

Cara Pendokumentasian Selama Pemadaman Internet

Menyiapkan Ponsel untuk Dokumentasi Luring Seri Pendokumentasian Saat Internet Shutdown

Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?

Mempertahankan Media yang dapat diverifikasi selama Internet Shutdown

Mencadangkan Media Ponsel Tanpa Internet atau Komputer

Berbagi File dan Komunikasi Selama Internet Shutdown

Cara Pendokumentasian Selama Pemadaman Internet

Tulisan berseri dengan sejumlah tips praktis

Oleh [Yvonne Ng](#)

Dengan kontribusi dari [Arul Prakkash](#)

Terakhir diulas: 31 Januari 2020

Pada bulan Juni 2019, saat pelanggaran HAM dan krisis kemanusiaan terus berlangsung di Myanmar, Menteri Perhubungan dan Komunikasi negara tersebut [memerintahkan perusahaan telekomunikasi](#) untuk memadamkan layanan internet seluler di wilayah Rakhine dan tetangganya Chin. Pemerintah Myanmar mengklaim melakukan pemadaman (shutdown) “[untuk kepentingan umum](#)”, menyebutnya sebagai “gangguan pada perdamaian” dan “aktivitas ilegal”. Pada kenyataannya, pemadaman internet terhadap sejuta orang itu memotong akses ke informasi dan komunikasi mendasar serta mengganggu upaya kemanusiaan. Seperti [pernyataan](#) yang disampaikan Matthew Smith dari Fortify Rights, “Shutdown ini terjadi dalam konteks berlangsungnya genosida atas etnis Rohingya dan kejahatan perang terhadap Rakhine, dan bahkan jika ini ditujukan untuk menarget militan, tindakan ini jelas-jelas tidak sesuai proporsi.”

Pemadaman ini [dipulihkan sebagian di 5 kota kecil](#) pada September 2019, tapi masih terus berlangsung. Di bulan yang sama, di negeri tetangga Bangladesh di mana banyak suku Rohingya mengungsi, pemangku kekuasaan memerintahkan operator ponsel untuk [memblokir layanan 3G](#)

[dan 4G](#) di kamp pengungsian Rohingya dan berhenti menjual kartu SIM kepada suku Rohingya. Memasuki tahun 2020, [4 kota kecil di Rakhine](#) terus mengalami pemotongan akses dari dunia, dan Bangladesh [terus membatasi layanan servis](#) di kamp-kamp pengungsian.

Pendokumentasian Selama Pemadaman Internet

Secara global, pemadaman internet terus meningkat. Berdasarkan [kampanye #KeepItOn AccessNow](#), ada 128 pemadaman yang disengaja selama bulan Januari-Juli 2019, dibandingkan dengan total 196 pada 2018, dan meningkat tajam dari tahun 2017 sebanyak 106 pemadaman, dan 75 pada tahun 2016. Di seluruh dunia, pemerintah bersama perusahaan telekomunikasi, melakukan pemadaman internet sebagai strategi untuk menekan masyarakat, mencegah mobilisasi, serta menghentikan penyebaran dan pendokumentasian informasi terkait pelanggaran hak asasi manusia.

“Pemadaman internet dan pelanggaran hak asasi manusia berjalan beriringan.”

– *Berhan Taye, AccessNow*

Pemadaman internet bisa dilakukan dalam berbagai bentuk, termasuk pemblokiran terhadap [platform spesifik yang menargetkan aplikasi dan situs populer](#), [pemadaman data seluler](#), [pembatasan bandwidth](#), atau [pemadaman total internet](#). Semua jenis *shutdown* ini bertujuan untuk mengganggu penyampaian informasi dan pengungkapan berbagai pelanggaran secara *real-time*. Hal ini sering terjadi selama unjuk rasa, pemilihan umum, dan periode ketidakstabilan politik, serta seringkali disertai dengan meningkatnya penindasan oleh negara, serangan militer dan kekerasan. Walaupun pemerintah mencoba untuk membenarkan *shutdown* [atas nama keamanan publik atau alasan lainnya](#), *shutdown* jelas dilakukan pada saat negara takut kehilangan kendali atas masyarakat, informasi, atau narasi politik. *Shutdowns* melanggar hak asasi manusia, sangat mengganggu [kehidupan dan mata pencaharian](#), serta berdampak pada [ekonomi global](#).

Mendokumentasikan pelanggaran HAM sama pentingnya selama pemadaman internet.

Bahkan jika informasi tidak dapat disebarkan pada saat itu, dokumentasi dapat menjadi cara untuk menjaga suara-suara yang berusaha dibungkam pihak berwenang, serta untuk mengamankan bukti pelanggaran yang dapat digunakan untuk menuntut pertanggungjawaban di kemudian hari. Proses pendokumentasian pelanggaran dan upaya menjaga dokumentasi ini tentu saja menjadi lebih menantang dan berisiko karena represi dan hambatan teknologi selama *internet shutdown*.

Bagaimana para aktivis bisa mengambil dan menyimpan video mereka selama *shutdown*, membagikannya secara *offline* dan melakukannya dengan lebih aman?

Dalam Seri Ini

Melalui kerja sama dengan para aktivis yang telah mengalami pemadaman internet, kami mempelajari beberapa tips dan pendekatan yang berguna untuk **mengambil dan menyimpan dokumentasi video selama *internet shutdown*** yang akan dibagikan melalui seri ini. Kami menulis tips ini untuk gawai Android, tetapi tips tersebut juga bisa diterapkan untuk iPhone. Beberapa strategi membutuhkan perencanaan terlebih dulu (dan seringkali, akses internet). Jadi sebaiknya baca, coba, dan terapkan dulu sebelum berada dalam situasi di mana sulit mendapatkan akses internet padahal harus melakukan pendokumentasian. Simpan salinan dari setiap tutorial sehingga

bisa dirujuk dan dibagikan selama *shutdown*. Terakhir, mulailah mempraktikkan teknik dan metode berikut dalam kegiatan sehari-hari, sehingga menjadi kebiasaan sebelum berada dalam krisis.

- **Persiapan**
 - [Menyiapkan ponsel untuk dokumentasi offline](#)
- **Pendokumentasian**
 - [Haruskah menggunakan aplikasi dokumentasi ini?](#)
- **Pemeliharaan**
 - [Menjaga media yang dapat diverifikasi selama *internet shutdown*](#)
 - [Mencadangkan media ponsel tanpa internet atau komputer](#)
- **Share dan Komunikasi**
 - [Berbagi file dan komunikasi selama *internet shutdown*](#)

Catatan akhir: Meskipun tips tersebut dapat membantu pendokumentasian selama pemadaman internet, kami menekankan bahwa solusi akhir adalah harus memulihkan akses internet dan berhasil membela [hak masyarakat untuk merekam](#), serta kebebasan berekspresi, informasi dan berkumpul. Untungnya, ada gerakan global yang dipimpin oleh organisasi seperti [NetBlocks](#), [AccessNow](#) dan lainnya yang secara aktif memantau dan berbagi informasi terkait *shutdown*. Para advokat secara global juga terlibat dalam [litigasi strategis terhadap shutdown](#). Kami berdiri dalam solidaritas dengan kerja-kerja mereka untuk menegakkan hak asasi manusia.

Menyiapkan Ponsel untuk Dokumentasi Luring Seri Pendokumentasian Saat Internet Shutdown

Also available in [Arabic](#), [Spanish](#) and [English](#).

Oleh [Yvonne Ng](#)

Dengan kontribusi dari [Arul Prakkash](#)

Artikel ini adalah bagian dari Seri [Pendokumentasian Selama Pemadaman Internet](#)

Terakhir diulas: 31 Januari 2020

Meskipun terjadi pemadaman internet, para dokumenter masih bisa mengambil bukti video penting yang dapat dibagikan secara luring (offline) atau saat mereka bisa kembali daring (online).

Berikut adalah beberapa kiat yang kami pelajari dari aktivis dan praktisi lain dalam menyiapkan ponsel untuk dokumentasi *offline*. Perhatikan bahwa beberapa langkah **memerlukan akses internet**, jadi harus dilakukan sebelum *shutdown* terjadi atau selama periode pemulihan. Selain itu, jangan menunggu sampai berada pada situasi darurat atau tegang untuk melakukan langkah-langkah ini; lakukan sekarang dan luangkan waktu **untuk berlatih menggunakan ponsel**

sebelum harus digunakan selama krisis.

Pemadaman internet sering bertepatan dengan kontrol terhadap informasi yang meningkat serta pembatasan kebebasan berekspresi dan berkumpul. Jika kamu melakukan dokumentasi foto/video/audio, lakukan tindakan pencegahan ekstra untuk melindungi diri dan informasi kamu selama periode ini. Jika ada risiko bahwa pihak berwenang akan menyita ponsel atau memaksa untuk membuka kunci dan menunjukkan kontennya (selama *shutdown* atau bukan), pertimbangkan untuk menggunakan ponsel untuk dokumentasi yang berbeda dari ponsel pribadi. Hal ini dapat membantu mengurangi informasi yang dapat dibocorkan (mis. kontak, pesan, akun, dll). Jika tidak bisa menggunakan gawai lain, panduan ini tetap dapat diikuti untuk mengurangi jumlah data sensitif dan meningkatkan keamanan pada ponsel utama.

Jika menggunakan ponsel lama, bersihkan dan hapus seluruh datanya terlebih dahulu

Untuk membersihkan ponsel, lakukan *Factory Reset* atau kembalikan pada pengaturan awal

Catatan: [Penelitian](#) menunjukkan bahwa melakukan *Factory Reset* tidak serta merta menghapus semua data. Faktanya, satu-satunya cara yang terbukti aman 100% untuk menghapus data adalah dengan menghancurkan ponsel, tetapi metode itu bukan pilihan jika kamu ingin menggunakan kembali ponsel tersebut! Pada [artikel ini](#), seorang teknisi Android menyarankan untuk memastikan konten pada gawai kamu dienkripsi sebelum *Factory Reset*. Enkripsi biasanya merupakan settingan awal pada sebagian besar ponsel saat ini, tetapi jika belum terenkripsi, buka Pengaturan > Keamanan > Enkripsi Telepon (Settings > Security > Encrypt Phone) sebelum mengatur ulang. Dengan cara ini, ketika dilakukan *Factory Reset*, kunci enkripsi akan hilang, dan semua data yang tidak terhapus tidak akan bisa dibaca.

Praktik keamanan dasar ponsel

Ada sejumlah praktik keamanan umum ponsel yang masih relevan di segala situasi, baik bagi mereka yang sedang mendokumentasikan selama *internet shutdown* atau tidak. [Berikut ini sejumlah sumber yang berguna bagi organisasi lain](#). Meskipun tidak ada yang menjamin 100% keamanan, sejumlah tips kunci meliputi:

- Pastikan ponsel terenkripsi. Ponsel lebih baru memiliki enkripsi *by default*. Kalau tidak yakin dengan ponsel yang digunakan, cek pengaturan keamanan di ponsel.
- Pastikan Sistem Operasi selalu *ter-update* secara rutin, karena kerap ada perbaikan celah keamanan.
- Perbaharui secara rutin aplikasi yang penting (seperti aplikasi Pesan Instan).
- Pasang kode sandi ponsel yang kuat yang memiliki setidaknya 6 digit dan tidak bergantung pada sidik jari / sentuhan atau ID wajah.
- Atur penguncian layar dan waktu penguncian.
- Matikan layanan lokasi jika kamu tidak membutuhkannya (termasuk layanan lokasi darurat, akurasi lokasi, riwayat lokasi, dan fitur berbagi lokasi, dan opsi pemindaian WiFi dan Bluetooth). Periksa juga izin lokasi untuk masing-masing aplikasi.

- Matikan Bluetooth dan WiFi saat tidak dibutuhkan, untuk menghindari pelacakan gawai.
- Matikan ponsel saat tidak digunakan.

Instal aplikasi dokumentasi yang berguna

Untuk dokumentasi foto atau video, gunakan aplikasi kamera bawaan pada ponsel. Atau gunakan aplikasi dokumentasi yang lebih khusus, seperti [ProofMode](#) atau yang lainnya, yang memungkinkan penangkapan metadata yang lebih kuat dan ekspor, identifikasi dan otentikasi, enkripsi, galeri aman, atau fitur lainnya.

Aplikasi yang berguna untuk mendokumentasikan suatu *shutdown* adalah [OONI Probe](#), aplikasi open-source yang menjalankan tes dari ponsel kamu untuk mengukur apakah situs atau platform sedang diblokir. Ini dapat menunjukkan bagaimana, kapan, di mana, dan oleh siapa situs diblokir. Pastikan untuk memahami [potensi resiko](#) sebelum menggunakan aplikasi ini.

Tidak yakin aplikasi dokumentasi mana untuk digunakan? Kami sediakan beberapa pertanyaan panduan dalam tutorial "Haruskah Saya Menggunakan Aplikasi Dokumentasi ini?".

Meng-*install* beberapa aplikasi sehari-hari

Hanya memiliki sedikit data dan aplikasi khusus di ponsel bisa memunculkan kecurigaan. Agar gawai terlihat seperti ponsel sehari-hari, pasanglah beberapa aplikasi yang umumnya digunakan di lokasi di mana kamu melakukan dokumentasi (tetapi mereka diunduh dari sumber-sumber terpercaya), dan mengambil beberapa foto tidak berbahaya dari galeri kamu.

Untuk aplikasi media sosial, kamu mungkin bisa membuat dan masuk akun-akun alternatif. Meskipun harus diingat bahwa membuat akun palsu melanggar Ketentuan Penggunaan sebagian besar platform, dan persyaratan verifikasi identitas beberapa aplikasi mungkin susah dipalsukan. Selain itu, kamu juga memerlukan waktu cukup lama untuk membuat konten dan menambahkan teman.

Meng-*install* aplikasi ketika tidak ada internet

Mengunduh dan menginstal aplikasi tanpa akses internet merupakan tantangan. Kamu perlu mengunduh aplikasi terlebih dahulu jika kamu mengantisipasi adanya pemadaman internet.

Salah satu strategi yang dapat membantu kamu dan orang lain di kemudian hari adalah mengunduh dan menyimpan file Paket Android (.apk) untuk aplikasi (**diunduh dari sumber terpercaya**, mis. langsung dari pengembang) di penyimpanan ponsel atau di drive. Memiliki APK ini secara *offline* memungkinkan kamu atau orang lain untuk berbagi aplikasi ketika tidak ada internet.

Meskipun kami belum berkesempatan mencobanya, aplikasi [F-Droid](#) menyediakan antarmuka untuk menukar APK ini secara *offline*. Inilah [tutorial](#) mereka.

Jangan simpan informasi riil pribadi/informasi sensitif di luar gawai

Cobalah untuk memiliki gawai khusus untuk melakukan dokumentasi. Jangan menggunakannya untuk email, panggilan telepon, atau pesan dengan kontak pribadi atau aktivis yang dapat berisiko, dan jangan sambungkan gawai ini ke akun riil dan/atau akun utama kamu.

Gunakan fitur-fitur untuk mengaburkan konten

Jika ponsel kamu diutak-atik, mungkin akan membantu jika pada ponsel, kamu menyamarkan intensimu atau membuat kontenmu lebih sulit ditemukan. Untuk mengantisipasi situasi di mana ponsel kamu hanya akan diperiksa (orang lain) secara dangkal dan cepat, kamu dapat menggunakan taktik sederhana seperti:

- Mengubah nama dan ikon pintasan aplikasi dengan menggunakan aplikasi Launcher (mis. [Nova Launcher](#), tetapi ada banyak ikon dan nama yang sama) sehingga aplikasi tertentu menjadi kurang jelas.
- Menggunakan fitur privasi bawaan seperti [Mode Pribadi](#) (Samsung) atau [Content Lock](#) (LG), jika ponsel kamu mendukungnya.
- Menempatkan file kosong bernama ".nomedia" di dalam folder apa saja yang ada, untuk mencegah media di folder muncul di galeri kamu. Catatan: Jika media masih muncul, kamu mungkin perlu menghapus cache Galeri kamu. Ini mungkin tidak sama hasilnya di semua gawai.
- Membuat folder tersembunyi (folder yang dimulai dengan ".") dengan menggunakan aplikasi manajer file. kamu dapat memindahkan file ke folder tersembunyi tersebut secara manual, atau jika bisa juga menggunakan aplikasi kamera seperti [Open Camera](#). Kamu dapat menentukan di mana media yang kamu rekam disimpan. Pastikan untuk mematikan opsi "tampilkan file tersembunyi" di Pengaturan kamu sehingga file yang tersembunyi tidak terlihat.
- Beberapa aplikasi dokumentasi khusus, seperti [Tella](#) atau [Eyewitness to Atrocities](#), menyimpan dokumentasi di galeri terenkripsi terpisah yang isinya hanya dapat diakses di dalam aplikasi, mungkin membuatnya kurang dapat dilihat jelas bagi seseorang yang mengutak-atik mencari-cari di ponsel kamu. Dokumentasi di galeri yang aman ini memerlukan kode sandi aplikasi yang terpisah, sehingga tetap dienkripsi bahkan ketika ponsel kamu tidak terkunci.

Catatan penting tentang mengaburkan konten kamu

Penting untuk dicatat bahwa teknik-teknik di atas mungkin cukup untuk menghindari seseorang untuk dengan cepat menggeser-geser tampilan ponsel kamu, tetapi tidak akan secara efektif menyembunyikan kontenmu dari seseorang yang benar-benar menyelidiki.

Ingat juga bahwa beberapa negara mungkin memiliki undang-undang yang membatasi atau mengkriminalkan penggunaan aplikasi keamanan yang mengenkripsi atau menghapus data kamu.

Menggunakan aplikasi tersebut untuk mencegah pihak berwenang mengakses data kamu dapat dilihat sebagai menghancurkan bukti atau menghambat penyelidikan, dan dapat dihukum sebagai kejahatan. [Peta](#) ini (komprehensif, tetapi dibuat pada tahun 2017) memberikan awalan yang baik jika kamu memiliki pertanyaan tentang undang-undang di negara kamu.

Persiapan Berbagi Luring/Offline

Ketika berada dalam situasi *offline*/luring, kamu mungkin ingin tetap menghapus beberapa dokumentasi, baik atas dasar keamanan, mengosongkan tempat penyimpanan, atau membagikannya dengan orang lain. Menghapus dokumentasi secara rutin di ponsel kamu, akan membantu mengurangi informasi jika dicuri atau dibuka kunci pengamannya.

Walaupun kamu tidak terhubung ke internet, kamu tetap dapat mengakses wifi atau bluetooth lokal yang ada di dalam ponsel, seperti melalui ponsel lain atau perangkat wifi USB. Ponsel kamu seharusnya sudah memiliki sebuah aplikasi untuk terhubung dengan kedua fitur diatas. Jika mendukung, kamu dapat memasang perangkat USB On-The-Go (OTG) guna memindahkan dokumentasi ke gawai lain.

Metode tersebut dapat didiskusikan secara lebih rinci di tutorial "[Cara berbagi data dan berkomunikasi ketika Internet Shutdown](#)" dan video "[As Evidence: Tech Tools — Transferring Files](#)".

Berlatihlah sebelum kamu berada dalam situasi krisis

Setel ponselmu sekarang, selagi kamu sedang memiliki akses internet. Mulai berlatih menggunakan aplikasi dalam situasi sehari-hari (di mana tidak ada masalah keamanan) agar terbiasa dan nyaman menggunakannya. Jadikan keamanan dasar telepon yang baik sebagai praktik sehari-harimu. Dengan cara ini, metode yang digunakan kemudian akan menjadi hal yang biasa ketika kamu berada dalam situasi krisis saat banyak hal yang perlu dikhawatirkan.

Lihat posting berikutnya dalam seri ini, "[Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?](#)"

Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?

Seri Mendokumentasikan selama Pemadaman Internet

Also available in [Arabic](#), [Spanish](#) and [English](#).

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 dijangka.

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 negara 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 mengeksport data dari aplikasi?

Tergantung pada tujuanmu mendokumentasi, mungkin penting untuk dapat mengeksport 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 mengeksport 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 mengeksport, sedangkan aplikasi lainnya mungkin saja memang tidak dirancang untuk mengeksport. Perlu diketahui juga bahwa beberapa aplikasi seperti *Eyewitness* dan *Atrocities*, mungkin saja tidak mengizinkan kamu untuk mengeksport, sampai kamu selesai mengunggah media ke server berbeda (yang membutuhkan akses internet), dan beberapa aplikasi mungkin mengizinkan pengguna untuk mengeksport ke media, namun tidak dengan meta datanya.

Jika kamu ingin mengeksport, 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 mengeksport file ke aplikasi *offline* atau yang tidak tergantung pada internet. Kebanyakan aplikasi yang dapat mengeksport, 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.

Mempertahankan Media yang dapat diverifikasi selama Internet Shutdown

Oleh [Yvonne Ng](#)

Dengan kontribusi dari [Arul Prakkash](#)

Artikel ini adalah bagian dari Seri [Pendokumentasian Selama Pemadaman Internet](#)

Also available in [Arabic](#), [Spanish](#) and [English](#).

Ulasan terakhir: 31 Januari 2020

[Pembela HAM](#), [penyidik](#), [peneliti](#), dan [jurnalis](#) biasanya bergantung pada dokumentasi awal dari

saksi untuk melakukan pemantauan, pelaporan, dan menganalisis pelanggaran HAM. Guna memastikan mereka tetap menggunakan informasi yang tepat, pengguna-pengguna ini dapat melakukan otentifikasi dan verifikasi dokumentasi yang mereka dapatkan--di mana proses ini memakan waktu yang cukup lama.

Sebagai pendokumentasi, terdapat beberapa langkah sederhana yang dapat kamu lakukan dalam melakukan verifikasi dan memperkuat informasi, sehingga dapat digunakan secara efektif dan sesuai. Berikut beberapa langkah ekstra yang mungkin dapat berguna selama *Internet Shutdown*, yang mempertimbangkan:

- Jika kamu tidak dapat mengunggahnya langsung, fitur tanggal dan lokasi dari publikasi yang disediakan oleh media sosial tidak cukup bermanfaat untuk menunjukkan bahwa video tersebut direkam pada tanggal atau lokasi tertentu
- Jika rekan lainnya tidak dapat mengunggah juga, akan sangat sedikit dokumentasi yang tersedia secara keseluruhan yang dapat digunakan untuk memperkuat video kamu
- Jika kamu membutuhkan untuk menggeser perekam kamu ke banyak orang secara *offline* untuk sampai ke lokasi tujuan, akan sangat sulit bagi yang lainnya untuk melacak sumber video tersebut
- Jika kamu ingin menghapus video asli dari ponsel kamu karena pertimbangan keamanan atau kapasitas memori yang terbatas, atau jika kamu ingin menyingkirkan ponsel tersebut, akan sangat sulit untuk mengkonfirmasi keaslian dari video tersebut.
- Jika kamu lupa rincian dari video tertentu dan aplikasi yang digunakan tidak mencatat rincian tersebut, rekan lain mungkin akan sulit mengidentifikasinya di masa depan.

Saran di bawah ini dapat membantu kamu menjaga kualitas video kamu selama *Internet Shutdown*.

Film atau mengidentifikasi rincian di dalam video

Sertakan rincian di dalam video kamu sehingga dapat memudahkan bagi penyidik atau jurnalis dalam mengidentifikasi waktu dan tempat, seperti tempat unik, garis langit, penanda jalan, etalase toko, plat kendaraan, bendera, jam, halaman depan koran, dan lainnya. kamu juga dapat menarasikan informasi dasar seperti namamu dan informasi kontak (jika aman), waktu, tanggal, dan lokasi atau koordinat GPS. Semakin rinci informasi tersebut, akan semakin mudah bagi orang lain dalam melakukan pencarian dan memverifikasi video tersebut di kemudian hari.

Cari tahu saran lain di [Basic Practices for Capturing, Storing, and Sharing](#).

Menambahkan deskripsi / metadata

Ambil keuntungan dari aplikasi yang memiliki fitur dokumentasi yang spesifik menggunakan metadata atau informasi teknis dari dalam ponsel, dan izinkan agar dapat secara manual menambahkan informasi deskriptif lain. Perlu diingat bahwa selama *Internet Shutdown*, dibutuhkan sebuah aplikasi yang tidak bergantung pada akses internal untuk merekam atau menyimpan metadata.

Lihat "[Haruskah menggunakan aplikasi dokumentasi ini?](#)" untuk mengetahui cara memilih

aplikasi yang sesuai.

Bahkan jika kamu tidak menggunakan sebuah aplikasi yang memiliki fitur dokumentasi spesifik, kamu tetap dapat membuat informasi tambahan ke dalam lembar catatan, peta, atau foto dalam ponsel kamu. Kamu dapat membuat videomu dengan informasi tambahan tersebut dengan menggunakan aplikasi file manager favoritmu.

Informasi tambahan kunci meliputi waktu, tanggal, lokasi, dan juga sumber perekaman (namamu dan kontak informasi, jika aman). Pindahkan ke dalam metadata dan sertakan itu ke dalam sebuah video ketika membagikannya.

Simpanlah Cadangan

Cadangkan media dari ponsel kamu secara rutin, idealnya dua kali di dalam dua perangkat penyimpanan yang berbeda. Kamu dapat menghubungkannya dengan On-the-GO (OTG) atau perangkat *wireless* (nirkabel) ke ponsel, bahkan tanpa komputer. Lihat rinciannya di "[Membuat salinan media di ponsel tanpa internet atau komputer](#)".

Menyimpan cadangan dapat meminimalisir salinan video hilang jika ponsel kamu hilang atau hancur, atau saat kamu butuh untuk menghapus video dari ponsel.

Memiliki salinan yang aman dari video asli juga dapat membuat kerja penyidik atau jurnalis menjadi lebih mudah.

Lihat lebih lengkap di seri berikutnya, "[Mencadangkan media ponsel tanpa internet atau komputer](#)".

Mencadangkan Media Ponsel Tanpa Internet atau Komputer

Oleh [Yvonne Ng](#)

Dengan kontribusi dari [Arul Prakkash](#)

Artikel ini adalah bagian dari Seri [Pendokumentasian Selama Pemadaman Internet](#)

Also available in [Arabic](#), [Spanish](#) and [English](#).

Terakhir diulas: 31 Januari 2020

[Cadangan](#) merupakan kunci dalam memastikan data dan dokumentasi kamu tidak terhapus, rusak, atau hilang secara tiba-tiba apabila perangkat kamu hilang.

Selama *Internet Shutdown* atau penurunan kecepatan internet, kamu mungkin tidak dapat secara rutin mengoperasikan cadangan *cloud* atau mengirimkan dokumentasi kamu ke lokasi penyimpanan yang aman.

Memindahkan dari desktop atau laptop merupakan cara lain dalam melakukan pencadangan, namun karena banyak orang tidak memiliki akses ke komputer, berikut beberapa pilihan dan saran untuk mencadangkan media dari ponsel kamu selama internet shutdown tanpa komputer.

Gunakan OTG atau Drive Nirkabel (*Wireless*)

OTG atau perangkat *on-the-go*, merupakan tipe USB yang cocok dengan banyak (meski tidak semua) Android. Kamu dapat memasang perangkat kabel OTG secara langsung ke ponsel kamu, atau menggunakan adapter *OTG-to-USB* untuk menghubungkan ponsel kamu ke perangkat keras USB yang reguler. Dengan OTG, ponsel kamu menyediakan daya ke perangkat.

Merek populer dari OTG termasuk SanDisk, Kingston, dan Samsung, meskipun sebenarnya ada banyak lainnya. Biasanya seharga 8-25 USD tergantung dari kapasitas penyimpanan.

Perangkat nirkabel/perangkat keras serupa dengan perangkat keras pada umumnya, kecuali tidak memerlukan kabel. Hal ini memungkinkan untuk menghubungkan perangkat yang biasanya tidak terhubung ke perangkat keras, misalnya ponsel kamu.

Keunggulan dari perangkat nirkabel dibandingkan perangkat OTG adalah kamu dapat menghubungkan banyak pengguna ke satu perangkat dalam waktu bersamaan. Hal ini dapat bermanfaat, misalnya, ketika dalam situasi protes ketika kamu sedang membuat film dalam sebuah tim--semua rekaman dari tiap orang dapat dicadangkan ke sebuah perangkat keras yang tiap anggota tim lain dapat gunakan.

Perhatikan apabila mereka tidak menyerap daya dari perangkat lain, perangkat nirkabel bergantung pada daya baterai dan butuh di-charge.

SanDisk mungkin sebuah brand yang paling populer dari perangkat keras, walaupun ada yang lainnya. Perangkat nirkabel secara umum lebih mahal dari perangkat OTG, dan berkisar antara 25-100 USD tergantung pada kapasitas penyimpanan. Perangkat keras eksternal mulai berkisar dari 150 USD tergantung pada kapasitas penyimpanan.

Alternatif: Gunakan ponsel lama yang tidak terpakai

Jika tidak memiliki OTG atau perangkat nirkabel, tetapi memiliki ponsel lama yang tidak digunakan tetapi masih berfungsi, kamu juga bisa menggunakannya sebagai cadangan. Selama kedua ponsel berada dalam jangkauan fisik, kamu bisa menyambungkan dan menyalin media dari satu perangkat ke perangkat lainnya melalui Bluetooth, WiFi Direct, atau Near Field Communication (NFC)/Android Beam. Bluetooth dan WiFi Direct merupakan teknologi nirkabel yang dapat menyambungkan kedua perangkat tanpa menggunakan *router* atau *access point* di antara keduanya. WiFi Direct menyediakan cakupan yang lebih luas dan data transfer yang lebih cepat daripada Bluetooth, tetapi menghabiskan lebih banyak energi. Sedangkan NFC memiliki jangkauan yang jauh lebih pendek (~4

cm) dan kecepatan transfer yang lebih lambat, tetapi terhubung lebih cepat dan menggunakan daya yang lebih hemat, sehingga berguna untuk mengalihkan sesuatu yang kecil dengan cepat jika memiliki kedua perangkat di tangan.

Ponsel kamu barangkali telah dilengkapi dengan fitur Bluetooth, WiFi Direct, atau NFC bawaan yang memungkinkan dapat memilih perangkat mana yang bisa dibagikan. Jika pada kedua ponsel terpasang Files By Google, kamu juga bisa membagikan file secara offline menggunakan aplikasi tersebut.

Penting: kekurangan dari kemudahan koneksi yang disediakan oleh layanan tersebut adalah hal tersebut tidak aman. Bluetooth dan pemindai wifi dapat digunakan untuk melacak lokasi atau menyelidiki perangkat kamu demi mendapatkan informasi. Penyusup dapat mencoba untuk terhubung dengan perangkat kamu, mengirim kamu file yang tidak diinginkan, atau bahkan menguasai perangkat jika rentan. **Agar lebih aman, matikan layanan ini ketika tidak digunakan dan hanya nyalakan saat berada di tempat yang aman, batasi izin aplikasi hanya untuk apa / siapa yang dibutuhkan, serta praktikkan keamanan ponsel yang baik; seperti melakukan *update* dan menggunakan kata sandi yang kuat.**

Sertakan deskripsi/metadata yang terpisah

Saat menyalin media ke perangkat OTG, perangkat nirkabel, atau ponsel lama, ada baiknya menyertakan informasi deskriptif atau metadata yang mungkin terpisah dari media. Banyak aplikasi dokumentasi menghasilkan dokumen teks CSV atau JSON yang menyertakan metadata yang ditarik dari perangkat (mis. Geolokasi, waktu, tanggal) dan deskripsi apapun yang dimasukkan secara manual oleh pengguna. Pastikan untuk mengeksport dan memasukkan dokumen metadata ini ke dalam cadangan juga.

Lindungi perangkat dengan kata sandi

Banyak drive nirkabel dapat dilindungi oleh kata sandi dengan aplikasi seluler yang disertakan bersama drive tersebut. Perhatikan bahwa perlindungan kata sandi tidak sama dengan enkripsi (lihat di bawah). Sebagian besar perangkat nirkabel atau OTG tidak bisa mengaktifkan *full-disk encryption* (FDE) jika hanya menggunakan ponsel, meskipun perangkat tersebut mungkin dienkripsi dengan penuh jika menggunakan komputer.

Pertimbangkan untuk mengenkripsi file

Jika ingin menyimpan file dengan lebih aman, kamu mungkin perlu mempertimbangkan untuk mengenkripsi *file* cadangan. Meskipun kamu mungkin tidak dapat mengenkripsi sebagian besar drive nirkabel atau OTG dengan ponsel, tetapi kamu dapat mengenkripsi *file* itu sebelum dipindahkan ke drive. Beberapa aplikasi dapat digunakan untuk mengenkripsi *file* di Android

termasuk [ZArchiver](#), dan [RAR](#). Ketahuilah bahwa kata sandi enkripsi harus diingat, karena tidak ada cara untuk memulihkan *file* yang terenripsi jika kamu kehilangan kata sandi.

Perlu diingat bahwa beberapa negara mungkin memiliki undang-undang yang membatasi atau mengkriminalisasi penggunaan enkripsi. Menggunakannya untuk mencegah pihak berwenang mengakses data kamu dapat dianggap menghancurkan bukti atau menghambat penyelidikan, dan dapat dihukum sebagai kejahatan. [Peta 2017](#) ini mungkin sudah usang tetapi menyediakan informasi awal yang baik jika ada pertanyaan tentang undang-undang di negaramu.

Buat 2 cadangan di lokasi yang berbeda

Satu *backup* (cadangan) tidak selalu dapat diandalkan. Misalnya, kamu mungkin kehilangan perangkat cadangan, merusaknya, atau mungkin gagal secara acak. Pakar TI biasanya menyarankan orang untuk memiliki 2 cadangan (mis. total 3 salinan), pada perangkat berbeda yang disimpan di lokasi terpisah. Ini membantu mengurangi berbagai risiko terhadap satu salinan tertentu.

Lihat pos terakhir dalam seri ini, ["Berbagi File dan Komunikasi Selama Internet Shutdown."](#)

Berbagi File dan Komunikasi Selama Internet Shutdown

Artikel ini adalah bagian dari Seri [Pendokumentasian Selama Pemadaman Internet](#)

Oleh [Yvonne Ng](#)

Dengan kontribusi dari [Arul Prakkash](#)

Also available in [Arabic](#), [Spanish](#) and [English](#).

Terakhir diulas: 31 Januari 2020

Internet shutdown dan kerusuhan yang sedang berlangsung di Kashmir merupakan internet shutdown terlama yang pernah diberlakukan dalam iklim demokrasi, juga menimbulkan [dampak bencana](#) pada kehidupan orang-orang di wilayah tersebut. Lebih parah lagi, pada Desember 2019, [akun WhatsApp warga Kashmir mulai dicabut](#) sesuai kebijakan WhatsApp karena tidak aktif selama 120 hari.

Pada saat penulisan ini pada Januari 2020, Mahkamah Agung India memutuskan bahwa internet shutdown tidak terbatas di Kashmir adalah [ilegal dan merupakan penyalahgunaan kekuasaan](#). Pembatasan internet broadband dan mobile telah dipulihkan di beberapa daerah, tetapi hanya berlaku untuk situs web yang masuk daftar putih.

Internet shutdown dirancang untuk memblokir orang dari berbagi informasi dan berkomunikasi (dan

juga mendorong orang ke bentuk komunikasi yang kurang aman seperti ponsel dan SMS, yang lebih mudah bagi pihak berwenang untuk menyadap dan memantau). Tidak selalu ada solusi yang baik selama total internet shutdown. Selama periode ketat penutupan di Kashmir, misalnya, orang terpaksa [menggunakan catatan tulisan tangan dan kurir](#) untuk mengirim pesan ke orang yang mereka cintai.

Kami tidak memiliki cara ampuh untuk menghindari semua pemadamam internet, tetapi melalui percakapan dengan aktivis dan rekan-rekan, kami telah mempelajari beberapa metode dan pendekatan untuk berbagi secara *offline* dan komunikasi yang mungkin bekerja untuk kamu, tergantung pada keadaan. Perhatikan bahwa beberapa opsi ini memerlukan pengaturan internet pada awalnya (mis. Untuk mengunduh aplikasi, dll).

Berbagi dokumen secara langsung lewat Bluetooth, Wifi Direct, atau NFC

Kamu tidak perlu memiliki koneksi internet untuk menghubungkan ponselmu dengan perangkat terdekat lainnya melalui Bluetooth, Wifi Direct, atau Near Field Communication (NFC) (kadang-kadang disebut Android Beam pada perangkat yang lebih lama). Bluetooth dan Wifi Direct adalah teknologi nirkabel yang dapat "memasangkan" dua perangkat tanpa *router* atau titik akses di antaranya. WiFi Direct menyediakan jangkauan yang lebih luas dan transfer data yang lebih cepat daripada Bluetooth, tetapi menggunakan daya yang jauh lebih besar. Sementara itu, NFC memiliki jangkauan yang jauh lebih pendek (~ 4cm) dan kecepatan transfer yang lebih lambat daripada Bluetooth atau WiFi Direct, tetapi menghubungkan lebih cepat dan menggunakan daya lebih sedikit, sehingga dapat berguna untuk transfer kecil ketika kedua perangkat berada di tangan kamu.

Kamu mungkin memiliki fitur Bluetooth, WiFi Direct, dan NFC di dalam ponselmu yang muncul dalam opsi berbagi kamu. Selain itu, aplikasi dengan fitur berbagi file, seperti [Files By Google](#), juga mengintegrasikan teknologi ini.

Catatan Penting: kerugian dari kemudahan koneksi yang disediakan oleh layanan ini adalah bahwa hal tersebut tidak aman. Bluetooth dan wifi beacon / scanner dapat digunakan untuk melacak lokasimu atau menyelidiki perangkatmu untuk mendapatkan informasi. Penyusup dapat mencoba *pairing* dengan perangkatmu, mengirimimu file yang tidak diinginkan, atau bahkan menguasai perangkatmu jika rentan. Agar lebih aman, matikan layanan ini ketika kamu tidak menggunakannya dan hanya nyalakan saat kamu berada di tempat yang aman, batasi izin aplikasi hanya untuk apa / siapa yang kamu butuhkan, dan praktikkan keamanan telepon yang baik seperti menjalankan update dan menggunakan sandi yang kuat.

Berbagi dokumen lewat *hard drive* nirkabel atau via Wireless Local Area Network (WLAN)

Hard drive nirkabel atau *flash drive* dapat digunakan untuk berbagi *file* di antara tim, atau beberapa orang sekaligus. *Drive* wifi biasanya datang dengan instruksi dan / atau aplikasi untuk menghubungkan ponselmu ke *drive*, dan relatif mudah digunakan. Ingatlah untuk mengatur kata sandi di *drive* untuk keamanan.

Jika kamu tidak memiliki *drive* nirkabel, kamu juga dapat berbagi *file* di *drive* USB biasa dengan menghubungkannya ke *router* nirkabel. *Router* perjalanan dengan *port* USB, misalnya, relatif murah dan sangat portabel. Pengguna dapat terhubung ke *drive* USB melalui jaringan lokal (tidak perlu internet). Untuk mengakses *file* pada drive USB yang terhubung pada ponselmu, kamu harus menggunakan aplikasi manajer *file* yang dapat terhubung ke penyimpanan jaringan, seperti [Solid Explorer](#). Alamat IP router kamu biasanya dapat ditemukan di pengaturan wifi canggih ponselmu.

Sementara itu, opsi lain adalah [PirateBox](#), proyek *do-it-yourself* yang menyediakan perangkat lunak berlisensi gratis. Pengguna dapat berbagi *file* seperti di atas, tetapi Piratebox memungkinkan mereka melakukannya secara anonim, dan juga menyertakan fitur obrolan dan pesan. Menyiapkan Piratebox membutuhkan pengunduhan, penginstalan, dan pengaturan beberapa perangkat lunak. [Instruksi](#) ada di situs web Piratebox.

Kabar: proyek Pirate Box perlahan diakhiri. Situs web dan repositori github masih online, tetapi pengembang utama proyek tidak lagi secara aktif mengembangkannya.

Komunikasi lewat percakapan *Peer-to-Peer* (P2P)

Dua aplikasi *peer-to-peer* perpesanan baru yang kami ketahui melalui jaringan aktivis adalah [Briar](#) dan [Bridgefy](#). Kami belum mencobanya, tetapi kami tahu orang lain yang mengujinya.

[Briar](#) adalah aplikasi pesan terenkripsi *open-source* terpercaya, yang tidak bergantung pada server pusat, melainkan menyinkronkan pesan di antara perangkat pengguna (sehingga konten tinggal di perangkat masing-masing pengguna). Briar dapat menyinkronkan bahkan ketika tidak ada internet, menggunakan Bluetooth atau WiFi (ketika ada internet, aplikasi menyinkronkan perangkat melalui jaringan [Tor](#)). Briar juga menampilkan grup pribadi, forum publik, dan blog. Saat menggunakan secara *offline*, jangkauanmu dibatasi oleh rentang Bluetooth atau WiFi (maksimum ~ 100 meter).

Sementara itu, [Bridgefy](#) adalah aplikasi pesan terenkripsi terpercaya (kecuali ketika menggunakan fitur "siaran") yang menggunakan Bluetooth untuk mengirim pesan. Tidak seperti Briar, pesan dapat menempuh jarak yang lebih jauh dengan melompat di sepanjang jaringan *mesh* dari pengguna Bridgefy lainnya (hanya penerima yang dituju dapat membaca pesan). Bridgefy tidak memiliki grup pribadi Briar, forum, dan fitur blog, tetapi memiliki mode Broadcast agar kamu dapat mengirim pesan ke hingga 7 pengguna Bridgefy dalam jangkauan, yang tidak perlu menjadi kontakmu (pesan Broadcast karena kebutuhan tidak terenkripsi).

Komunikasi lewat SMS terenkripsi

Pesan teks SMS dikirim melalui jaringan seluler dan tidak bergantung pada internet, jadi mungkin masih berfungsi selama *internet shutdown*. Namun, SMS dianggap sangat tidak aman. Tidak seperti aplikasi yang bergantung pada internet seperti WhatsApp atau Signal, SMS tidak dienkripsi ujung ke ujung (*end-to-end encryption*). Ini berarti bahwa pesan teks (dan metadata mereka) dapat dibaca oleh pemerintah dan operator seluler, atau dicegat oleh peretas. SMS juga dapat "dipalsukan," yang berarti bahwa pengirim dapat memanipulasi informasi alamat mereka untuk menyamar sebagai

pengguna lain.

Jika kamu perlu menggunakan SMS, [Silence](#) adalah aplikasi yang mengenkripsi pesan SMS secara end to end. Aplikasi ini adalah *open-source program* dan menggunakan protokol enkripsi Signal. Meskipun kami belum mencobanya sendiri, kami telah mendengar bahwa orang lain telah menggunakannya. Baik pengirim dan penerima harus menginstal dan bertukar kunci satu sama lain. Karena pesan SMS harus melalui server telekomunikasimu, bahkan dengan Silence kenyataan bahwa kamu mengirim pesan terenkripsi dan metadata tentang pesanmu akan dapat diakses oleh perusahaan telekomunikasi.

Shutdown sebagian: Memotong pemblokiran situsweb

"Internet shutdown" seringkali tidak berarti pemadaman internet total, melainkan memblokir akses ke situs web atau *platform* media sosial tertentu. Pemerintah, melalui penyedia layanan internet (ISP), dapat memblokir situs berdasarkan alamat IP, konten, atau melalui pencarian DNS. Tidak yakin apakah suatu situs sedang diblokir? Organisasi seperti [Open Observatory of Network Interference](#) (OONI) dan [Netblocks](#) memantau dan mengukur gangguan internet dan sensor di seluruh dunia.

Untungnya, selama kamu memiliki akses internet, ada beberapa cara untuk mencoba menyiasati sebagian blok. Seperti halnya enkripsi, perlu diingat bahwa menghindari situs yang diblokir dapat dikriminalisasi di negaramu.

VPN

Salah satu cara untuk memotong pemblokiran berbasis IP dan berbasis konten adalah dengan menggunakan VPN, seperti [ProtonVPN](#) atau [TunnelBear](#). Ketika kamu terhubung melalui VPN, lalu lintas internet kamu dienkripsi dan dialihkan melalui server VPN di lokasi lain, seperti di negara lain, sehingga menyembunyikan tujuan sebenarnya dan konten lalu lintas kamu ke ISP.

Ingatlah bahwa beberapa pemerintah melarang penggunaan VPN atau mungkin mencoba mendeteksi dan memblokir koneksi VPN. Penting juga untuk menggunakan penyedia VPN yang dapat dipercaya, sebaiknya yang tidak menyimpan data atau log, karena penyedia akan dapat melihat aktivitas internetmu. Berhati-hatilah dengan negara mana penyedia VPN itu berada, dan proses hukum apa yang harus mereka patuhi berdasarkan yurisdiksinya. Juga pertimbangkan bahwa VPN yang disetujui pemerintah sebenarnya dapat mengaktifkan pengawasan dan inspeksi datamu.

Server DNS

Server DNS ("sistem nama domain") berfungsi dengan menerjemahkan nama domain atau URL yang diketik pengguna ke dalam browser ke alamat IP numerik yang digunakan internet untuk mengidentifikasi halaman web. ISP dapat memodifikasi server DNS yang dikontrolnya untuk memblokir pertanyaan tertentu, atau untuk mengembalikan halaman yang salah yang mengatakan bahwa situs web itu tidak ada.

Pada tahun 2014, Perdana Menteri Turki Recep Tayyip Erdoğan [berusaha memblokir Twitter](#) selama

pemilihan umum Turki menggunakan teknik ini. Larangan itu dengan [cepat digagalkan](#) oleh aktivis yang berbagi kiat langkah demi langkah tentang cara menggunakan VPN dan mengubah server DNS.

Twitter is blocked in Turkey. On the streets of Istanbul, the action against censorship is graffiti DNS addresses. pic.twitter.com/XcsfN7IJvS

— Utku Can (@utku) [March 21, 2014](#)

Main opposition party (CHP) in [#Turkey](#) publicizes DNS #'s to circumvent [#twitter](#) block. As seen in Istanbul pic.twitter.com/XjlvnudfgG

— Abdelrahman Ayyash (@3yyash) [March 21, 2014](#)

Kamu dapat mengubah server DNS default di jaringan atau pengaturan wifi ponsel kamu. Alih-alih server DNS default, kamu dapat menggunakan server DNS alternatif seperti [Google Public DNS](#).

Ini hanya dua cara untuk menghindari teknik pemblokiran yang paling umum. Lihatlah panduan bermanfaat dari [Internet Society](#), [Access Now](#), [Security-in-a-Box](#), dan [EFF](#) untuk informasi lebih lanjut.