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/XcsfN7lJvS
>
> — 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/XjIvnudfgG
>
> — 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 atau CloudFlare untuk menyiasati blok berbasis DNS. Cloudflare juga memiliki aplikasi bernama 1.1.1.1 yang memungkinkan pengguna untuk beralih ke server DNS Cloudflare melalui antarmuka aplikasi sederhana.

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.