimpan. Seberapa data rentan untuk terekspos di negara-negara itu, apakah dengan perintah pengadilan atau dengan cara lain? Risiko apa yang akan dihadapi dengan terbukanya data kamu di sana?

Apakah aplikasi mengenkripsi media saya?

Beberapa aplikasi, seperti Tella dan Eyewitness to Atrocities, menyediakan enkripsi file dan/atau penyimpanan terenkripsi untuk dokumentasi kamu, terpisah dari galeri utama ponsel kamu dan enkripsi ponselmu, sehingga media dan metadata kamu tidak pernah dienkripsi pada perangkat kamu kecuali diakses melalui aplikasi dengan kode sandi. Ini berarti bahwa meskipun ponsel kamu tidak terkunci, dokumentasi kamu tetap terenkripsi. Ini dapat memberikan tingkat perlindungan ekstra untuk dokumentasi kamu.

Jika aplikasi mengirim dan menyimpan media kamu ke lokasi yang jauh setelah internet kamu dipulihkan, pertimbangkan juga apakah perlu media kamu dienkripsi saat dalam perjalanan dan saat berada di lokasi yang jauh, seperti yang dilakukan oleh aplikasi EyeWitness.

Perlu diingat bahwa walaupun enkripsi di sebagian besar tempat legal, beberapa negara mungkin memiliki hukum yang membatasi atau mengkriminalkan penggunaannya. Peta ini (komprehensif, tetapi dibuat pada 2017) memberikan tempat awal yang baik jika kamu memiliki pertanyaan tentang undang-undang di negera kamu.

Apakah aplikasi menangkap metadata penting (tanpa internet)?

Metadata adalah data yang menggambarkan video atau fotomu, seperti waktu dan tanggal atau lokasi. Informasi ini bermanfaat untuk mengidentifikasi, memahami, mengotentikasi, dan memverifikasi video atau fotomu sebagai dokumentasi dari peristiwa tertentu. Dalam konteks internet *shutdown*, kemampuan aplikasi untuk secara otomatis mengumpulkan metadata tertentu dan/atau memungkinkan kamu untuk dengan mudah memasukkan informasi deskriptif yang berguna di tempat itu sangat berguna, karena mungkin ada jangka waktu yang lama sebelum kamu dapat membagikan dokumentasi dengan siapa pun (yang mana kamu mungkin sudah lupa detail waktu, keadaan mungkin berubah, dll, dll).

Sebagian besar aplikasi dokumentasi khusus seperti ProofMode telah meningkatkan fitur metadata, dan mengumpulkan lebih banyak metadata daripada aplikasi kamera bawaan yang khas. Metadata yang ditingkatkan mungkin mencakup berbagai data sensor, wifi terdekat atau sinyal bluetooth, data perangkat, hash kriptografi, dan informasi yang disediakan pengguna, yang semuanya dapat memfasilitasi autentikasi dan verifikasi media di kemudian hari.

Ingatlah bahwa selama *Internet shutdown*, kamu akan membutuhkan aplikasi yang tidak memerlukan transmisi data untuk menghasilkan atau merekam metadata. Beberapa aplikasi mungkin mengandalkan internet, alih-alih sensor piranti keras dari perangkat, untuk mengumpulkan

metadata tertentu. Misalnya, jika data lokasi diambil dari pencarian perangkat, metadata dapat mencerminkan lokasi terakhir tempat perangkat memiliki koneksi data, alih-alih posisi aktual dari piranti keras perangkat. Aplikasi ini juga idealnya memungkinkan kamu untuk menyimpan metadata secara lokal tanpa internet, termasuk menyimpan formulir apapun yang kamu isi (mis. "Mode offline" Tella).

Bisakah saya mengekspor data dari aplikasi?

Tergantung pada tujuanmu mendokumentasi, mungkin penting untuk dapat mengekspor dokumentasi video dan metadata-nya dari aplikasi, dalam format yang tidak eksklusif hanya untuk aplikasi. Yaitu, untuk dapat membuka, melihat dan menggunakan media dan metadata di luar aplikasi tersebut. Ada fitur untuk mengekspor akan membantumu dan orang lain untuk tidak bergantung pada satu aplikasi atau penyedia layanan untuk mengakses dokumentasi kamu, dan memberimu lebih banyak waktu untuk bekerja dengan konten yang akan datang. Ingatlah bahwa beberapa metadata mungkin tidak dapat dibaca jika kamu tidak memiliki akses ke database atau bagan konversi tertentu untuk menginterpretasikan angka-angka (misalnya, dalam kasus menara sel atau jaringan Wi-Fi).

Perhatikan bahwa beberapa aplikasi mungkin saja memiliki mekanisme penguncian yang tidak mengizinkan pengguna untuk mengekspor, sedangkan aplikasi lainnya mungkin saja memang tidak dirancang untuk mengekspor. Perlu diketahui juga bahwa beberapa aplikasi seperti *Eyewitness* dan *Atrocities*, mungkin saja tidak mengizinkan kamu untuk mengekspor, sampai kamu selesai mengunggah media ke server berbeda (yang membutuhkan akses internet), dan beberapa aplikasi mungkin mengizinkan pengguna untuk mengekspor ke media, namun tidak dengan meta datanya.

Jika kamu ingin mengekspor, idealnya kamu perlu mengizinkan aplikasi kamu untuk melakukan salinan file ekspor ke media dalam standar format teks yang dapat dibaca. Metadata *Tella*, sebagai contoh, ditaruh di dalam sebuah galeri Tella yang sudah terenkripsi, namun dapat diekspor ke dalam format CSV. Sebagai tambahan, dalam situasi *Internet Shutdown*, akan sangat penting untuk memiliki pilihan untuk mengekspor file ke aplikasi *offline* atau yang tidak tergantung pada internet. Kebanyakan aplikasi yang dapat mengekspor, memiliki sebuah menu “Berbagi/*Share*” yang dapat langsung berpindah ke menu berbagi, di mana mayoritas Android memiliki fitur ini. Sayangnya, pengembang aplikasi dapat mengubah menu berbagi ini, dan tidak ada konsistensi diantara aplikasi-aplikasi.

Untuk *file-file* berkuantitas besar, akan lebih efisien jika mengakses melalui aplikasi *file manager* dan menyalin *file*-nya dari sana, walaupun kamu mungkin saja tidak dapat mengakses metadatanya. Pilihan ini juga biasanya tidak tersedia di aplikasi-aplikasi yang menyediakan keamanan galeri tersendiri, dimana *file-file* tersebut dienkripsi di memori. Untuk *file-file* ini, akan sangat penting untuk memiliki fungsi berbagi di dalam aplikasi.

Lihat posting berikutnya dalam seri ini, “Mempertahankan Media yang dapat diverifikasi selama Internet Shutdown” dan bagan perbandingan aplikasi dokumentasi kami yang akan datang.