

1. [Documenting During Internet Shutdowns](#) | အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

[Setting Up a Phone for Offline Documentation](#) | အော့ဖ်လိုင်း(offline) မှတ်တမ်းတင်ခြင်းအတွက် ဖုန်းကိုပြင်ဆင်(setup)ခြင်း

[Should I Use This Documentation App?](#) | “ဒီမှတ်တမ်းတင် app ကို သုံးသင့်ပါသလား?”

[Maintaining Verifiable Media During an Internet Shutdown](#) |

ခိုင်လုံသောမီဒီယာ အချက်အလက်များကို အင်တာနက်ဖြတ်တောက်ချိန်တွင် ထိန်းသိမ်းခြင်း

[Backing Up Phone Media Without Internet or a Computer](#) | ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲbackup အရန်သိမ်းခြင်း

[File Sharing and Communication During an Internet Shutdown](#) | အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဖိုင်ဝေမျှခြင်းနှင့် ဆက်သွယ်ခြင်း

<p>Documenting During Internet Shutdowns</p> <p>A blog series with practical tips.</p> <p>By Yvonne Ng With contributions by Arul Prakkash</p> <p>Last reviewed: 31 January 2020</p>	<p>အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း</p> <p>လက်တွေ့ကျသော အကြံပေးချက်များပါဝင်သည့်ဘလော့ဂ်စီးရီး</p> <p>ရေးသားသူ - Yvonne Ng ပံ့ပိုးသူ - Arul Prakkash</p> <p>နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်</p>
<p><i>In June 2019, as human rights abuses and a humanitarian crisis were continuing in Myanmar, the country’s Ministry of Transport</i></p>	<p>၂၀၁၉ ဇွန်လမှစ၍ မြန်မာနိုင်ငံတွင် လူ့အခွင့်အရေးချိုးဖောက်မှုနှင့်</p>

and Communication [directed telecom companies](#) to shut down their mobile internet service in parts of Rakhine State and neighboring Chin State. Citing “disturbances of the peace” and “illegal activities,” the Myanmar government claims to have enacted the shutdown “[for the benefit of the people](#).” In reality, the blackout cut [over a million people](#) off from access to essential information and communication, and disrupted humanitarian efforts. As Matthew Smith from Fortify Rights has [stated](#), “This shutdown is happening in a context of ongoing genocide against Rohingya and war crimes against Rakhine, and even if it were intended to target militants, it’s egregiously disproportionate.”

The shutdown was [partially lifted on five of the townships](#) in September 2019, but is ongoing. During the same month, in neighboring Bangladesh where many Rohingya have fled, authorities ordered mobile phone operators to [block 3G and 4G services](#) in Rohingya refugee camps and to stop selling SIM cards to Rohingya. As we enter 2020, [four townships in Rakhine](#) continue to be cut off from the world, and Bangladesh [continues to limit service](#) in the refugee camps.

လူသားချင်းစာနာမှုဆိုင်ရာအကြပ်အတည်းပြဿနာများဆက်တိုက်ဖြစ်ပွားလျက်ရှိရာ နိုင်ငံပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန၏ [ညွှန်ကြားတယ်လီဖုန်းကုမ္ပဏီများ \(directed telecom companies\)](#) သည် ယင်းတို့၏ မိုဘိုင်းအင်တာနက်ဝန်ဆောင်မှုများကို ရခိုင်ပြည်နယ်နှင့် အိမ်နီးချင်း ချင်းပြည်နယ်တို့တွင် ဖြတ်တောက်ထားခဲ့သည်။

‘ငြိမ်းချမ်းရေး၏အနှောင့်အယှက်များ’ နှင့် ‘တရားမဝင်လှုပ်ရှားမှုများ’ ဟူ၍ ကိုးကားပြီး [\(for the benefit of the people\) လူများ၏အကျိုးအတွက်](#) အင်တာနက်ဖြတ်တောက်ခြင်းကို ဥပဒေပြဋ္ဌာန်းသည်ဟု မြန်မာအစိုးရက ပြောဆိုခဲ့သည်။ အဖြစ်မှန်မှာ အင်တာနက်ဖြတ်တောက်ခြင်းကြောင့် [လူသန်းပေါင်းများစွာအား](#) မရှိမဖြစ်သော သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးကိုအသုံးပြုခွင့်၊ လူသားချင်းစာနာမှုဆိုင်ရာ ကြိုးပမ်းမှုများကို ရပ်တန့်စေခဲ့သည်။

“ထိုကဲ့သို့အင်တာနက်ဖြတ်တောက်ခြင်းသည် ဆက်လက်ဖြစ်ပွားနေသော ရိုဟင်ဂျာလူမျိုးတုံးသတ်ဖြတ်မှုနှင့် ရခိုင်ပြည်နယ်ရှိ စစ်ပြစ်မှုကျူးလွန်းခြင်းများအတွက် စစ်သွေးကြွများကို ပစ်မှတ်ထားစေကာမူ အချိုးအစားမညီမျှသော ဖြတ်တောက်ခြင်းသာ ဖြစ်သည်” ဟု Fortify Rights အဖွဲ့မှ Matthew Smith က [ဖော်ပြ](#)ခဲ့သည်။

အင်တာနက်ဖြတ်တောက်ခြင်းအား ၂၀၁၉ စက်တင်ဘာလတွင် [မြို့နယ် ၅ မြို့နယ်၌ တစ်စိတ်တစ်ပိုင်း ရုပ်သိမ်းပေးခဲ့သော်လည်း](#) ဆက်လက်ဖြစ်ပွားနေဆဲ ဖြစ်သည်။ ထိုတလတည်းမှာပင် ရိုဟင်ဂျာလူများစု ထွက်ပြေးခဲ့သော အိမ်နီးချင်းဘင်္ဂလားဒေ့ရှ်နိုင်ငံတွင်လည်း သက်ဆိုင်ရာအာဏာပိုင်များက

	<p>3G 4G services များကိုပိတ်ဆို့ထားဆီးရန် တယ်လီဖုန်းအော်ပရေတာများကို ညွှန်ကြားခဲ့ပြီး ရိုဟင်ဂျာဒုက္ခသည်စခန်းများတွင် တယ်လီဖုန်း SIM ကဒ်များ ရောင်းချခြင်းကိုရပ်ရန်ညွှန်ကြားခဲ့သည်။</p> <p>၂၀၂၀ နှစ်ဆန်းပိုင်းမှစ၍ ရခိုင်ပြည်နယ် ၊ မြို့နယ်အား ကမ္ဘာနှင့် အဆက်အသွယ်ပြတ်တောက်စေခဲ့ပြီး ဘင်္ဂလားဒေ့ရှ်နိုင်ငံရှိ ဒုက္ခသည်စခန်း များတွင်လည်း ဝန်ဆောင်မှုကို ဆက်လက်၍တန့်သတ် ထားခဲ့သည်။</p>
<p>Documenting During Internet Shutdowns</p>	<p>အင်တာနက်ဖြတ်တောက်ချိန်တွင် မှတ်တမ်းတင်ခြင်း</p>

Globally, internet shutdowns are on the rise. According to AccessNow's [#KeepItOn campaign](#), there were 128 intentional shutdowns between January – July 2019, compared to 196 in all of 2018, and up sharply from 106 in 2017, and 75 in 2016. Around the world, governments, with the cooperation of telecom companies, are increasingly turning to internet shutdowns as a strategy to repress communities, prevent mobilization, and stop information about human rights violations from being documented and shared.

အင်တာနက်ဖြတ်တောက်ခြင်းသည် ကမ္ဘာနှင့်အဝှမ်းမြင့်တက်လျက်ရှိသည်။ AccessNow's ၏ [#keepItOn campaign](#) အရ ၂၀၁၉ ဇန်နဝါရီမှဇူလိုင်လအတွင်း ၁၂၈ ကြိမ်၊ ၂၀၁၈ တွင် ၁၉၆ ကြိမ် တို့မှာ ၂၀၁၇ တွင် ၁၀၆ ကြိမ်၊ ၂၀၁၆ တွင် ၇၅ ကြိမ်များနှင့် နှိုင်းစာလျှင် သိသာစွာမြင့်တိုး ဖြစ်ပေါ်ခဲ့သည်။ ကမ္ဘာတဝှမ်းတွင် အစိုးရများသည် ဆက်သွယ်ရေးကုမ္ပဏီများနှင့်ပူးပေါင်းပြီး အင်တာနက်ဖြတ်တောက်ခြင်းကို နည်းဗျူဟာတရပ်အနေဖြင့် တိုးမြှင့်ပြုလုပ်ခဲ့ပြီး လူထုအားဖိနှိပ်ခြင်း၊ စည်းရုံးလှုံ့ဆော်ရေးများကို တားဆီးခြင်းနှင့် လူ့အခွင့်အရေးချိုးဖောက်မှု အချက်အလက်များကို မှတ်တမ်းတင်ခြင်းနှင့် မျှဝေခြင်းများကို ရပ်တန့်စေခဲ့သည်။

[“Internet shutdowns and human rights violations go hand in hand.”](#)
– Berhan Taye, AccessNow

[“အင်တာနက်ဖြတ်တောက်ခြင်းနှင့် လူ့အခွင့်အရေးချိုးဖောက်မှုများသည် ချိတ်ဆက်မှုရှိရှိဖြစ်ပေါ်နေသည်”](#) – Berhan Taye, AccessNow

Shutdowns can take various forms, including [platform-specific blockages that target popular apps and sites](#), [mobile data shutdowns](#), [bandwidth throttling](#), or [total internet blackouts](#). All of these types of shutdowns are intended to disrupt the ability to communicate information and expose violations in real-time. They often occur during protests, elections, and periods of

အင်တာနက်ဖြတ်တောက်ခြင်းနည်းပုံစံအမျိုးမျိုးတို့မှာ လူကြိုက်များသော [ပလက်ဖောင်းအထူးပြုပိတ်ဆို့တားဆီးခြင်းဖြစ်သော](#) [ရေပန်းစားသော app](#) [နှင့် ဝက်ဘ်ဆိုက်များကို ပိတ်ပင်တားဆီးခြင်း၊ မိုဘိုင်းဒေတာကို](#) [ဖြတ်တောက်ခြင်း၊ အင်တာနက်မြန်နှုန်းကိုထိန်းချုပ်ခြင်းနှင့် အင်တာနက်ကို](#)

<p>political instability, and are often accompanied by heightened state repression, military offensives, and violence. While governments may try to justify shutdowns in the name of “public safety” or other reasons, shutdowns clearly take place at moments when repressive states fear losing tenuous control over their people, information, or political narrative. Shutdowns violate human rights, severely disrupt people’s lives and livelihoods, and also have a global economic impact.</p>	<p>လုံးဝဖြတ်တောက်ခြင်းတို့ ပါဝင်သည်။ အထက်ပါပိတ်ပင်ခြင်းအားလုံးသည် အချိန်နှင့်တပြေးညီ သတင်းအချက်အလက်များ ဆက်သွယ်ပို့ဆောင်ခြင်း၊ ချိုးဖောက်မှုများကို ဖော်ထုတ်ခြင်းကို အနှောင့်အတားဖြစ်စေသည်။ ထိုအခြေအနေများသည် လူထုဆန္ဒပြခြင်း၊ မဲဆန္ဒပေးခြင်းနှင့် နိုင်ငံရေး မတည်ငြိမ်သည့်အချိန်များတွင် မကြာခဏဖြစ်ပေါ်လေ့ရှိပြီး ပြည်နယ်တွင်း ဖိနှိပ်ခြင်း၊ စစ်တပ်၏ထိုးစစ်နှင့်အကြမ်းဖက်မှုများ မြင့်မားချိန်နှင့် မကြာခဏ အတူတကွ ဖြစ်ပေါ်သည်။ အာဏာပိုင်အစိုးရအနေဖြင့် အင်တာနက်ဖြတ်တောက်ခြင်းကို လူထုလုံခြုံရေးသို့မဟုတ် အခြားအကြောင်းပြချက်များ ရှင်းလင်းဖော်ပြသော်လည်း ထိုဖြတ်တောက်ခြင်းမှာ ဖိနှိပ်ခံရသောပြည်နယ်များတွင် ယင်းလူထုအား သတင်းအချက်အလက်နှင့် နိုင်ငံရေးဇာတ်ကြောင်းများ ထိန်းချုပ်နိုင်မှု ပျောက်ကွယ်မည်ကိုစိုးရိမ်ကြောင့်ကြသည်မှာ ထင်ရှားလှပေသည်။ အင်တာနက်ဖြတ်တောက်ခြင်းသည် လူ့အခွင့်အရေးချိုးဖောက်ခြင်းဖြစ်ပြီး၊ လူအများ၏ ဘဝနှင့်ရှင်သန်ရေးကိုဟန့်တားခြင်းနှင့် ကမ္ဘာလုံးဆိုင်ရာ စီးပွားရေးသက်ရောက်မှုများကိုဖြစ်စေနိုင်သည်။</p>
<p>[IMAGE] Types of internet shutdowns.</p>	<p>အင်တာနက်ဖြတ်တောက်ခြင်းအမျိုးအစားများ</p>
<p>[IMAGE] Embed from Getty Images</p>	<p>ဓာတ်ပုံများ</p>
<p>Documenting human rights violations is as important as ever during an internet shutdown. Even if information cannot</p>	<p>လူ့အခွင့်အရေးချိုးဖောက်မှုကို မှတ်တမ်းတင်ခြင်းသည် အင်တာနက်</p>

<p>be shared in the moment, documentation can be a way to preserve voices that authorities are trying to silence, and to secure evidence of abuses that can be used to demand accountability later on. Of course, the repressive context and the technological impediments of an internet shutdown make documenting violations — and maintaining that documentation securely — much more challenging and risky. How can activists capture and preserve their videos during a shutdown, and even share them offline, and do so in safer ways?</p>	<p>ဖြတ်တောက်ထားသည့် အချိန်တွင် ယခင်အခါများထက်ပိုပြီးအရေးပါသည်။</p> <p>သတင်းအချက်အလက်ကို ချက်ချင်း ဝေမျှခွင့်မရသော်လည်း မှတ်တမ်းတင် ထားခြင်းသည် သက်ဆိုင်ရာအားဏာပိုင်များ ရေငုံနှုတ်ပိတ်ရန် ကြိုးစားမှုအား အသံဖြစ်စေခြင်း နှိပ်စက်ခြင်းများအား သက်သေအဖြစ် လုံခြုံစွာထားရှိပြီး နောင်တချိန်တွင် တာဝန်ယူမှုရှိရန် ပြန်လည်အသုံးပြု နိုင်သည်။ ထိုသို့ဖိနှိပ်နေသောအခြေအနေတွင် အင်တာနက်ဖြတ်တောက် ခြင်းကဲ့သို့ စက်ပိုင်းဆိုင်ရာအနှောင့်အတားကြား မှတ်တမ်းတင်ခြင်းနှင့် အချက်အလက်များကို လုံခြုံစွာထိန်းသိမ်းရန်သည် ကျိန်းသေပေါက် အန္တရာယ်ရှိပြီး စွန့်စားရသော စိန်ခေါ်မှုတရပ်ဖြစ်သည်။</p> <p>တက်ကြွ လှုပ်ရှားသူများသည် အချက်အလက်များကို မှတ်တမ်းတင်ခြင်းနှင့် ဗီဒီယိုများ ထိန်းသိမ်းခြင်းအပြင် အော့ဖ်လင်း(offline)အချိန်တွင် မျှဝေခြင်း ကို မည်ကဲ့သို့ ပိုပြီးလုံခြုံစွာ ပြုလုပ်နိုင်သလဲ?</p>
<p>This series</p>	<p>စီးရီးများ</p>

Through our work with activists who have experienced internet shutdowns, we have learned some useful tips and approaches to **capturing and preserving video documentation during internet shutdowns** that we are sharing in this series. We wrote them with Android devices in mind, but the tips can be applied to iPhones as well. Some of the strategies require advance planning (and often, internet access), so it's a good idea to review them and implement any steps *before* you are in a situation where you do not have internet and you need to document. Save a copy of any of the tutorials so you can refer to them or share them during a shutdown. And finally, start practicing the techniques and methods in your everyday work so that they become second-nature before you're in a crisis situation.

- Prepare

အင်တာနက်ဖြတ်တောက်ထားချိန်တွင် အတွေ့အကြုံရှိခဲ့သော တက်ကြွလှုပ်ရှားသူများနှင့် ကျွန်ုပ်တို့အတူတူလုပ်ခဲ့သောအလုပ်များမှ လေ့လာခဲ့ရသော “အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဗီဒီယိုဖမ်းယူပြီး မှတ်တမ်းများကိုထိန်းသိမ်းခြင်း” အသုံးဝင်သည့် အကြံပေးချက်များနှင့် ချဉ်းကပ်နည်းများကို ဒီစီစီရီးတွင် မျှဝေသွားမှာဖြစ်ပါသည်။ အင်ဒရိုက်(Android)စက်များအတွက် ရည်စူး၍ ရေးသားသော်လည်း အိုင်ဖုန်း(iPhone)တွင်လည်း အသုံးပြုနိုင်ပါသည်။ အချို့နည်းဗျူဟာများသည် ကြိုတင်အစီအစဉ်ချခြင်းနှင့် (အင်တာနက်အသုံးပြုခြင်းများ)လိုအပ်သည်။ ထို့ကြောင့် ပြန်လည်သုံးသပ်ခြင်း၊ လက်တွေ့အခြေအနေဖြစ်သော အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းဖို့လိုအပ်ချိန်မတိုင်မီ တဆင့်ချင်း အကောင်အထည်ဖော်ထားသင့်သည်။ သင်ခန်းစာများကို ကော်ပီသိမ်းဆည်းထားခြင်းဖြင့် အင်တာနက်ဖြတ်တောက်ချိန်တွင် ပြန်လည်ရည်ညွှန်းခြင်း၊ မျှဝေခြင်းများပြုလုပ်နိုင်ပါသည်။ နောက်ဆုံးအနေဖြင့် ထိုနည်းပညာများနှင့် နည်းလမ်းများကို နေ့စဉ်နေ့တိုင်းလုပ်ငန်းတခုအနေနဲ့ လေ့ကျင့်ခြင်းဖြင့် အကြပ်အတည်းကြုံလာမည့်အချိန်မတိုင်မီတွင် သဘာဝ အလျောက်အလေ့အကျင့်ဖြစ်နေပေလိမ့်မည်။

- ပြင်ဆင်ခြင်း

<ul style="list-style-type: none"> ○ Setting up a phone for offline documentation ● Capture <ul style="list-style-type: none"> ○ Should I use this documentation app? ● Maintain <ul style="list-style-type: none"> ○ Maintaining verifiable media during an internet shutdown ○ Backing up phone media without internet or a computer ● Share and Communicate <p>File sharing and communication during an internet shutdown</p>	<p>ဖုန်းကို အော့ဖ်လင်း(offline)နဲ့ မှတ်တမ်းတင်ဖို့ ပြင်ဆင်ထားခြင်း</p> <ul style="list-style-type: none"> - အမိဖမ်းယူခြင်း <p>ဒီမှတ်တမ်းတင်တဲ့ App ကိုသုံးလို့ရမလား?</p> <ul style="list-style-type: none"> - ထိန်းသိမ်းခြင်း <p>အင်တာနက်ဖြတ်တောက်ချိန်တွင် ခိုင်လုံအတည်ပြုထားသော မီဒီယာကိုထိန်းသိမ်းခြင်း</p> <p>ဖုန်းမီဒီယာကို အင်တာနက် သို့မဟုတ် ကွန်ပျူတာမရှိဘဲ အရန်သိမ်းဆည်း back up ထားခြင်း</p> <ul style="list-style-type: none"> - မျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်း <p>အင်တာနက်ဖြတ်တောက်ချိန်တွင် မျှဝေခြင်းနှင့်ဆက်သွယ်ခြင်း</p>
<ul style="list-style-type: none"> ○ [IMAGE] From the #KeepItOn visual kit. 	<p>#KeepItOn ရုပ်မြင်သင်ထောက်ကူပစ္စည်းကိရိယာများ</p>
<p>One final note: While these tips can help you continue documenting in the face of a shutdown, we want to emphasize that the ultimate solution must be to restore internet access, and successfully defend people’s right to record, and freedom of expression, information, and assembly. Fortunately, there is a global movement led by organizations like NetBlocks, AccessNow, and many others who are actively monitoring and sharing information about shutdowns. Advocates globally are engaging in strategic litigation against shutdowns. We stand in solidarity with their work to uphold human rights.</p>	<p>နောက်ဆုံးမှတ်ချက်။ ။အင်တာနက်ဖြတ်တောက်ချိန်များတွင် ထိုအကြံပေးချက်များ မှတ်တမ်းတင်နိုင်ရန် အကူအညီဖြစ်စေသော်လည်း အထူးပြုပြောလိုသည်မှာ နောက်ဆုံးပိတ်ဖြေရှင်းမှုသည် အင်တာနက် အသုံးပြုခွင့်ကို ပြန်လည်ရရှိရန်၊ လူများ၏အခွင့်အရေးဖြစ်သော မှတ်တမ်းတင်ခြင်းကို အောင်မြင်စွာကာကွယ်ရန်၊ လွတ်လပ်စွာပြောဆိုခွင့် သတင်းအချက်အလက်ရရှိခွင့်နှင့်လူစုရုံးခွင့်တို့ဖြစ်သည်။</p> <p>ကံကောင်းသည်မှာ NetBlocks, AccessNow ကဲ့သို့အဖွဲ့အစည်းတော်တော်များများက</p>

	<p>ကမ္ဘာလုံးဆိုင်ရာလှုပ်ရှားမှုအနေဖြင့် တက်ကြွစွာ စောင့်ကြည့်လေ့လာနေပြီး အင်တာနက်ဖြတ်တောက်ခြင်းသတင်းအချက်အလက်များကိုမျှဝေနေသည်။</p> <p>။ကမ္ဘာလုံးဆိုင်ရာထောက်ခံပြောဆိုသူများအနေဖြင့်လည်း အင်တာနက် ဖြတ်တောက်ခြင်းနှင့် ဆန့်ကျင်သောတရားရေးများကို နည်းဗျူဟာများဆွဲ၍ စေ့စပ်ဆွေးနွေးလျက်ရှိသည်။</p> <p>လူ့အခွင့်အရေးခိုင်မာမှုအတွက် ကျွန်ုပ်တို့ကလည်း သူတို့နှင့်တသားတည်း စည်းလုံးစွာရပ်တည်နေသည်။</p>

<p>Setting Up a Phone for Offline Documentation</p>	<p>အော့ဖ်လိုင်(offline) မှတ်တမ်းတင်ခြင်းအတွက် ဖုန်းကိုပြင်ဆင်(setup)ခြင်း</p>
---	---

Documenting During Internet Shutdowns series

By [Yvonne Ng](#)

With contributions by [Arul Prakkash](#)

This post is part of a series on <Documenting During Internet Shutdowns>.

Last reviewed: 31 January 2020

အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

ရေးသားသူ - [Yvonne Ng](#)

ပံ့ပိုးသူ - [Arul Prakkash](#)

ဒီပို့စ်သည် “အင်တာနက်ဖြတ်တောက်ချိန်တွင် မှတ်တမ်းတင်ခြင်း”

စီးရီး၏အပိုင်းဖြစ်သည်

နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်

Despite an internet shutdown, documenters can still capture important video evidence that can be shared offline or when they are able to get back online.

Here are some tips that we've learned from activists and other practitioners to set up a phone for offline documentation. Note that some steps **require internet access**, so must be done before a shutdown occurs or during periods when it is restored. Also, don't wait until you're in a stressful situation to enact these steps; do them now, and take time to **practice using the phone** before you have to use it in a crisis.

အင်တာနက်ဖြတ်တောက်ထားသော်လည်း မှတ်တမ်းတင်သူများအနေနှင့် အရေးကြီးဗီဒီယိုများဖမ်းယူနိုင်ပြီး ထိုဗီဒီယိုအထောက်အထားများကို အော့ဖ်လိုင်း(offline) သို့မဟုတ် အွန်လိုင်း(online) ပြန်ရသည့်အချိန်တွင် မျှဝေခြင်း ပြုလုပ်နိုင်သည်။

အော့ဖ်လိုင်း(offline)မှတ်တမ်းတင်ခြင်းအတွက်ဖုန်းကိုပြင်ဆင်(setup)ခြင်း

အတွက်အသုံးဝင်မည့်အချက်အလက်များကို တက်ကြွလှုပ်ရှားသူများနှင့် အခြားကျင့်သုံးသူများဆီမှ ကျွန်ုပ်တို့ အောက်ပါအတိုင်းလေ့လာခဲ့သည်။

သတိပြုရန်မှာ အချို့သောအချက်များသည် **အင်တာနက်အသုံးပြုရန်** လိုအပ်သည်။ ထို့ကြောင့် အင်တာနက်ဖြတ်တောက်ချိန်မတိုင်မီ သို့မဟုတ် အင်တာနက်ပြန်လည်ရရှိချိန်တွင် လုပ်ဆောင်ထားရန်ဖြစ်သည်။

ထပ်မံပြောကြားလိုသည်မှာ ထိုအချက်များကို စိတ်ဖိစီးမှုရှိနေသည့်

	<p>အချိန်ကျမှ လုပ်ဆောင်ရန်မစောင့်ဆိုင်းပါနှင့်။ ယခုလုပ်ဆောင်ထားပါ။ အကြပ်အတည်း ကျရောက်သည့်အချိန် မတိုင်မီ ဖုန်းအသုံးပြုခြင်းကို အချိန်ယူ၍လေ့ကျင့်ထားပါ။</p>
<p>Shutdowns often coincide with heightened information control and restrictions on freedom of expression and assembly. If you are a documenter, take extra precautions to protect yourself and your information during these periods. If there is a risk that authorities will confiscate your phone, or compel you to unlock it and reveal the contents (during a shutdown or otherwise), consider using a separate phone for documenting than your primary personal one. This can help minimize what information you are carrying that can be compromised (e.g. your contacts, accounts, messages, etc). If you are unable to use another device, you can still follow this guide to reduce the amount of sensitive data and improve security on your primary phone.</p>	<p>အင်တာနက်ဖြတ်တောက်ချိန်သည် သတင်းအချက်အလက်များကို တိုးမြှင့်ထိန်းချုပ်ထားသည့်အချိန် သို့မဟုတ် လွတ်လပ်စွာသဘောထား ထုတ်ဖော်ခွင့်၊ စုရုံးခွင့်များကို ကန့်သတ်ထားသည့် အချိန်များနှင့် တိုက်ဆိုင်နေတတ်သည်။ သင်သည်မှတ်တမ်းတင်သူဖြစ်လျှင် မိမိကိုယ်ကို သော်လည်းကောင်း၊ မိမိ၏သတင်း အချက်အလက်များကိုသော် လည်းကောင်း အထူးသတိပြုကာကွယ်ရန်အချိန်ဖြစ်သည်။ သက်ဆိုင်ရာအာဏာပိုင်များက သင့်ဖုန်းကိုသိမ်းယူနိုင်ခြေအလားအလာ၊ ဖုန်းကို မဖြစ်မနေ unlock လုပ်ခိုင်းနိုင်ခြေ၊ အကြောင်းအရာများကိုထုတ်ပြ ခိုင်းသောအခြေအနေများရှိလျှင် (အင်တာနက်ဖြတ်တောက်ချိန်၊ အခြား) မှတ်တမ်းတင်ရန်အတွက် သီးသန့်ဖုန်းတလုံးသုံးရန်စဉ်းစားပါ။ ထိုသို့သုံးစွဲခြင်းဖြင့် မိမိကိုယ်ပိုင်အချက်အလက်များ (contacts, accounts, message, etc) ခိုးယူရရှိခြင်း အခွင့်အလမ်းကို နည်းစေလိမ့်မည်။ ထိုသို့သီးသန့်စက်မသုံးနိုင်လျှင်လည်း ယခုနည်းလမ်းများကို ဆက်လက်သုံးစွဲခြင်းဖြင့်လည်း အထိခိုက်မခံနိုင်သောဒေတာများကို ပိုမိုကောင်းမွန်စွာ လုံခြုံစေလိမ့်မည်။</p>
<p>If repurposing an older phone, wipe it first</p>	<p>ဖုန်းအဟောင်းကိုရည်ရွယ်ချက်ပြောင်းသုံးစွဲလျှင် ဒေတာအရင်ရှင်းပစ်ပါ</p>

<p>To wipe your phone, run a Factory Reset.</p>	<p>ဒေတာရှင်းရန် factory reset ကို run ပါ</p>
<p>Note: Studies have shown that running a Factory Reset on your phone does not necessarily wipe all the data. In fact, the only 100% secure way to wipe data is to destroy the phone, but that method isn't an option if you want to re-use the phone! In this article, an Android engineer suggests making sure the contents of your device are encrypted before the Factory Reset. Encryption is the default on most current phones anyway, but in case not, go to Settings > Security > Encrypt Phone before resetting. This way, when you factory reset the phone, the encryption key is lost, and any unerased data will be unreadable.</p>	<p>မှတ်ချက်။ ။ လေ့လာချက်များအရ ဖုန်းကို factory reset run သော်လည်း ရှိသမျှဒေတာအားလုံးရှင်းမည်မဟုတ်ပါ။ အမှန်မှာ ရာနှုန်းပြည့်လုံခြုံစွာ ဒေတာများကိုရှင်းလင်းချင်လျှင် ဖုန်းကို ဖျက်ဆီးရမည်။ သို့သော် ထိုနည်းလမ်းသည် ဖုန်းကိုပြန်လည်သုံးစွဲချင်လျှင် ရွေးချယ်လိုရမည့် နည်းလမ်း မဟုတ်ပါ။ ယခုဆောင်းပါးတွင် Android အင်ဂျင်နီယာတစ်ဦးက အကြံပေးထားသည်မှာ factory reset မလုပ်မီ ဖုန်းထဲရှိအကြောင်းအရာ များကို လျှို့ဝှက်လုံခြုံရန် သေချာစေရမည်။ ယခုလက်ရှိဖုန်း အများစုတွင် မူရင်းအားဖြင့် လျှို့ဝှက်လုံခြုံမှုရှိသော်လည်း အကယ်၍မရှိခဲ့လျှင် resetting မလုပ်မီ setting ကိုသွားပါ > security > encrypt လုပ်ပါ။ ထိုနည်းလမ်းသည် သင် factory reset လုပ်ချိန်မှာ encryption key ပျောက်သွားပါက မဖျက်ဆီးရသေးသော ဒေတာများသည်ပင် ဖတ်လို့မရသောအဆင့်သို့ ရောက်သွားမည်။</p>
<p>Practice basic phone security</p>	<p>ဖုန်းလုံခြုံရေးအခြေခံကိုလေ့ကျင့်ခြင်း</p>
<p>There are general phone security practices that are relevant in every situation, whether you are documenting during an internet shutdown or not. Here are some useful resources from other organizations. While nothing will guarantee 100% security, some key tips include:</p>	<p>အထွေထွေဖုန်းလုံခြုံရေးအလေ့အကျင့်များမှာ အခြေအနေအရပ်ရပ်တွင် အင်တာနက်ဖြတ်တောက်ချိန်ဖြစ်စေ၊ မဖြတ်တောက်ချိန်ဖြစ်စေ အကျိုးဝင်သည်။ အခြားအဖွဲ့အစည်းများ၏ အသုံးဝင်သောအရင်းအမြစ်များ</p>

- Make sure your phone is encrypted. Newer phones have encryption on by default. If you're not sure about yours, check the security settings on your phone.
- Run operating system (OS) updates regularly, as they often fix security vulnerabilities.
- Update your important apps (like messaging apps) regularly.
- Set a strong phone passcode that has at least 6 digits and does not rely on fingerprint/touch or face ID.
- Set up a screen lock and lock timer.
- Turn off location services if you don't need them (including emergency location service, location accuracy, location history, and location sharing features, and WiFi and Bluetooth scanning options). Also check location permissions for individual apps.
- Turn off Bluetooth and WiFi when you don't need them, to avoid device tracking.

Power down the phone when you're not using it.

အောက်ပါအတိုင်းဖြစ်သည်။ မည်သည့်အရာမှ ရာနှုန်းပြည့် အာမ မခံနိုင်သော်လည်း အချို့အသုံးဝင်သည့်အချက်များပါဝင်သည်မှာ

- သင့်ဖုန်းသည် လျှို့ဝှက်လုံခြုံကြောင်း(encrypted) သေချာပါစေ။ ဖုန်းအသစ်များသည် မူလပင်မကပင် လျှို့ဝှက်လုံခြုံသည် (encrypted)။ မိမိဖုန်း၏လျှို့ဝှက်လုံခြုံမှု မသေချာလျှင် security setting ကို စစ်ဆေးပါ။
- OS (operating system) updates ကို ပုံမှန်စစ်ဆေးပါ။ သူတို့သည် လုံခြုံရေးထိခိုက်နိုင်မှုကို ပြုပြင်နိုင်သည်။
- အရေးကြီးသော app (like message apps) များကို ပုံမှန် update လုပ်ပါ။
- ဖုန်းလျှို့ဝှက်ကုန်ပိတ်ကိုခိုင်မာပါစေ။ အနည်းဆုံး ဂဏန်းခြောက်လုံးထားပါ။ လက်ဗွေ မျက်နှာ အမှတ်အသား fingerprint/touch or face ကို အားမကိုးပါနှင့်။
- Screen lock, lock timer ကို set up လုပ်ထားပါ။
- တည်ရှိနေရာ location service ကို (off) မလိုလျှင်ပိတ်ထားပါ။ (emergency location service, location accuracy, location history, location sharing, Wifi, Bluetooth scanning) အကုန်ပါသည်။ အခြား app တွေမှာရှိသည့် check location permission များလည်းပိတ်ထားပါ။
- Bluetooth နဲ့ Wifi ကိုလည်း မလိုအပ်လျှင်ပိတ်ထားခြင်းဖြင့် device ကို နောက်ယောင်ခံခြင်းမှ ရှောင်ရှားနိုင်သည်။

ဖုန်းကို မသုံးလျှင် power down ထားပါ။

<h2>Install useful documentation apps</h2>	<p>အသုံးဝင်သောမှတ်တမ်းတင်Appများကို Install လုပ်ခြင်း</p>
<p>For photo or video documentation, you can use the built-in camera app on your phone, or you can use a more specialized documentation app, like ProofMode or others, that allow for more robust metadata capture and export, identification and authentication, encryption, secure galleries, or other features.</p>	<p>ဓာတ်ပုံသို့မဟုတ်ဗီဒီယိုမှတ်တမ်းတင်သောအခါ ဖုန်းထဲရှိ built-in camera app ကို အသုံးပြုနိုင်သည်။ သို့မဟုတ် ပိုပြီးအထူးပြုသောမှတ်တမ်းတင်app (ProofMode သို့မဟုတ် အခြား)များကိုလည်း အသုံးပြုနိုင်သည်။ ထို app များသည် ပိုမိုအားကောင်းသည့် metadata များကို ဖမ်းယူ၊ ပြင်ပသို့ထုတ်ပို့၊ သရုပ်ခွဲ၊ အတည်ပြု၊ လျှို့ဝှက်ထိန်းသိမ်း၊ လုံခြုံသော galleries နှင့် တခြား အင်္ဂါရပ်များကို ခွင့်ပြုစေသည်။</p>
<p>A useful app for documenting a shutdown <i>itself</i> is OONI Probe, an open-source app that runs tests from your phone to measure whether sites or platforms are being blocked. It can show you how, when, where, and by whom sites are being blocked. Be sure to understand the potential risks before using this app.</p> <ul style="list-style-type: none"> • Not sure which documentation app(s) to use? We provide some guiding questions in our tutorial, "Should I Use this Documentation App?". 	<p>အင်တာနက်ဖြတ်တောက်ချိန်ကို မှတ်တမ်းတင်သည့် app ဖြစ်သော OONI Probe သည် ပွင့်လင်းအရင်းအမြစ် app ဖြစ်ပြီး ဖုန်းမှတစ်ဆင့်စမ်းသပ်ကာ ဆိုက်သို့မဟုတ် ပလက်ဖောင်းများကို ပိတ်ဆို့သလားဟု စမ်းသပ်နိုင်သည်။ ထိုစမ်းသပ်မှုမှ ဘယ်လို၊ ဘယ်အချိန်၊ ဘယ်နေရာ၊ ဘယ်သူက ဆိုက်တွေကို ပိတ်ဆို့ထားသလဲ ပြသနိုင်သည်။ ဒီ app ကို အသုံးမပြုမီ ဖြစ်နိုင်ခြေရှိသော အန္တရာယ်များကို နားလည်ထားဖို့လိုအပ်သည်။</p> <ul style="list-style-type: none"> - မည်သည့် app ကို အသုံးပြုရမလဲ မသေချာဖြစ်နေပါသလား? ကျွန်ုပ်တို့က လမ်းညွှန်မေးခွန်းများဖြင့် "ဒီမှတ်တမ်းတင်app ကို သင်သုံးသင့်ပါသလား" သင်တန်းတွင်ပံ့ပိုးပေးပါမည်။

<p>Install some everyday apps</p>	<p>နေ့စဉ်အသုံးပြုမည့် App များ Install လုပ်ခြင်း</p>
<p>Having very little data and only a few specialized apps on your phone may arouse suspicion. To make the device appear as if it's an everyday phone, install some everyday apps that are common in the area where you are documenting (but that are downloaded from reputable sources), and take some innocuous photos for your gallery.</p>	<p>သင့်ဖုန်းထဲတွင် ဒေတာအနည်းငယ်သာရှိပြီး အထူးပြုသော app များရှိနေခြင်းကြောင့် သံသယဖြစ်ခံရဖွယ်ဖြစ်နိုင်သည်။ သင့်ဖုန်းကို နေ့စဉ် သုံးနေသော deviceပုံစံပေါ်လွင်စေရန် မိမိမှတ်တမ်းတင်သော နေရာဒေသတွင် အသုံးများသော app များ install လုပ်ထားပါ (သို့သော် နာမည်ကောင်းရှိသောအရင်းအမြစ်များမှ download) လုပ်ပြီး ဘေးကင်းသောဓာတ်ပုံများကို gallery တွင်ထားပါ။</p>
<p>For social media apps, you may wish to create and log into alternate accounts, although keep in mind that fake accounts violate the Terms of Service for most platforms, and identity verification requirements of some platforms may make it difficult to create fake accounts. In addition, you will need to spend some time creating content and adding friends to these, which can be laborious.</p>	<p>ဆိုရှယ်မီဒီယာ app သုံးလျှင် အခြားနာမည်များနှင့် အကောင့်ဖွင့်လိုက ဖွင့်ထားနိုင်သော်လည်း အကောင့်တူသည် အချို့ပလက်ဖောင်းများ၏ ဝန်ဆောင်မှုစည်းကမ်းကို ဖောက်ဖျက်ရာရောက်သည်။ အချို့ပလက်ဖောင်း များသည် အကောင့်တူဖွင့်ရန်ခက်ခဲအောင် ကိုယ်ရေးကိုယ်တာအချက်များ စိစစ်အတည်ပြုခြင်းလိုအပ်ချက်များထားရှိသည်။ ထို့အပြင် အကြောင်းအရာများ ဖြည့်သွင်းခြင်း သူငယ်ချင်းလက်ခံခြင်း စသည့် လုပ်ငန်းများအတွက် ကြိုးစားအားထုတ်အချိန်သုံးရမည် ဖြစ်သည်။</p>
<p>Installing apps when there is no internet</p>	<p>အင်တာနက်မရှိချိန်တွင် app များ install လုပ်ခြင်း</p>
<p>Downloading and installing apps without internet access is obviously a challenge. You need to download apps in advance if</p>	<p>အင်တာနက်ချိတ်ဆက်ခွင့်မရဘဲ app များကို download and install လုပ်ခြင်းသည် သိသာထင်ရှားသော စိန်ခေါ်မှုဖြစ်သည်။</p>

<p>you anticipate an internet outage.</p> <p>One strategy that can help you and others later on is to download and save the Android Package (.apk) file for the app (downloaded from a trusted source, e.g. directly from the developer) on your phone storage or on a drive. Having these APKs offline allows you or others to share apps when there is no internet.</p> <p>While we haven't had a chance to give this a try, the F-Droid app provides an interface to swap these APKs offline. Here is their tutorial.</p>	<p>အင်တာနက်ပြတ်တောက်နိုင်ချေရှိသည်ကို မျှော်မှန်း၍ ကြိုတင်ပြီး download လုပ်ထားရမည်။</p> <p>သင့်အားအထောက်အကူပြုနိုင်သည့် အခြားသောနည်းဗျူဟာမှာ Android Package (.apk) file ကို download and save လုပ်ထားပါ</p> <p>(ယုံကြည်ရသော အရင်းအမြစ်, ဥပမာ တီထွင်သူထံမှ တိုက်ရိုက်download) Phone storage or drive မှာ .apk file အနေနဲ့ သိမ်းထားပါ။ ထို APKများကို အော့ဖ်လိုင်း ထားခြင်းသည် အင်တာနက် မရှိသည့်အချိန်တွင် သင်ရော တခြားသူများပါ မျှဝေခြင်းကို ခွင့်ပြုသည်။</p> <p>စမ်းသပ်သုံးစွဲဖို့အခွင့်အလမ်းမရှိသော်လည်း F-Droid app သည် ထို APK အော့ဖ်လိုင်းများနှင့် လဲလှယ်သုံးစွဲနိုင်သည်။ သင်ခန်းစာ</p>
<p>[IMAGE] F-Droid app's offline sharing interface.</p>	<p>F-Droid app ကို အော့ဖ်လိုင်းမျှဝေသော ဆက်သွယ်ရေးစနစ်</p>
<p>Keep real personal or private / sensitive information off the device</p>	<p>ကိုယ်ရေးကိုယ်တာ၊ လျှို့ဝှက်၊ အထိခိုက်မခံသော သတင်းအချက်အလက်များကို ဖုန်း(device) ထဲမှ ဖယ်ထုတ်ထားခြင်း</p>
<p>Try to reserve the device for doing documentation. Don't use it for email, phone calls, or messages with personal or activist contacts who could be put at risk, and do not connect this</p>	<p>ဖုန်း(device)ကို မှတ်တမ်းတင်ရုံသက်သက်သာအသုံးပြုရန် ဖယ်သိမ်းထားဖို့ ကြိုးစားပါ။ email, phone calls, message အတွက်</p>

<p>device to any of your real, primary accounts.</p>	<p>ကိုယ်ရေးကိုယ်တာဖြစ်စေ၊ အန္တရာယ်ရှိသွားနိုင်သောတက်ကြွလှုပ်ရှားမှု အဆက်အသွယ်များနှင့်ဖြစ်စေ ဒီဖုန်း(device)ဆက်သွယ်မှု လုပ်ရန် မသုံးပါနှင့်</p>
<p>Use features for obscuring content</p>	<p>အကြောင်းအရာများကို မှေးမှိန်သွားစေမည့် features သုံးခြင်း</p>
<p>In the event that your phone is searched, it may be helpful to make your intentions less obvious or your content harder to find. In anticipation of situations where your phone will <i>only be superficially and quickly examined</i>, you can employ simple tactics such as:</p>	<p>အကယ်၍ သင့်ဖုန်းကို ရှာဖွေခံရသည့်အခါ သင့်ရည်ရွယ်ချက်ကို သိသာမှု နည်းစေရန် သို့မဟုတ် အကြောင်းအရာများကို တွေ့ရှိဖို့ ခက်ခဲစေရန် ကူညီပေးသည်။ သင့်ဖုန်းကို အပေါ်ယံလျင်မြန်စွာ စစ်ဆေးခြင်းခံရတဲ့အခါ ယခုကဲ့သို့ရှင်းလင်းသည့် နည်းဗျူဟာများကို လုပ်ဆောင်သင့်သည်။</p>
<p>Changing the names and icons of your app shortcuts using a Launcher app (e.g. Nova Launcher, but there are many) so it's less obvious what certain apps are.</p>	<p>Launcher app ကို အသုံးပြု၍ app ၏ shortcut နာမည်နဲ့ အိုင်ကွန် များကို ပြောင်းလဲလိုက်ပါ။ (ဥပမာ - Nova Launcher , အခြား app များလည်းရှိသေးသည်) အချို့ app တွေရဲ့ သိသာထင်ရှားမှုကို နည်းစေမည်။</p>
<p>Using a built-in privacy feature like Private Mode (Samsung) or Content Lock (LG), if your phone supports it.</p>	<p>Private Mode (Samsung) or Content Lock (LG) ကဲ့သို့ ဖုန်းနဲ့ တပါတည်းပါလာသော လျှို့ဝှက် feature များကို အထောက်အကူ သုံးနိုင်သည်။</p>

Placing an empty file named “.nomedia” inside any folder to prevent media in a folder from appearing in your gallery. Note: If media still appears, you may need to clear your Gallery cache. This may not work consistently on all devices.

အချက်အလက်မပါဝင်သော ဖိုင်တခုဆောက်၍ “.nomedia” ဟုအမည်ပေး Folder တခုအောက်တွင်သိမ်းခြင်းဖြင့် gallery ထဲမှာ သင့်မီဒီယာတွေ မပေါ်လာအောင် ကာကွယ်နိုင်သည်။ မှတ်ချက် - အကယ်၍ မီဒီယာတွေ ပေါ်နေဆဲဖြစ်လျှင် gallery cache ကို clear လုပ်ပါ။ ဖုန်း(devices) အားလုံးတွင် တသမတ်တည်း အလုပ်ဖြစ်ချင်မှ ဖြစ်လိမ့်မည်။

Creating hidden folders (folders that start with a “.”) using a file manager app. You can either move files to the hidden folder manually, or if you use a camera app like [Open Camera](#), you can specify where the media you record gets stored. Make sure to turn off “show hidden files” option in your Settings so that hidden files are not visible.

ဖွက်ထားသော folderများ (“.” နှင့်စသောfolder)ကို file manager app သုံး၍ ဖန်တီးပါ။ ဖွက်ထားသော folderများကို manually ဖြစ်စေ၊ [Open Camera](#) ကဲ့သို့သော app သုံးပြီးဖြစ်စေ ရွှေ့ခြင်းဖြင့် ဘယ်မီဒီယာကို သိမ်းထားလဲ သတ်မှတ်နိုင်သည်။ ဖွက်ထားသောဖိုင်များကို မမြင်စေရန် setting သို့သွား၍ “show hidden files”ကို “turn off” လုပ်ထားကြောင်း သေချာပါစေ။

Some specialized documentation apps, like [Tella](#) or [Eyewitness to Atrocities](#), store documentation in separate encrypted galleries whose contents are only accessible within the app, which may make it less obvious to someone searching your phone. Documentation in these secure galleries requires a separate app passcode, so it remains encrypted even when your phone is unlocked.

[Tella](#) or [Eyewitness to Atrocities](#) ကဲ့သို့ မှတ်တမ်းတင်ခြင်းကို အထူးပြု app များသည် လျှို့ဝှက်ထိန်းသိမ်းသော encrypted gallery များတွင် သီးသန့် မှတ်တမ်းတင်ထားနိုင်ပြီး app ကို သုံး၍သာ လက်လှမ်းမီ နိုင်သောကြောင့် သင့်ဖုန်းကို ရှာဖွေစစ်ဆေးခြင်းခံရသောအခါ သိသာထင်ရှားမှုကို လျော့နည်းစေသည်။ ထို gallery များတွင် မှတ်တမ်းတင်သောအခါ သီးသန့်လျှို့ဝှက်နံပါတ်passcodeလိုအပ်ပြီး သင့်ဖုန်း unlocked ဖြစ်သောအချိန်တွင်တောင် လျှို့ဝှက်ထိန်းသိမ်းမှု

	(encrypted) ဆက်လက်တည်ရှိနေမည်။
<p>Important note about obscuring your content</p>	<p>အကြောင်းအရာကိုမှေးမှိန်အောင်လုပ်ရာတွင်အရေးကြီးသောမှတ်ချက်</p>
<p>It is important to note that the techniques above might be enough to throw off someone who is just quickly swiping through your phone, but will not effectively hide your content from someone who is really looking.</p> <p>Also keep in mind that some countries may have laws that restrict or criminalize the use of security apps that encrypt or wipe your data. Using them to prevent authorities to accessing your data may be seen as destroying evidence or obstructing an investigation, and may be punishable as a crime. This map (comprehensive, but from 2017) provides a good starting place if you have questions about the laws in your country.</p>	<p>အရေးကြီးသောသတိပြုရန်မှာ အထက်ပါနည်းစနစ်များသည် တစ်စုံတစ်ယောက်က လျင်မြန်စွာလှည့်လှေ့ချိန်တွင်သာ ချုပ်စိတ်ရန်ဖြစ်ပြီး တစ်စုံတစ်ယောက်ကသေချာစွာကြည့်ရှုသည့်အခါတွင် အကြောင်းအရာများကို အကျိုးသက်ရောက်စွာ ဖွတ်ထားနိုင်မည်မဟုတ်ပါ။</p> <p>မှတ်ထားသင့်သည်မှာ အချို့နိုင်ငံများတွင် သင့်ဒေတာများကို လုံခြုံလျှို့ဝှက်ရန်နှင့်ရှင်းလင်းရန်သုံးသော security app များကို ဥပဒေအရ ကန့်သတ်ခြင်း ပြစ်မှုပေးခြင်း ပြုလုပ်နိုင်သည်။ ထို app များကိုအသုံးပြု၍ သင့်ဒေတာများကို အာဏာပိုင်များကို ရယူခြင်းမှာ ကာကွယ်ရန် ရည်ရွယ်ချက်ဖြင့် သက်သေကိုဖျက်ဆီးခြင်း သို့မဟုတ် စုံစမ်းစစ်ဆေးမှုကို ပိတ်ဆို့ခြင်းများ ပြုလုပ်ပါက ရာဇဝတ်မှုအနေဖြင့် ပြစ်ဒဏ်ပေးနိုင်သည်။ ယခုမြေပုံသည် သင့်နိုင်ငံဥပဒေနှင့်ပတ်သက်၍ မေးခွန်းရှိပါက အစပြုလေ့လာနိုင်သည် (ပြည့်စုံသော်လည်း ၂၀၁၇)</p>
<p>Set up offline sharing</p>	<p>အော်ဖ်လိုင်းမျှဝေရန်ပြင်ဆင်ခြင်း</p>
<ul style="list-style-type: none"> In a situation where you don't have internet after you've captured content, you may still want to get the 	<p>အကြောင်းအရာများကို ဖမ်းယူပြီးသော်လည်း အင်တာနက်မရှိသည့်</p>

<p>documentation off your phone for security reasons, to free up space, or to share with others. Regularly offloading documentation from your phone will also help to minimize what information is compromised should your phone ever be confiscated and unlocked.</p>	<p>အခြေအနေတွင် သင့်လုံခြုံရေးအရသော်လည်းကောင်း၊ နေရာလွတ်ရရင်လည်းကောင်း၊ မျှဝေရန်လည်းကောင်း လိုအပ်လာလျှင် မှတ်တမ်းများကို ဖုန်းမှ ဖယ်ထုတ်ထားသင့်သည်။ မှတ်တမ်းများကို ပုံမှန် offload ဖယ်ထုတ်ထားခြင်းဖြင့် သင့်ဖုန်းကို သိမ်းဆည်းရှာဖွေပြီး unlock လုပ်ခံရလျှင် အချက်အလက်များပေါက်ကြားသွားသော အခြေအနေကို လျော့နည်းစေသည်။</p>
<p>Even if you cannot connect to the internet, you can still connect to wifi-enabled or Bluetooth-enabled devices locally, such as another phone or a wifi USB drive. Your phone should typically come with an app / interface for you to connect and transfer. If your phone supports it, you can also plug in a USB On-The-Go (OTG) drive or connector to offload documentation to the OTG drive or another device.</p> <p>These methods are discussed in more detail in our File sharing and communication during an internet shutdown tutorial and our Video As Evidence: Tech Tools – Transferring Files tipsheet.</p>	<p>အင်တာနက်မဆက်သွယ်နိုင်သော်လည်း အခြားဖုန်း သို့မဟုတ် Wifi USB drive စသဖြင့် Wifi or Bluetoothနှင့် ချိတ်ဆက်ထားသော deviceများမှ တဆင့် ဆက်သွယ်နိုင်သည်။ သင့်ဖုန်းသည် ပုံမှန်အားဖြင့် app ဆက်သွယ်မှုစနစ်များမှ ဆက်သွယ်ပို့ဆောင်နိုင်စွမ်း ရှိလိမ့်မည်။ အကယ်၍ ထိုနည်းကိုပံ့ပိုးလျှင် USB on-the-go (OTG) drive သို့မဟုတ် ကွန်နက်တာနှင့် ပလပ်ထိုးပြီး မှတ်တမ်းများကို OTG drive သို့မဟုတ် အခြား device ထဲသို့ offload (ဖယ်ထုတ်) လုပ်နိုင်သည်။</p> <p>“အင်တာနက်ဖြတ်တောက်ချိန်အတွင်းဖိုင်များမျှဝေခြင်းနှင့်ဆက်သွယ်ခြင်း” သင်ခန်းစာနှင့် “ဗီဒီယိုဖြင့်သက်သေ - နည်းပညာကိရိယာ - ဖိုင်များလွှဲပြောင်းခြင်း” တွင် ထိုနည်းလမ်းများကို အသေးစိတ်ဆွေးနွေးမည်။</p>
<ul style="list-style-type: none"> Practice before you're in a crisis situation 	<p>အကြပ်အတည်းမကျရောက်မီအခြေအနေတွင်လေ့ကျင့်ခြင်း</p>
<p>Set up the phone now if and while you have internet access.</p>	<p>ယခုသို့မဟုတ်အင်တာနက်အသုံးပြုခွင့်ရှိချိန်တွင် ဖုန်းအား setup လုပ်ခြင်း</p>

<p>Start practicing using the apps in everyday situations (where there are no security concerns) so that you become familiar and comfortable using them. Make good basic phone security your default practice. This way the methods will be second-nature when you're in a crisis situation with other things to worry about.</p>	<p>နေ့စဉ်အခြေအနေတွင် appများကို စတင်သုံးစွဲလေ့ကျင့်ရန် (လုံခြုံရေးစိုးရိမ်မှုမရှိသောအချိန်) သို့မှသာ သုံးစွဲရာတွင် ရင်းနှီးပြီး သက်တောင့်သက်သာရှိစေမည်။ မူသေလေ့ကျင့်ရန် ကောင်းမွန်သော အခြေခံဖုန်းလုံခြုံရေး ပြုလုပ်ထားပါ။ အခြားစိတ်ပူစရာများရှိလာသော အခြေအနေတွင် သဘာဝအလျောက်သုံးစွဲတတ်ရန်နည်းလမ်းဖြစ်သည်။</p>
<ul style="list-style-type: none">• Check out the next post in this series, “Should I Use This Documentation App?”	<p>ဒီစီးရီးမှနောက်ထပ်ခေါင်းစဉ်ဖြစ်သော “ဒီမှတ်တမ်းတင်appကို သုံးသင့်ပါသလား?” ကိုကြည့်ရန်</p>

Should I Use This Documentation App?

Documenting During Internet Shutdowns series

By [Yvonne Ng](#)

With contributions by [Arul Prakkash](#)

This post is part of a series on [Documenting During Internet Shutdowns](#). Look out for our comparison chart of various documentation apps, coming soon!

Last reviewed: 31 January 2020

“ဒီမှတ်တမ်းတင် app ကို သုံးသင့်ပါသလား?”

အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

ရေးသားသူ - [Yvonne Ng](#)

ပံ့ပိုးသူ - [Arul Prakkash](#)

ဒီပို့စ်သည် “အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း” စီးရီး၏ အပိုင်းဖြစ်သည်။ မှတ်တမ်းတင်သော app များကို နှိုင်းပြသော ဇယားများ မကြာမီ လာမည်!!

နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်

There are many apps that documenters can use to capture video, ranging from your phone’s native [camera app](#), to more specialized documentation apps like [ProofMode](#), [Tella](#), or [Eyewitness to Atrocities](#). Some apps have features that rely on internet access, so keep in mind that those features may not be available in the event of an internet shutdown.

We can’t tell you which specific app is the most appropriate for you, since that depends on your situation, needs, and risks (check out this blog post for more on [how to assess your risks](#)

ဗီဒီယိုဖမ်းယူရန် မှတ်တမ်းတင်သူများ အသုံးပြုနိုင်သော app များစွာမှာ ဖုန်းထဲတွင်ပါဝင်သော “[Camera App](#)” မှ အစ ပိုမိုအထူးပြုထားသော မှတ်တမ်းတင် app များဖြစ်သည့် “[ProofMode](#), [Tella](#), [Eyewitness to Atrocities](#)” အထိရှိသည်။ အချို့ app ၏ အင်္ဂါရပ်များသည် အင်တာနက်ချိတ်ဆက်ခွင့်ကို မှီခိုသည့်အတွက် အင်တာနက်ဖြတ်တောက်ချိန်တွင် ရရှိနိုင်မည်မဟုတ်သည်ကို သတိချပ်သင့်သည်။

<p>and threats). With your risk assessment in hand, these guiding questions below can help you evaluate which video documentation app might work best for you.</p>	<p>ဘယ်တီကျသော app က သင့်အတွက်အသင့်တော်ဆုံးဖြစ်သည်ကို ကျွန်ုပ်တို့ မပြောနိုင်ပါ။ သင့်အခြေအနေ၊ လိုအပ်ချက်၊ အန္တရာယ် တွင် မှုတည်သည် (ဒီဘလော့ဂ်ပို့စ်တွင်ကြည့်ပါ - “သင့်အန္တရာယ်နှင့် ခြိမ်းခြောက်မှုကို ဘယ်လိုအကဲဖြတ်မလဲ”)။</p> <p>အန္တရာယ်အကဲဖြတ်မှုလက်ဝယ်ရှိချိန်တွင် ယခုလမ်းညွှန်မေးခွန်းများသည် ဘယ်မှတ်တမ်းတင် app ကို သုံးရင် သင့်အတွက် အကောင်းဆုံးဖြစ်မှာလဲ ဆိုတာကို သုံးသပ်ပေးသွားမှာပါ။</p>
<p>Who made the app and do I trust them?</p>	<p>App တွေကို ဘယ်သူကလုပ်သလဲ? ယုံကြည်ရသလား?</p>
<p>You should always consider the creators of any app that you download and install on your device, and whether you can trust them to not put you at risk, intentionally or unintentionally.</p> <p>Some things to look out for are:</p>	<p>App တွေကို download and install မလုပ်မီ တီထွင်ထားသူကို ယုံကြည်ရသလား ရည်ရွယ်လို့ဖြစ်စေ မရည်ရွယ်ဘဲဖြစ်စေ မိမိအပေါ် အန္တရာယ်ရှိနိုင်လားဆိုတာ စဉ်းစားပါ</p> <p>ကြည့်ရှုရမည့် အချို့အချက်များမှာ</p>
<ul style="list-style-type: none"> • Is the app developer reputable? What are people in your community and wider network saying about them and their tools? • Is the app developer vulnerable? Consider their context and how likely they could be compelled to hand over your data or create a backdoor for authorities (or whether they've actually done so in the past). What country is the data stored in and what are the laws concerning court orders in that jurisdiction? • Is the app developer maintaining the app? Unmaintained 	<ul style="list-style-type: none"> - Appကို တီထွင်ထုတ်လုပ်သူသည် နာမည်ကောင်းရသူလား? သူတို့နှင့်သူတို့ရဲ့tools တွေနဲ့ပတ်သက်ပြီးကိုယ့်ရဲ့ကွန်ယက်ထဲမှာ ဘာတွေပြောကြသလဲ? - Appကို တီထွင်ထုတ်လုပ်သူသည် ထိခိုက်လွယ်သူလား? သူ့ရဲ့အခြေအနေကို စဉ်းစား၍ သူသည်သင့်ဒေတာများကို အတင်းအကြပ်လက်လွှဲခိုင်းခံရမည့်သူလား

tools are susceptible to hacks that exploit discovered vulnerabilities. Check the developer's website or the app's Google Play page for the "last updated" date.

- How established is the app developer, and does it seem like they will be able to sustain the app over time?
- Is the app open-source? Apps that are open to scrutiny are more likely to have their security issues addressed or at least identified. Is the developer being transparent about the efficacy and security of the app?
- What motivations or incentives drive the app developer's work, and how might that influence their trustworthiness? For example, are they mission-driven? For-profit? Sponsored by a particular funder?

While not a direct indicator of trustworthiness or not, the cost of the app may be an important consideration. Some apps have a high monthly subscription fee or per-video fee.

အာဏာပိုင်များကနောက်ကွယ်မှာစေခိုင်းခံရသူလား (ဒါမျိုးဖြစ်ဖူးသူလား)။ ဘယ်တိုင်းပြည်မှာ ဒေတာကို ထိန်းသိမ်းတာလဲ သူတို့ရဲ့တရားရုံးဥပဒေအဆုံးအဖြတ်က ဘာတွေလဲ

- Appကို တီထွင်သူကပဲ app ကို maintain လုပ်တာလား maintain မလုပ်ထားတဲ့ tools တွေဟာ ခိုးယူခြင်းခံရဖို့အတွက် ခံနိုင်ရည်ရှိလား။ ရှာဖွေတွေ့ရှိတဲ့အခါ အမြတ်ထုတ်ခံရနိုင်လား app တီထွင်သူရဲ့ဝက်ဘ်ဆိုက် သို့မဟုတ် app google play page မှာသွားပြီးလေ့လာ၍ “နောက်ဆုံးupdateရက်စွဲ” ကိုကြည့်ပါ။
- App ကိုတီထွင်သူသည် ဘယ်လောက်ခိုင်မာစွာဖွဲ့စည်းထားလဲ ဒီapp ကိုရှေ့ရည်တည်တဲ့အောင်ထိန်းသိမ်းထားနိုင်လား
- App သည် ပွင့်လင်းအရင်းအမြစ် ဖြစ်ရဲ့လား။ စိစစ်ရေးကဖွင့်ပေးထားတဲ့ app တွေအားများသောအားဖြင့် သူတို့ရဲ့လုံခြုံရေးပြဿနာတွေကို အမည်တပ်ပြီး ဖော်ထုတ် ပြသထားလေ့မရှိပါဘူး။ တီထွင်သူ သည် app ရဲ့လုံခြုံရေးနဲ့ ထိရောက်မှုကို ပွင့်လင်းမြင်သာစေပါသလား။
- ဘယ်လိုအားပေးလှုံ့ဆော်မှု၊ မက်လုံးတွေကြောင့် ဒီ app ကို တီထွင်စေခဲ့သလဲ သူတို့ရဲ့ယုံကြည်မှုအတွက် ဘယ်လိုလွှမ်းမိုးမှုရှိသလဲ? ဥပမာ သူတို့က မစ်ရှင်တခု အတွက်လား? အကျိုးအမြတ်အတွက်လား? ငွေကြေးထောက်ပံ့သူ တယောက်ကြောင့်က ပံ့ပိုးတာလား?

ကုန်ကျစရိတ်သည် ယုံကြည်စိတ်ချရမှုကို တိုက်ရိုက်ရည်ညွှန်း

	<p>ပြသခြင်းမရှိသော်လည်း app ၏ ကုန်ကျစရိတ်သည်လည်း ထည့်သွင်းစဉ်းစားရန် အရေးကြီးသည်။ အချို့ app များ၏လပေးခ သို့မဟုတ် ဗီဒီယိုတစ်ခုစီ၏ အဖိုးခကြေးငွေသည်မြင့်မားလှသည်။</p>
<ul style="list-style-type: none"> • Check out the EFF surveillance self-defense guide on choosing apps for more. 	<ul style="list-style-type: none"> - App ရွေးချယ်ရန်အတွက် EFF စောင့်ကြည့်လေ့လာရေး ကာကွယ်ရေး လမ်းညွှန်ကို ဒီမှာကြည့်ပါ
<p>Where is the app downloadable from?</p>	<p>ဒီ app ကို ဘယ်နေရာက download လုပ်နိုင်မလဲ?</p>
<p>You should always only download and install apps from reputable app stores or websites. Even if you have done thorough research to determine the trustworthiness of an app, sketchy app stores may misrepresent their wares and lead you to download an illegitimate imposter created for nefarious purposes. For example, last year the digital rights organization SMEX issued a warning about various websites marketing an app called “WhatsApp Plus” (to be clear, this is not a WhatsApp product!), which could potentially be saving and selling users’ data, or enabling phones that install it to be hacked.</p> <p>Some security-conscious developers even provide cryptographic keys that enable you to verify their authenticity. They will usually provide an explanation for how to verify these signatures.</p>	<p>နာမည်ကောင်းရှိသော app store သို့မဟုတ် websites မှသာ အမြဲတမ်း Download and install လုပ်ပါ။ သေချာစေ့စပ်စွာ သုတေသနပြုသော်လည်း အချို့ app store များသည် မှားယွင်းစွာ ဖော်ပြထားခြင်းကြောင့် မကောင်း သောရည်ရွယ်ချက်ဖြင့် တရားမဝင်သော အတုအယောင်များကို download လုပ်စေလိမ့်မည်။ ဥပမာ - လွန်ခဲ့သောနှစ်က ဒစ်ဂျစ်တယ်အခွင့်အရေးဆိုင်ရာ အဖွဲ့အစည်းဖြစ်သော SMEX မှ သတိပေးချက် ထုတ်ခဲ့သည်မှာ ဝက်ဘ်ဆိုက်မျိုးစုံနှင့်ပတ်သက်ပြီး အရောင်းမြှင့်တင်ခဲ့သည့် “WhatsApp Plus” ဟုခေါ်သော app တခုသည် (သတိပြုရန် WhatsApp ၏ ထုတ်ကုန်မဟုတ်ပါ) သုံးစွဲသူများ၏ ဒေတာများကို စုဆောင်းပြီး ရောင်းချနိုင်ချေရှိခြင်း သို့မဟုတ် install လုပ်ထားသည့် ဖုန်းများထဲသို့ ခိုးဝင်အချက်အလက်ယူခြင်းလုပ်နိုင်ခွင့်များ ရရှိစေခဲ့သည်ဟု သတိပေးခဲ့သည်။</p>

	<p>လုံခြုံရေးကိုသတိထားသော တီထွင်သူများသည် cryptographic keys များ ပံ့ပိုးထားခြင်းဖြင့် သူတို့၏ စစ်မှန်မှုကို အတည်ပြုနိုင်စေသည်။ ထိုသို့သော လက်မှတ် signature များကို မည်ကဲ့သို့အတည်ပြုနိုင်ကြောင်းလည်း ထည့်သွင်းရှင်းပြချက်များပါရှိသည်။</p>
<p>Where will the data be stored?</p>	<p>ဒေတာကို ဘယ်နေရာမှာ သိမ်းမလဲ?</p>
<p>Some documentation apps only store your data and documentation locally on your device, while some only or additionally send and store your data elsewhere. In many cases this is inherent to the design and purpose of the app, such as the Eyewitness to Atrocities app, which sends an unaltered copy of your documentation to a Lexis Nexis storage facility so that Eyewitness can vouch for the chain of custody and integrity of the material. You can only export your media out of the encrypted gallery within the Eyewitness app after it's been sent for safeguarding.</p>	<p>အချို့မှတ်တမ်းတင် app များသည် သင့်ရဲ့ဖုန်း(device)ထဲတွင်သာ ဒေတာနဲ့ မှတ်တမ်းများကိုသိမ်းဆည်းနိုင်သော်လည်း အချို့တွင် ဒေတာများကို အခြားအရပ်တွင်နှင့် ထိုအရပ်တွင်သာပို့ပေးသိမ်းဆည်းနိုင်သည်။ အခြေအနေများစွာတွင် app ၏ ဒီဇိုင်းနဲ့ ရည်ရွယ်ချက်အရ - ဥပမာ Eyewitness to Atrocities app သည် သင်၏မပြောင်းလဲထားသော ကော်ပီမှတ်တမ်းများကို Lexis Nexis ထိန်းသိမ်းရာဌာနသို့ ပို့ပေးခြင်းဖြင့် Eyewitness သည် မူရင်း၏ခိုင်မာမှုနှင့် ချုပ်နှောင်ခြင်း၏ကွင်းဆက်ကို အာမခံနိုင်သည်။ သင်၏မီဒီယာကို လျှို့ဝှက်ထိန်းသိမ်းသော encrypted gallery မှ ပြင်ပသို့ထုတ်ပို့ရာသော်လည်း Eyewitness app အတွင်းတွင်သာ ဖြစ်ပြီး ပို့ပြီးချိန်တွင် လုံခြုံသောကာကွယ်မှုရှိမည်။</p>

<p>It's up to you to determine whether you need your documentation to stay on your device only, whether you need it sent and stored to a remote location that you control (as is an option with Tella), or whether to need to send it an external organization / platform that you allow to access and use your documentation. Keep in mind that during an internet shutdown, you won't be able to transmit your documentation over the internet right away, so you will need an app that at least temporarily enables you store (and ideally back up) your documentation locally (Check out Backing up phone media without internet or a computer).</p>	<p>သင်မှတ်တမ်းတင်ထားသောအချက်အလက်များကို သင့်ဖုန်း(device)တွင် သိမ်းမလား၊ အဝေးထိန်းနေရာတွင်ပို့ပေး၍ (Tella ကို ရွေးချယ်လျှင်) ထိန်းသိမ်းမလားဆိုတာကို သင်ကိုယ်တိုင်ဆုံးဖြတ်နိုင်သည်။ သို့မဟုတ် သင့်မှတ်တမ်းများကိုသုံးစွဲမည့် ပလက်ဖောင်းသို့မဟုတ် ပြင်ပအဖွဲ့အစည်းများဆီပို့ပြီး အသုံးပြုဖို့ခွင့်ပြုမလားဆိုတာကို ဆုံးဖြတ်ပါ။ အင်တာနက်ဖြတ်တောက်ချိန်တွင် သင်မှတ်တမ်းများကို အင်တာနက်မှတစ်ဆင့်ပို့လို့မရဆိုသည့်အချက်ကို သတိပြု၍ အနည်းဆုံးယာယီ ထိန်းသိမ်းရန် (အရန်သိမ်းရန်) သိမ်းဖို့ app လိုအပ်မည်။ (ဖုန်းမီဒီယာကို အင်တာနက် သို့မဟုတ် ကွန်ပျူတာမရှိဘဲ အရန်သိမ်းခြင်း)</p>
<p>If your data will be sent to a remote location, be aware of which countries the data will reside. How vulnerable is data to being exposed in those countries, whether by court orders or other means? What risks do you face by having your data exposed there?</p>	<p>သင့်ဒေတာတွေကို အဝေးထိန်းနေရာကို ပို့ပေးရာတွင် မည်သည့်နိုင်ငံတွင် သိမ်းဆည်းမည်ကို သတိပြုပါ။ သင့်ဒေတာသည် ထိုနိုင်ငံများတွင် မည်မျှထိခိုက်နိုင်ရည် ရှိကြောင်း၊ တရားရုံးမှ ညွှန်ကြားချက်ဖြင့် သို့မဟုတ် အခြားနည်းဖြင့် ထုတ်ယူနိုင်ခြင်းရှိမရှိ? ထိုနေရာတွင် ဒေတာများပေါက်ကြားလျှင် မည်သို့ အန္တရာယ် ရင်ဆိုင်နိုင်ရသလဲ?</p>
<p>Does the app encrypt my media?</p>	<p>App က သင့်မီဒီယာကို လျှို့ဝှက်ထိန်းသိမ်းမှာလား?</p>
<p>Some apps, such as Tella and Eyewitness to Atrocities, provide file encryption and/or encrypted storage for your documentation, separate from your phone's main gallery and your phone's encryption, so that your media and metadata are never unencrypted on your device unless accessed through the app with a passcode. This means that even if your phone is unlocked, your documentation remains encrypted. This can</p>	<p>Tella and Eyewitness to Atrocitiesစတဲ့ appတွေက သင့်မှတ်တမ်းတွေ အတွက် လျှို့ဝှက်ထိန်းသိမ်း သိုလှောင်မှုများကို ဖုန်း၏ပင်မgalleryမှ ခွဲ၍ သိမ်းဆည်းနိုင်ရန် ပံ့ပိုးပေးသည်။ ထိုနည်းဖြင့် သင့်မီဒီယာနှင့် metadata များသည် app ကို လျှို့ဝှက်နံပါတ်နဲ့ သုံးနေသ၍ ဘယ်တော့မှ လျှို့ဝှက်မှု</p>

<p>provide an extra level of protection for your documentation.</p>	<p>ပေါက်ကြားမည်မဟုတ်။ ဆိုလိုသည်မှာဖုန်းသည် unlock ဖြစ်သွားသည့်တိုင် မှတ်တမ်းများသည် လျှို့ဝှက်ထိန်းသိမ်းထားရှိမည်။ ထိုနည်းလမ်းဖြင့် သင့်မှတ်တမ်းများကို အပိုအဆင့်ကာကွယ်ထားမည်ဖြစ်သည်။</p>
<p>If the app sends and stores your media to a remote location after your internet is restored, also consider whether you need your media to be encrypted while in transit and while in the remote location, as the EyeWitness app, for example, does.</p> <p>Keep in mind that while encryption is legal in most places, some countries may have laws that restrict or criminalize its use. This map (comprehensive, but from 2017) provides a good starting place if you have questions about the laws in your country.</p>	<p>ထို app သည် အင်တာနက်ပြန်လည်ရရှိပြီးနောက် သင့်မီဒီယာများကို အဝေးထိန်းနေရာသို့ ပို့ဆောင်သိမ်းဆည်းသည့်အခါ လမ်းတွင်တဆင့်နားချိန်၌ မီဒီယာများသည် လျှို့ဝှက်ထိန်းသိမ်းရန် လိုအပ်ချက်ရှိမရှိ စဉ်းစားပါ (ဥပမာ - EyeWitness app)</p> <p>လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption သည် တချို့နိုင်ငံများတွင် တရားဝင်ဖြစ်ပြီးတချို့နိုင်ငံများတွင် ကန့်သန့်ချက် သို့မဟုတ် သုံးစွဲခြင်းကြောင့် ရာဇဝတ်မှု မြောက်နိုင်သည်။</p>
<p>Does the app capture important metadata (without internet)?</p>	<p>အရေးကြီးသော metadata များကို အင်တာနက်မရှိဘဲ app ကနေ ဖမ်းယူထားနိုင်ပါသလား?</p>
<p>Metadata is data that describes your video or photo, like the time and date or the location. This information is valuable for identifying, understanding, authenticating, and verifying your video or photo as documentation of a specific event. In the context of an internet shutdown, an app's ability to automatically collect certain metadata and/or to allow you to easily input useful descriptive information on the spot is especially useful, as</p>	<p>Metadata ဆိုသည်မှာ သင့်မီဒီယို သို့မဟုတ် ဓာတ်ပုံများကို အချိန်နေရာနှင့်အရပ်ဒေသ ညွှန်ပြသော ဒေတာဖြစ်သည်။ ထိုသတင်းအချက်အလက်များသည် သင့်မီဒီယိုနှင့် ဓာတ်ပုံများကို ဖြစ်ရပ်တခုအတွက် မှတ်တမ်းတင်ရာတွင် ခွဲခြားသတ်မှတ်ခြင်း၊</p>

<p>there may be a long period of time before you can share the documentation with anyone (time during which details can be forgotten, circumstances might change, etc, etc).</p>	<p>နားလည်စေခြင်း၊ စစ်မှန်ကြောင်းသက်သေပြခြင်းနှင့် အတည်ပြုခြင်းများအတွက် တန်ဖိုးရှိသည်။ အင်တာနက်ဖြတ်တောက်ချိန်အခြေအနေမျိုးတွင် ထိုapp၏ အလိုအလျောက် စုဆောင်းသွားခြင်း သို့မဟုတ် ရှင်းပြချက်များကို လွယ်ကူစွာထည့်သွင်းနိုင်ခြင်းကြောင့် metadata များသည် လွန်စွာအသုံးဝင်သည်။ အဘယ်ကြောင့်ဆိုသော် တစ်စုံတစ်ယောက်နဲ့ သင်မျှဝေနိုင်သောအချိန်မတိုင်မီ (အသေးစိတ်ဖြစ်ရပ်များသည် မေ့လျော့နိုင်ခြင်း အခြေအနေအရပ်ရပ်ပြောင်းလဲခြင်းတို့ကြောင့်ဖြစ်သည်။</p>
<p>Most specialized documentation apps such as ProofMode have enhanced metadata features, and gather more metadata than typical built-in camera apps. Enhanced metadata might include various sensor data, nearby wifi or bluetooth signals, device data, cryptographic hash, and user-supplied information, all which can facilitate authentication and verification of the media later on.</p>	<p>ProofMode ကဲ့သို့သော အထူးပြုထားသည့် app များတွင် ပိုမိုကောင်းမွန်သော metadata features ပါနိုင်ပြီး built-in camera ထက် metadata များကို ပိုပြီးစုဆောင်းနိုင်သည်။ ပိုမိုကောင်းမွန်သော metadata တွင် အမျိုးမျိုးသော ဆင်ဆာဒေတာ၊ အနီးတဝိုက်ရှိ wifi or Bluetooth အချက်များ ဖုန်း(device)၏ ဒေတာ cryptographic hash နှင့် သုံးစွဲသူထည့်သွင်းထားသော အချက်အလက်များ အားလုံးကို မီဒီယာတွင် စစ်မှန်ကြောင်းသက်သေပြခြင်းနှင့် အတည်ပြုခြင်းများ ပါဝင်သည်။</p>

<p>Keep in mind that during an internet shutdown, you will need an app that does not require data to be transmitted in order to generate or record the metadata. Some apps may rely on the internet, instead of the hardware sensors, to collect certain metadata. For example, if the location data is captured from look ups on the device, the metadata may reflect the last location where the device had data connection, instead of the actual position of the hardware. The app should also ideally allow you to store the metadata locally without internet, including saving any forms you are filling out (e.g. Tella’s “offline mode”).</p>	<p>သတိပြုရန်မှာ အင်တာနက်ဖြတ်တောက်ချိန်တွင် metadata ထုတ်လုပ်နှင့် ရိုက်ကူးရန်အတွက် ဒေတာမလိုသော app ကို သုံးရမည်။ အချို့ app များသည် metadata များကို စုဆောင်းရန် hardware ဆင်ဆာအစား အင်တာနက်ကို အားကိုးခြင်းဖြစ်နိုင်ချေရှိသည်။ ဥပမာ - ဒေတာ၏အရပ်ဒေသကို ဖုန်း (device)၏ စောင့်ကြည့်မှုများမှ ဖမ်းယူသည့်အခါ metadata သည် hardware ၏ တကယ့်ရှိနေသော အနေအထား အစား ဖုန်း(device)၏ ဒေတာနောက်ဆုံးရခဲ့သည်နေရာကို ရောင်ပြန်ဟပ်သည်။ ဒီ app သည် metadata များကိုထိုနေရာတွင်ပင် အင်တာနက်မရဘဲ သိုလှောင်ထားပေးပြီး မည်သည့်ပုံစံဖြင့်ဖြည့်သည်ဖြစ်စေ စုဆောင်းထားပေးမည် (ဥပမာ - Tell ၏ အော်ဖ်လိုင်းပုံစံ)</p>
<p>Can I export data from the app?</p>	<p>App က ဒေတာတွေကို ပြင်ပသို့ ထုတ်ပို့လို့ရသလား?</p>
<p>Depending on your intentions for the documentation, it may be essential to be able to export the video documentation and its metadata from the app, in a format that is not proprietary to the app; that is, to be able to open, view, and use the media and metadata outside of the app. The ability to export means that you and others are not dependent on a single app or service provider to access your documentation, and gives you more leeway in working with the content going forward. Keep in mind that some metadata may not be comprehensible if you do not have access to certain databases or conversion charts to interpret the numbers (for instance, in the case of cell tower IDs or Wi-Fi networks).</p>	<p>သင့်ရဲ့မှတ်တမ်းတင်ချင်တဲ့ရည်ရွယ်ချက်ပေါ်မူတည်ပြီးတော့ ဒီဒီဟိုမှတ်တမ်းနဲ့ သူ့ရဲ့ metadataတွေကို ပြင်ပသို့ထုတ်ပို့နိုင်စွမ်းဟာ မရှိမဖြစ်လိုအပ်ပါတယ်။ သူ့ရဲ့ format ဟာ app မှာပဲ ပိုင်ဆိုင်တာမဟုတ်ဘဲ တခြားသူတွေ ဖွင့်လို့ မြင်လို့ သုံးလို့ရတဲ့အခြေအနေဖြစ်ဖို့လိုပါတယ်။ ပြင်ပသို့ထုတ်ပို့နိုင်စွမ်းဆိုတာ သင်ရော တခြားသူများရောဟာ app တခုတည်း သို့မဟုတ် ဝန်ဆောင်မှုတခုတည်းကို သုံးတာမဟုတ်ဘဲ အကြောင်းအရာတွေကို လွတ်လပ်စွာ နောက်ထပ်တဆင့်ထပ်ပြီး ဖြန့်ဖြူးနိုင်ဖို့လိုပါတယ်။ သတိပြုရန်မှာ တချို့ metadata တွေဟာ certain databases ထဲကိုဝင်လို့မရရင် ဇယားတွေကို နံပါတ်အဖြစ်</p>

	<p>လွှဲပြောင်းလို့မရရင် နားလည်အောင် ဘာသာပြန်ထုတ်ဖော်အသုံးပြုလို့ မရပါဘူး (ဥပမာ - ဆဲလ်တာဝါတိုင်နံပါတ် သို့မဟုတ် wifi ကွန်ယက်)</p>
<p>Note that some apps may have a deliberate closed chain of custody and not allow users to export, while some apps may simply not be designed with an export use case in mind. Also be aware that some apps, like Eyewitness to Atrocities, may not let you export until you have uploaded the media to a remote server (which you need internet access to do), and some apps may allow you to export the media, but not the metadata (other than any metadata that lives in the file itself).</p>	<p>သတိပြုရန်မှာ အချို့ app တွေကျတော့ ကွင်းဆက်အပိတ်ထိန်းထားတာ ဖြစ်နေလို့ အပြင်ကိုထုတ်ပို့ခွင့်မရှိပါဘူး၊ အချို့ app တွေကတော့ အပြင်ထုတ်ပို့ဖို့အတွက်ကို ဒီဇိုင်းမလုပ်ထားတာပါ။</p> <p>တချို့ app တွေက (Eyewitness to Atrocities) မီဒီယာကို ရိုမိုက်ဆာဗာဆီ မတင်ဘဲ အပြင်ထုတ်ပို့ခွင့်မပေးပါဘူး (အင်တာနက်သုံးဖို့လိုပါတယ်)</p> <p>တချို့ App က မီဒီယာတွေအပြင်ထုတ်ပို့လို့ရပြီး တခြား metadata တွေ ပို့လို့မရပါ (ဖိုင်ထဲမှာသက်ရှိနေတဲ့ metadata မှအပ)</p>
<p>If you need to export, ideally your app should allow you to export a copy of the media without any changes or transformations, and a copy of the metadata in a stkamurdized readable text format. Tella metadata, for example, is stored encrypted in the Tella gallery, but can be exported as CSV. Additionally, during an internet shutdown, it is necessary to have options for exporting to offline apps or non-internet dependent services. Most apps that allow you to export have some kind of “Share” button that triggers a share menu, which Android populates with a list of apps on your phone that are capable of handling that type of content. Unfortunately app developers can customize their share menus and there is no consistency between apps.</p>	<p>သင့်အနေနဲ့ ပြင်ပထုတ်ပို့ဖို့လိုအပ်လာရင် သင်သုံးတဲ့ app က မီဒီယာ ကော်ပီကိုသာ ပြောင်းလဲခြင်းမရှိဘဲ၊ metadata ကော်ပီကိုလည်း ဖတ်လို့ရတဲ့စာသားပုံစံနဲ့သာ ပို့ဖို့ခွင့်ပြုတဲ့ app ဖြစ်ရပါမယ်</p> <p>ဥပမာ Tella metadata ဆိုရင် Tella gallery ထဲမှာ လျှို့ဝှက်ထိန်းသိမ်းထားတာဖြစ်ပြီး ပြင်ပကိုထုတ်ပို့တဲ့အခါမှာ CSV အနေနဲ့ ထုတ်ပို့လို့ရပါတယ်။ ဒါ့အပြင် အင်တာနက်ဖြတ်တောက်ချိန်မှာ ပြင်ပထုတ်ပို့ဖို့အတွက် ရွေးချယ်ရန်နည်းလမ်းတွေဖြစ်တဲ့ offline apps သို့မဟုတ် အင်တာနက်ကိုမမှီခိုတဲ့ ဝန်ဆောင်မှုဖြစ်ဖို့လိုအပ်ပါတယ်။</p> <p>များသောအားဖြင့် app အများစုဟာ ပြင်ပကိုထုတ်ပို့ဖို့အတွက် “share” ဆိုတဲ့ခလုတ်နှိပ်ရင် မျှဝေနိုင်အောင် Android မှာဆိုရင် app စာရင်းတွေထားပြီး ဒီလိုအကြောင်းအရာမျိုးကို ကိုင်တွယ်နိုင်အောင်</p>

	<p>စုစည်းထားပါတယ်။ ကံမကောင်းတာတခုကတော့ တီထွင်သူဟာ share menu ကို သူ့စိတ်ကြိုက်လုပ်နိုင်တဲ့အတွက် app တခုနဲ့တခုကြားမှာ တသမတ်တည်းမဖြစ်တတ်ပါဘူး။</p>
<p>For a larger quantity of files, it may be more efficient to access the stored files via a file manager app and copy the files from there, although you may not be able to access metadata stored in an app’s database this way. This option is also not available for apps that provide their own secure galleries, as the files will be encrypted in storage. For these apps, it is necessary to have a sharing function within the app.</p>	<p>အရေအတွက်များတဲ့ဖိုင်အတွက်ဆိုရင် app database မှာသိမ်းထားတဲ့ metadata တွေကို ဝင်ပြီးသုံးလို့မရသော်လည်း သိမ်းထားတဲ့ဖိုင်တွေကို ဖိုင်မန်နေဂျာ app ကနေတဆင့် ဝင်ပြီးသုံးမယ် ကူးယူမယ်ဆိုရင် ပိုပြီးထိရောက်မှုရှိပါတယ်။ ဒီရွေးချယ်မှုနည်းလမ်းဟာ သူတို့ရဲ့ကိုယ်ပိုင်လုံခြုံသော gallery တွေပံ့ပိုးထားတဲ့ app တွေအတွက် ရမှာမဟုတ်ပါဘူး။ ဘာကြောင့်လဲဆိုတော့ အဲဒီဖိုင်တွေဟာ သိုလှောင်နေရာ (storage) ထဲမှာပဲ လျှို့ဝှက်ထိန်းသိမ်းထားလို့ဖြစ်ပါတယ်။ အဲဒီ app တွေဟာဆိုရင် app အတွင်းမှာ sharing function ရှိဖို့လိုအပ်ပါတယ်။</p>
<p><i>Check out the next post in this series, “Maintaining Verifiable Media During an Internet Shutdown” and our forthcoming comparison chart of documentation apps.</i></p>	<p>ဒီစီးရီးထဲမှ နောက်ထပ်ပိုစ် “အင်တာနက်ဖြတ်တောက်ချိန်တွင် ခိုင်လုံသောမီဒီယာ အချက်အလက်များကိုထိန်းသိမ်းခြင်း” နှင့် မှတ်တမ်းတင်သော app များကို နှိုင်းပြထားသော လာမည့် ဇယားချပ်</p>

Maintaining Verifiable Media During an Internet Shutdown

Documenting During Internet Shutdowns series

By [Yvonne Ng](#)

With contributions by [Arul Prakkash](#)

This post is part of a series on [Documenting During Internet Shutdowns](#).

Last reviewed: 31 January 2020

[Human rights defenders](#), [investigators](#), [researchers](#), and [journalists](#) often rely on first-hand documentation filmed by witnesses to monitor, report, and address human rights violations. To ensure that they are acting on correct information, these users take steps to authenticate and verify the documentation they receive, a process that can be painstaking and time-consuming.

ခိုင်လုံသောမီဒီယာ အချက်အလက်များကို အင်တာနက်ဖြတ်တောက်ချိန်တွင် ထိန်းသိမ်းခြင်း

အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

ရေးသားသူ - [Yvonne Ng](#)

ပံ့ပိုးသူ - [Arul Prakkash](#)

ဒီပို့စ်သည် “[အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း](#)” စီးရီးမှ တပိုင်းဖြစ်သည်

နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်

လူ့အခွင့်အရေးကာကွယ်သူများ၊ စုံစမ်းစစ်ဆေးသူများ၊ သုတေသနပြုသူများနှင့် သတင်းထောက်များသည် မျက်မြင်သက်သေများက ရိုက်ကူးထားသော ဦးဆုံးလက်မှတ်တမ်းများကို အားကိုးပြီးမှ လေ့လာစောင့်ကြည့်၊ အစီရင်ခံ၊ လူ့အခွင့်အရေး ချိုးဖောက်မှုများကို အမည်တပ်ခြင်း ပြုလုပ်ရသည်။ ထိုသူများက မှန်ကန်သော အချက်အလက်များပေါ်တွင် ဆောင်ရွက်ကြောင်း

	<p>သေချာအောင် သုံးစွဲသူများသည် အဆင့်များစွာ လုပ်ဆောင်၍ သူတို့ရရှိသော မှတ်တမ်းများကို စစ်မှန်ကြောင်းအတည်ပြုသည့် ဆောင်ရွက်ချက်သည် အချိန်ကြာမြင့်နိုင်သည်။</p>
<p>As a documenter, there are simple things you can do to make it easier for others to verify and corroborate your documentation, so that it can be used in timely and effective ways. These few extra steps are even more valuable during an internet shutdown, considering that:</p> <ul style="list-style-type: none"> • If you can't upload right away, the publication date and location info provided by social media is not as helpful for showing that your video was filmed on or prior to a certain date or in a certain location. • If others can't upload either, there may be less documentation available overall that can be used to corroborate your video. • If you need to pass your video through many hands offline to get it to its destination, it may be harder for others to trace the source of the video. • If you need to delete the original video from your phone because of heightened security or limited storage capacity with no cloud backup, or if you have to get rid of the phone, it may be harder to confirm the authenticity of the video. • If you forget the details about a particular video and the app you're using doesn't capture / record metadata without internet access, others may not be able to identify it later. 	<p>မှတ်တမ်းတင်သူတယောက်အနေဖြင့် အခြားသူများက သင့်မှတ်တမ်းကို အတည်ပြုပြီးဆောင်ရွက်နိုင်ရန် ရိုးရှင်းသော အချက်တချို့ လုပ်ဆောင်နိုင်သည်။ သို့မှသာ ထိုမှတ်တမ်းများသည် အချိန်မီ ထိရောက်စွာ အသုံးပြုနိုင်မည်။ အောက်ပါ အပိုအချက်များသည် အင်တာနက်ဖြတ်တောက်ချိန်တွင် ပိုပြီးတန်ဖိုးရှိသောကြောင့် ထည့်သွင်းစဉ်းစားသင့်သည်။</p> <ul style="list-style-type: none"> - ချက်ချင်း upload မလုပ်နိုင်သေးရင်ထုတ်လုပ်သောရက်နဲ့နေရာကို ဆိုရှယ်မီဒီယာတွင်တင်ထားခြင်းသည် ရိုက်ကူးထားသော ဗီဒီယိုတွင်ပြသနေသော ရက်တခုအချိန်တခုဒေသတခုရှေ့တွင် ပြသခြင်းသည် အထောက်အကူမဖြစ်ပါ - တခြားသူ upload မလုပ်နိုင်ရင်လည်း မှတ်တမ်းရရှိနိုင်ချေအလုံးစုံ နည်းပါးသည့်အတွက် သင့်ဗီဒီယိုနဲ့ အတည်ပြုနိုင်သည်။ - အော်ဖ်လိုင်းကနေလူများကတဆင့်ဖြတ်ပြီးသင့်ဗီဒီယိုကိုပို့ရမယ် ဆိုရင် ဗီဒီယိုရဲ့ပင်မရင်းမြစ်ကိုခြေရာခံဖို့ခက်ပါသည်။ - လုံခြုံရေးတင်းကြပ်လို့ နေရာလွတ်မကျန်လို့ အရန်ကူးစရာမရှိလို့ အော်ရီဂျင်နယ်ဗီဒီယိုကို ဖုန်းကနေဖျက်ပစ်ဖို့ လိုအပ်မယ်ဆိုရင်၊ ဖုန်းကိုလွှင့်ပစ်ရမယ်ဆိုရင် အဲဒီဗီဒီယိုရဲ့စစ်မှန်မှုကို အာမခံဖို့ ခက်မယ်

	<ul style="list-style-type: none"> - ဗီဒီယိုတစ်ခုရဲ့ အသေးစိတ်အချက်တွေကို မေ့သွားပြီး app ကလည်း မဖမ်းယူထားဘူးဆိုရင် metadata ကိုအင်တာနက်မသုံးဘဲ ဖမ်းယူထားတယ်ဆိုရင် အဲဒါကို နောက်ပိုင်းမှ သူများတွေက သတ်မှတ်ဖော်ထုတ်လို့ရမှာမဟုတ်ပါ
<p>The following tips can help you maintain your video during an internet shutdown to maximize its verifiability and usability as documentation later on.</p>	<p>အောက်ပါအသုံးဝင်မည့်အချက်အလက်များက “အင်တာနက်ဖြတ်တောက်ချိန်တွင် ခိုင်လုံသောမီဒီယာ အချက်အလက်များကိုထိန်းသိမ်းခြင်း” ကို ကူညီပြီး နောက်ပိုင်းမှာ မှတ်တမ်းတွေကို အတည်ပြုခြင်း အသုံးပြုခြင်းကို အကျယ်ချဲ့နိုင်ပါမယ်</p>
<p>Film or provide identifying details in the video</p>	<p>အသေးစိတ်အချက်အလက်များကို ဗီဒီယိုတွင် ထုတ်ဖော်ခြင်းရိုက်ကူးခြင်း</p>
<p>Try to include details in your video that make it easier for an investigator or journalist to later identify the time and place, like unique landmarks, the skyline, street signs, storefronts, license plates, flags, clocks, newspaper front pages, etc. You can also narrate basic information such as your name and contact information (if safe to do so), the time, date, and location/GPS coordinates (or write down on a piece of paper and film the paper). The more details you include, the easier it will be for someone else to research and verify the video later, even if they don't know you or where the video came from. Check out our tips on Basic Practices for Capturing, Storing, and Sharing for more.</p>	<p>သင့်ဗီဒီယိုတွင် အသေးစိတ်အချက်အလက်များပါဝင်စေခြင်းဖြင့် နောင်အခါ စုံစမ်းထောက်လှမ်းသူသို့မဟုတ် သတင်းထောက်မှ အချိန်နေရာစသဖြင့် ထုတ်ဖော်ဖို့လွယ်ကူနိုင်ရန် သိသာသော မြေပြင်အမှတ်အသား၊ လမ်းအမှတ်အသား၊ လိုင်စင်နံပါတ်ပြား၊ အလံ၊ တိုင်ကပ်နာရီ၊ သတင်းစာ၏ ပထမမျက်နှာ စသည့်အချက်အလက်များပါအောင် ရိုက်ကူးသင့်သည်။ သင့်ရဲ့နာမည်နှင့်ဆက်သွယ်ရန်အချက်အလက်များ(အန္တရာယ်ကင်းသည်ဆို) အချိန်၊ ရက်စွဲ၊ နေရာ၊ GPS နဲ့ကိုက်ညီပြောဆိုထည့်သွင်းခြင်း သို့မဟုတ် (စာရွက်ပေါ်တွင်ချရေး၍ စာရွက်ကို ထည့်သွင်းရိုက်ကူးခြင်း)ပြုပါ။</p>

	<p>အသေးစိတ်အချက်အလက်များများပါလေ နောက်ပိုင်းတွင် (သင့်ကိုမသိ ဗီဒီယိုဘယ်နေရာကလာမှန်းမသိသော်လည်း) သုတေသနလုပ်ပြီး အတည်ပြုရန် တစ်စုံတယောက်အတွက် လွယ်ကူလေဖြစ်သည်။</p> <p>“ရိုက်ကူးခြင်းထိန်းသိမ်းခြင်းမျှခြင်းအတွက်အခြေခံအလေ့အကျင့်များ” တွင် ကြည့်ပါ</p>
<p>Add description / metadata</p>	<p>Metadata/ဖော်ပြချက်များထည့်သွင်းရန်</p>
<p>Take advantage of one of the many specialized documentation apps that pull enhanced metadata or technical information from your phone, and allow you to manually input additional descriptive information. Keep in mind that, during a shutdown, you need an app that does not rely on internet access to record or store this metadata. Check out “Should I Use This Documentation App?” for more on how to choose an appropriate app.</p>	<p>မှတ်တမ်းတင်သော အထူးပြုထားသော app များထဲမှ တခု ရဲ့ အခွင့်ကောင်းယူအသုံးပြုခြင်းဖြင့် ပိုကောင်းမွန်သော metadata သို့မဟုတ် စက်ပိုင်းဆိုင်ရာသတင်းအချက်အလက်များကို ဖုန်းမှ ဆွဲထုတ်ခြင်းနှင့် အခြားသော အပိုဖော်ပြချက်အချက်အလက်များကို ထည့်သွင်းခွင့်ရရှိသည်။ သတိပြုရန်မှာ အင်တာနက်ပိတ်ထားချိန်တွင် အင်တာနက် သုံးစရာ မလိုသော app ဖြင့် မှတ်တမ်းတင်ရိုက်ကူးရန်နှင့် အချက်အလက်များအား ထိန်းသိမ်းရန်ဖြစ်သည်။ သင့်တော်သော app ကို ဘယ်လိုရွေးချယ်မလဲ ဆိုတာကို “ဒီမှတ်တမ်းတင် app ကိုအသုံးပြုသင့်ပါသလား” တွင်ကြည့်ပါ</p>
<p>[IMAGE] Some of the metadata captured using ProofMode.</p>	<p>ProofMode ကိုသုံး၍ အချို့သော metadata များကို ဖမ်းယူခြင်း</p>

<p>Even if you're not using a specialized documentation app, you can still create supplementary information in the form of notes, maps, or photos on your phone. You can organize your video with this additional information using your favorite file manager app. The key supplementary information to include is time, date, location of the recorded incident, as well as the source of the recording (i.e. your name and contact information) if safe to include. Export the metadata and include it with the video (you can put it all in a folder and zip it) when you share it.</p>	<p>အထူးပြုထားသောမှတ်တမ်းတင်appကို အသုံးမပြုသော်လည်း ဖြည့်စွက်အချက်အလက်များကို ဖန်တီးပြီး မှတ်ချက် မြေပုံ ဓာတ်ပုံများကို ဖုန်းတွင်ထည့်သွင်းနိုင်သည်။ အနှစ်သက်ဆုံး ဖိုင်မန်နေဂျာappကို သုံးကာ သင့်ဗီဒီယိုထဲရှိဖြည့်ပေါင်းအချက်အလက်များကို စုစည်းထိန်းသိမ်းနိုင်သည်။ အဓိကကျသော ဖြည့်စွက်အချက်အလက်မှာ အချိန် ရက်စွဲ ရိုက်ကူးထားသောဖြစ်ရပ်တည်ရှိရာနေရာနှင့်တကွ ရိုက်ကူးသည့် အရင်းအမြစ် (ရိုက်ကူးသူ၏နာမည်နဲ့ဆက်သွယ်ရန် အချက်အလက်များ) ထည့်သွင်းနိုင်သည်။ ထိုအချက်metadata များကို ဗီဒီယိုထဲထည့်သွင်းခြင်း (အားလုံးကိုfolderထဲထည့် zipped) လုပ်ပြီး ထုတ်ပို့ခြင်းဖြင့်မျှဝေနိုင်သည်။</p>
<p>[IMAGE] Video with additional descriptive documents.</p>	<p>အချက်အလက်ဖော်ညွှန်းမှုများပါသောမှတ်တမ်းများပါဝင်သောဗီဒီယို</p>
<p>Keep a backup</p>	<p>အရန်သိမ်းထားခြင်း back up</p>

Back up media from your phone regularly, ideally to 2 separate storage devices. You can, for example, connect On-the-Go (OTG) or wireless thumb drives to your phone, even without a computer. Check out our tips on [“Backing up phone media without internet or a computer”](#) for more details. Backing up will ensure you retain a copy of your video in case you lose or break your phone, or you need to delete videos from your phone. Having a secure copy of your original video also enables an investigator or journalist who sees your video through some other means to get the video directly from you later (as long as they are able to trace it back to you), creating a shorter and more complete chain of custody.

ဖုန်းထဲရှိမီဒီယာများကို backup အရန်သိမ်းခြင်းပုံမှန်လုပ်ပါ။ သီးသန့် storage နှစ်ခုခွဲထားပါ။ ဥပမာ - On-the-Go (OTG) သို့မဟုတ် wireless thumb drive ကိုဖုန်းနဲ့ချိတ်ဆက်ပြီး ကွန်ပျူတာမပါဘဲဆက်နိုင်သည်။
[“ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲ backup အရန်သိမ်းခြင်း”](#) တွင် အသေးစိတ်ကြည့်ပါ။ အရန်သိမ်းခြင်းဖြင့် ဖုန်းပျောက်သွား ပျက်သွားခဲ့သော် သင့်တွင်မီဒီယိုကော်ပီတခု လက်ကျန် ရှိနိုင်ကြောင်း သေချာစေလိမ့်မည်။ အော်ရီဂျင်နယ်မီဒီယို၏ စိတ်ချရသော ကော်ပီရှိခြင်းသည် သင့်မီဒီယိုကို တခြားနည်းလမ်းမှမြင်သော စုံစမ်းထောက်လှမ်းသူ သို့မဟုတ် သတင်းထောက်က နောက်ပိုင်းတွင် သင့်ထံမှ တိုက်ရိုက်လာယူရန် ထောက်ကူသည်။
 (သင့်ကိုနောက်ယောင်ခံလိုက်လာလို့ရတယ်ဆိုပါစို့)၊ တိုပြီးပြည့်စုံသောကွင်းဆက်ကို ဖန်တီးနိုင်လာမည်။

[IMAGE] Backup your media off your phone, such as with an OTG or wireless thumb drive.

OTG or wireless thumb drive ဖြင့် ဖုန်းထဲက ဖိုင်တွေကို backup အရန်သိမ်းဆည်းခြင်း

Check out the next post in this series, [“Backing Up Phone Media Without Internet or a Computer.”](#)

[“ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲ backup အရန်သိမ်းခြင်း”](#) ကို ဒီစီးရီးတွင်ကြည့်ပါ။

--	--

<p>Backing Up Phone Media Without Internet or a Computer</p> <p>Documenting During Internet Shutdowns series</p> <p>By Yvonne Ng With contributions by Arul Prakkash</p> <p><i>This post is part of a series on Documenting During Internet Shutdowns.</i></p> <p>Last reviewed: 31 January 2020</p>	<p>ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲ backup အရန်သိမ်းခြင်း</p> <p>အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း</p> <p>ရေးသားသူ - Yvonne Ng ပံ့ပိုးသူ - Arul Prakkash</p> <p>ဒီပို့စ်သည် “အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း” စီးရီး၏ တပိုင်းဖြစ်သည်။</p> <p>နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်</p>
<p>Backup is key to ensuring your data and documentation are not accidentally deleted, corrupted, or lost if your device is confiscated. During an internet shutdown or slowdown, you might not be able to run your regular cloud backup or send your documentation to a safe offsite location. Offloading to a desktop</p>	<p>အရန်သိမ်းဆည်းခြင်းသည် အချက်အလက်တွေ မှတ်တမ်းတွေကို အခန့်မသင့်ဖျက်မိတာ ဖျက်ဆီးမိတာ သင့်ဖုန်းသိမ်းဆည်းခံရတဲ့အခါ ပျောက်တာတွေ မဖြစ်အောင် သေချာစေတဲ့နည်းပါ။</p>

<p>or laptop computer is one way to back up, but since people often do not have access to one, here are some options and tips for backing up your media from your phone during an internet shutdown without a computer.</p>	<p>အင်တာနက်ပိတ်သွားတဲ့အချိန်၊ နှေးသွားတဲ့အချိန်မှာ နောက်ခံသိမ်းဆည်းတဲ့ အလုပ်ကို ပုံမှန်မလုပ်နိုင်တာတို့ သင့်မှတ်တမ်းကို လုံခြုံတဲ့နေရာကို မပို့နိုင်တာတို့ ဖြစ်နိုင်ပါသည်။ ဒက်စတော့ သို့မဟုတ် လက်တွေ့ ကွန်ပျူတာထဲ ထည့်ချလိုက်တာလည်း တနည်းအားဖြင့် အရန်သိမ်းနည်း တမျိုးဖြစ်သည် သို့သော်လူတိုင်းမှာတော့ ရှိမှာမဟုတ်လို့ အောက်ပါရွေးချယ်ခွင့်လမ်းများနဲ့ အသုံးဝင်သော အချက်များသည် ဖုန်းထဲမှာရှိတဲ့ ဖိုင်တွေကို အင်တာနက်ပိတ်သွားတဲ့အချိန် ကွန်ပျူတာမရှိတဲ့အချိန်မှာ အရန်ခံသိမ်းနည်းတခုပဲ ဖြစ်ပါသည်။</p>
<p>Use an OTG or wireless drive</p>	<p>OTG or wireless thumb drive အသုံးပြုခြင်း</p>
<p>OTG, or on-the-go, drives are a type of USB drive compatible with many (but not all) Androids. You can plug an OTG thumb drive directly into your phone, or use a OTG-to-USB adapter to connect your phone with a regular USB hard drive. With OTG, your phone provides the power for the drive.</p> <p>Popular brands of OTG drives include SanDisk, Kingston, and Samsung, although there are many others. They typically cost between US\$8-\$25 depending on the storage capacity.</p>	<p>OTG or wireless thumb drive များသည် USB drive ဖြစ်ပြီး Android (အားလုံးမဟုတ်သော်လည်း) တော်တော်များများနဲ့ compatible ဖြစ်သည် OTG thumb drive ကိုဖုန်းနဲ့တိုက်ရိုက်ပလပ်ထိုးပြီးဖြစ်စေ OTG-to-USB adapter သုံးပြီးဖြစ်စေ OTG နဲ့ ဆက်ခြင်းဖြင့် drive ကို ဖုန်းကနေ အားသွင်းနိုင်သည်။ ရေပန်းစားသော OTG driveများမှာ Sandisk, Kingston, Samsung တို့ဖြစ်ပြီး အခြားအမျိုးပေါင်းများစွာလည်းရှိသည်။ သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး တခုကို \$ 8-25 ကုန်ကျနိုင်သည်။</p>

<p>[IMAGE] Use an OTG drive to back up media from a phone.</p>	<p>ဖုန်းထဲကမီဒီယာဖိုင်တွေ (backup) အရန်သိမ်းဆည်းဖို့ OTG drive သုံးပြုခြင်း</p>
<p>Wireless thumb drives / hard drives are similar to regular hard drives except that they do not require cables. This allows you to connect devices that don't normally connect to hard drives, such as your phone. An advantage of a wireless drive over an OTG drive is that you can connect multiple users to the same wireless drive at once. This can be useful, for example, in a protest situation when you are filming as a team — everyone's footage can be backed up to a hard drive that another team member is carrying. Note that because they are not drawing power from a device, wireless drives rely on battery power and need to be charged.</p> <p>SanDisk is probably the most popular brand of wireless thumb drives, although there are others. Wireless thumb drives are generally more expensive than OTG drives, and range from about US\$25-\$100 depending on the storage capacity. Larger wireless external hard drives start at around US\$150 depending on the storage capacity.</p>	<p>ကြိုးမဲ့ thumb drive / hard drives တွေဟာ ကြိုးမလိုတာကလွဲရင် အခြားပုံမှန် hard drive တွေနဲ့ အတူတူဖြစ်သည်။ ဖုန်းကဲ့သို့ Hard drive နဲ့ ပုံမှန်အားဖြင့် ဆက်လို့မရတဲ့ ဖုန်း(device) တွေကို ဆက်သွယ်လို့ရအောင် ခွင့်ပြုမှာဖြစ်သည်။ ကြိုးမဲ့ drive မှာ OTG drive ထက် အားသာချက်ကတော့ သုံးစွဲသူများစွာကို wireless drive တခုတည်းကနေ တပြိုင်နက်တည်း ဆက်နိုင်တာဖြစ်သည်။ ဘယ်အချိန်မှာအသုံးဝင်လဲဆိုရင် ဆန္ဒပြမှုများဖြစ်နေချိန်မှာ အဖွဲ့လိုက်ရိုက်ကူးမှတ်တမ်းတင်တဲ့အခါမှာ တယောက်ချင်းစီရဲ့မီဒီယာဖိုင်တွေကို တခြားတယောက်သယ်ဆောင်ထားတဲ့ hard drive ထဲမှာ backup အရန်သိမ်းဆည်းလို့ရနိုင်သည်။ ဖုန်းdevice ကနေ ပါဝါကိုမဆွဲတဲ့အတွက်ကြောင့် ကြိုးမဲ့ drive တွေက ဘတ်ထရီကို သုံးပြီး အားပြန်သွင်းဖို့လိုအပ်တယ်ဆိုတာ မှတ်ထားရမည်ဖြစ်သည်။ တခြားအမျိုးအစားတွေ အများကြီးရှိသော်လည်း SanDisk ကတော့ လူကြိုက်အများဆုံး ကြိုးမဲ့ thumb drive ဖြစ်သည်။ ကြိုးမဲ့ thumb drives တွေက OTG drives တွေထက် ဈေးပိုများပါတယ်။ သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး \$ 25-100 ကုန်ကျနိုင်သည်။ ပိုပြီးကြီးတဲ့ အပြင်ပ hard drive တွေကတော့ သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး \$ 150 လောက်ကုန်ကျနိုင်ပါသည်။</p>
<p>[IMAGE] Use a wireless thumb drive to back up media from a</p>	<p>ကြိုးမဲ့ thumb drive ကိုသုံးပြီး ဖုန်းdeviceထဲက မီဒီယာဖိုင်များကို backup အရန်သိမ်းဆည်းခြင်း</p>

phone	
<p>Alternative: Use an old unused phone</p>	<p>အပြောင်းအလဲ- မသုံးတော့သောဖုန်းအဟောင်းများကိုသုံးခြင်း</p>
<p>If you don't have an OTG or wireless drive, but you have an old phone that still works that you no longer use, you can also re-purpose it for backup. As long as both phones are in physical range, you can connect and copy media from one to the other using Bluetooth, WiFi Direct, or Near Field Communication (NFC) / Android Beam. Bluetooth and Wifi Direct are both wireless technologies that can "pair" two devices without another router or access point in between. WiFi Direct provides a wider range and faster data transfer than Bluetooth, but uses up a lot more power. Meanwhile, NFC has a much shorter range (~4cm) and much slower transfer speeds than either Bluetooth or WiFi Direct, but connects faster and uses less power, so can be useful for quick small transfers when you have both devices in hand.</p>	<p>OTG သို့မဟုတ် wireless drive မရှိဘူးဆိုရင် မသုံးတော့တဲ့ ဖုန်းအဟောင်းတွေကိုလည်း backup အရန်သိမ်းဆည်းဖို့အတွက် ရည်ရွယ်ချက်ပြောင်းသုံးနိုင်ပါသည်။ ဖုန်းနှစ်ခုနီးကပ်သောအကွာအဝေးရှိရင် Bluetooth, Wifi Direct သို့မဟုတ် NFCအနီးကပ်ဆက်သွယ်မှုစနစ်၊ အင်ဒရိုက်ဘီနီးဆက်သွယ်မှုစနစ်Android Beam ဆက်သွယ်ပြီး မီဒီယာတွေကို ကော်ပီလုပ်လို့ရပါသည်။</p> <p>Bluetooth or Wifi Direct တွေက ကြိုးမဲ့စနစ်ဖြစ်ပြီး ကွန်ယက်ဖြန့်ခွဲမှု သို့မဟုတ် ဆက်သွယ်မှုစုံရပ် မရှိဘဲ စက်နှစ်ခုကို "စုံတွဲဆက်သွယ်"နိုင်ပါသည်။</p> <p>Wifi Direct ကတော့ Bluetooth ထက်စာရင် ဝေးဝေးရောက်ပြီး ဒေတာတွေကို မြန်မြန်ပြောင်းရွှေ့နိုင်စွမ်းရှိပေမယ့် ပါဝါသုံးတာ အရမ်းများပါသည်။ တချိန်တည်းမှာ NFC အနီးကပ်ဆက်သွယ်မှု (~ ၄ စင်တီမီတာ) နှင့် ပိုပြီးနီးနီးအကွာအဝေးမှုရှိပြီး ပြောင်းရွှေ့ချိန်လည်းပိုနှေးကွေးပါသည်။</p> <p>သို့သော် သူက ဆက်သွယ်မှုပိုမြန်ပြီး ပါဝါသုံးတာပိုနည်းတာမို့ ခပ်မြန်မြန်နဲ့ နည်းနည်းပဲ ပြောင်းရွှေ့သည်။ စက်နှစ်ခုလုံးလက်ထဲမှာရှိမယ်ဆို အသုံးဝင်။</p>

<p>[IMAGE] Send files via NFC, Bluetooth or Wifi Direct</p>	<p>အနီးကပ်ဆက်သွယ်မှုစနစ် NFC, Bluetooth ကြိုးမဲ့အနီးကပ်ဆက်သွယ် Wifi Direct မှတစ်ဆင့် ဖိုင်ပို့ခြင်း</p>
<p>Your phone probably has built-in Bluetooth, WiFi Direct, or NFC apps / features that allow you to choose nearby devices to share with. If both phones have Files By Google installed, you can also share files offline using these technologies within the app.</p>	<p>သင့်ရဲ့ဖုန်းမှာ တပါတည်းဖြစ်သော Bluetooth, NFC ကြိုးမဲ့အနီးကပ် ဆက်သွယ်စနစ်၊ Wifi Direct or NFC app နဲ့ feature အင်္ဂါရပ်များက အနီးမှာရှိတဲ့စက်တွေကို မျှဝေရာမှာ ရွေးချယ်ဖို့ ခွင့်ပြုပါလိမ့်မယ် ဖုန်းနှစ်ခုလုံးမှာ ဖိုင်တွေက Files By Google Installed နဲ့ သိမ်းထားတာဆိုရင် ဖိုင်တွေကို ဒီနည်းပညာတွေသုံးပြီး app အချင်းချင်း အော်ဖ်လိုင်းနဲ့ မျှဝေနိုင်ပါသည်။</p>
<p>[IMAGE] Send files offline over Files by Google.</p>	<p>Files by Google ကနေ အော်ဖ်လိုင်းနဲ့ ဖိုင်များပို့ခြင်း</p>
<p>Important: the downside to the ease of connection provided by these services is that they are not secure. Bluetooth and wifi beacons/scanners can be used to trace your location or probe your device for information. Infiltrators may try to pair with your device, send you unwanted files, or even gain control of your device if it is vulnerable. To be safer, turn these services off when you are not using them and only turn them on when you're in safe locales, limit app permissions to only what/who you need, and practice good phone security like running updates and having a strong passcode.</p>	<p>အရေးကြီးမှတ်ချက်။ ဒီဝန်ဆောင်မှုတွေကတော့ ဆက်သွယ်ဖို့လွယ်ကူပြီး အားနည်းချက်ကတော့ လုံခြုံမှုမရှိပါ။ Bluetooth and wifi များသည် တည်နေရာဒေသကို ခြေရာခံခြင်း သင့်ဖုန်းdeviceအချက်အလက်တွေကို စုံစမ်းစစ်ဆေးလိုရနိုင်ပါသည်။ ကြားဖြတ်ဖောက်ထွင်းသူများကလည်း သင့်ဖုန်းdevice ကို စုံတွဲဆက်သွယ်ဖို့ ကြိုးပမ်းတာမျိုး မလိုချင်တဲ့ဖိုင်တွေကို ပို့လိုက်တာမျိုး သို့မဟုတ် ထိခိုက်လွယ်တဲ့အခြေအနေမှာသင့်ဖုန်းdeviceကို ထိန်းချုပ်တာမျိုးတွေ လုပ်နိုင်ပါသည်။ ပိုပြီးလုံခြုံမှုရှိဖို့ဆိုရင် စက်တွေကို မသုံးတဲ့အချိန်မှာ ဝန်ဆောင်မှုတွေအားလုံးကိုပိတ်ထားပြီး လုံခြုံသောနေရာမှ ပြန်ဖွင့်တာမျိုး app တွေကို လိုအပ်တာဘဲ ဘာလဲ/ဘယ်သူလဲခွင့်ပြုချက်</p>

	<p>ကန့်သတ်ထားတာမျိုး ဖုန်းလုံခြုံရေးစနစ်ကိုလေ့ကျင့်ပြီး update အမြဲလုပ်နေတာမျိုး ခိုင်မာသောလျှို့ဝှက်နံပါတ် passcode ထားတာမျိုးလုပ်ရမှာဖြစ်သည်။</p>
<p>Include any separate description / metadata</p>	<p>သီးသန့်ဖော်ပြခြင်း/metadata များပါဝင်စေခြင်း</p>
<p>When copying media to an OTG drive, wireless drive, or an old phone, it is useful to include any descriptive information or metadata that may be separate from the media. Many documentation apps, for example, generate CSV or JSON text documents that include metadata pulled from the device (e.g. geolocation, time, date) and any description manually inputted by the user. Make sure to export and include these metadata documents in your backups too.</p>	<p>OTG drive ဆီကို ကြိုးမဲ့drive သို့မဟုတ် ဖုန်းအဟောင်းတွေကနေ မီဒီယာတွေကော်ပီလုပ်တဲ့အခါ ဖော်ပြသောအချက်အလက်များ ပါဝင်စေခြင်း သို့မဟုတ် metadata ကို မီဒီယာနဲ့ သီးသန့်ခွဲထားခြင်းသည် အသုံးဝင်သည်။ မှတ်တမ်းတင်သော app အများစုသည် CSV သို့မဟုတ် JSON မှတ်တမ်းများကို ထုတ်လုပ်ပြီး စက်မှာရှိသော metadata (ဥပမာ ပထဝီအရပ်ဒေသ အချိန် ရက်စွဲ) များကိုရော သုံးစွဲသူက လက်နဲ့ထည့်ထားသော ဖော်ပြချက်မှန်သမျှကိုပါ ဆွဲထုတ်လေ့ရှိသည်။ ပြင်ပသို့ထုတ်ပို့ခြင်းလုပ်သည့်အခါ အထက်ပါ metadata များကိုပါ ပါဝင်အောင် မှတ်တမ်းတင်ပြီး အရန်သိမ်းဆည်း backup ထားသင့်သည်။</p>
<p>[IMAGE] Additional metadata files generated using ProofMode app.</p>	<p>ProofMode app ကိုသုံး၍ အပို metadata ဖိုင်များကိုထုတ်လုပ်ခြင်း</p>
<p>Password protect the drive</p>	<p>Drive ကို ကာကွယ်သော လျှို့ဝှက်နံပါတ်</p>

<p>Many wireless drives can be password-protected with a mobile app that comes with the drive. Note that password-protection is not the same as encryption (see below). Most wireless or OTG drives do not enable full-disk encryption using only a mobile phone, although they may be full-disk encrypted using a computer.</p>	<p>ကြိုးမဲ့ drive အများစုသည် မိုဘိုင်း app လျှို့ဝှက်နံပါတ်နဲ့ ကာကွယ်နိုင်သည်။ လျှို့ဝှက်နံပါတ်ဖြင့် ကာကွယ်ခြင်းသည် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption နဲ့ မတူသည်ကို သတိပြုပါ။ ကြိုးမဲ့သို့မဟုတ် OTG drive များသည် ကွန်ပျူတာ ဓာတ်ပြားအပြည့် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ဆောင်နိုင်သော်လည်း မိုဘိုင်းဖုန်းသုံးရုံဖြင့် မလုပ်ဆောင်နိုင်ပါ။</p>
<p>[IMAGE] Password-protect your drives.</p>	<p>သင့်ရဲ့ drive အား လျှို့ဝှက်စနစ် ကာကွယ်ခြင်း</p>
<p>Consider encrypting the files</p>	<p>ဖိုင်များကို လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ရန် စဉ်းစားပါ</p>
<p>If you need to store your files more securely, you might consider encrypting your backups. While you may not be able to encrypt most wireless or OTG drives with a mobile phone, you can encrypt the files themselves before you move them onto the drive. Some apps that can encrypt files on Android include ZArchiver, and RAR. Be aware that you must remember your encryption passwords. There is no way to recover encrypted files if you lose the password.</p>	<p>သင့်ရဲ့ဖိုင်များကို ပိုမိုလုံခြုံစိတ်ချစွာ စုဆောင်းထားချင်လျှင် အရန်သိမ်းဆည်းခြင်း backup များကို လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ရန် စဉ်းစားပါ။ ကြိုးမဲ့စနစ် သို့မဟုတ် OTG drives ပါသော မိုဘိုင်းဖုန်းအများစုကို encryption လျှို့ဝှက်ထိန်းသိမ်း၍ မရနိုင်သော်လည်း ဖိုင်များကိုယ်တိုင်ကို အခြား drive ထဲကို မရွေ့မီတွင် encrypt လျှို့ဝှက်ထိန်းသိမ်းထားနိုင်သည်။ ZArchiver and RAR ကဲ့သို့ app များသည် Android ပေါ်တွင် ဖိုင်များကို encrypt လျှို့ဝှက်ထိန်းသိမ်းထားနိုင်သည်။ ကိုယ့်ရဲ့ encryption လျှို့ဝှက်နံပါတ်ကို သတိရနေဖို့အတွက် သတိထားပါ။ အကယ်၍ လျှို့ဝှက်နံပါတ် password ပျောက်သွားလျှင် encrypted လျှို့ဝှက်ထိန်းသိမ်းထားသော ဖိုင်များအား ပြန်လည်ဖော်ယူရန်</p>

	နည်းလမ်းမရှိတော့ပါ။
[IMAGE] Zipping and encrypting files using ZArchiver on a phone before moving to backup.	အရန်သိမ်းဆည်းခြင်းမပြုမီ ZArchiver ကိုသုံး၍ ဇစ်ဖိုင် လျှို့ဝှက်ထိန်းသိမ်းဖိုင်များပြုလုပ်ခြင်း
Keep in mind that some countries may have laws that restrict or criminalize the use of encryption. Using them to prevent authorities to accessing your data may be seen as destroying evidence or obstructing an investigation, and may be punishable as a crime. This 2017 map may be outdated but provides a good starting place if you have questions about the laws in your country.	သတိပြုရန်မှာ အချို့နိုင်ငံများမှာ encryption လျှို့ဝှက်ထိန်းသိမ်းခြင်းကို ဥပဒေအရတားမြစ်တာ သို့မဟုတ် ရာဇဝတ်မှုပြုတာမျိုးတွေရှိတတ်ပါသည်။ အာဏာပိုင်တွေကသင့်ရဲ့အချက်အလက်တွေကို ရှာဖွေလို့မရအောင် ကာကွယ်ဖို့သုံးတာဖြစ်ပေမယ့် သက်သေကိုဖျက်ဆီးမှု စုံစမ်းစစ်ဆေးခြင်းကို ပိတ်ဆို့မှု စတဲ့ပြစ်မှုများဟာ ရာဇဝတ်မှုအဖြစ် အပြစ်ပေးခံရနိုင်ပါသည်။ ဒီမြေပုံက (2017 map) ရက်လွန်နေပြီ ဖြစ်သော်လည်း သင့်နိုင်ငံရဲ့ ဥပဒေနဲ့ပတ်သက်ပြီးမေးစရာရှိရင်နေရာတို့ရဲ့အစအနေနဲ့ ပံ့ပိုးမှာဖြစ်ပါသည်။
Make 2 backups in separate locations.	သီးခြားနေရာများတွင် အရန် ၂ခု ပြုလုပ်သိမ်းဆည်းခြင်း
A single backup is not always reliable. For example, you might lose the backup device, damage it, or it might just randomly fail. IT experts usually advise people to have 2 backups (i.e. 3 copies total), on separate devices kept in separate locations. This helps mitigate the variety of risks to any one particular	တခုတည်း အရန်သိမ်းဆည်းတာက ယုံကြည်စိတ်ချစရာမဖြစ်ပါ။ ဥပမာ အရန်သိမ်းထားတဲ့ device ပျောက်တယ် ပျက်တယ် သို့မဟုတ် တခုခု ရှုံးနိမ့်တာမျိုး ဖြစ်နိုင်တယ်။ အိုင်တီကျွမ်းကျင်သူတွေ အကြံပေးတာက သိမ်းတဲ့အခါနှစ်ခု နှစ်နေရာသိမ်းတာဆိုရင် (သုံးစုံဖြစ်သွားပြီ)

<p>copy.</p>	<p>နောက်စက်တခုထဲထည့်ပြီး သီးသန့်တနေရာမှာထားရင် ဘယ်တခုပဲ ပျောက်ပျောက် ဖြစ်နိုင်ချေရှိသော အန္တရာယ်များကို ကာကွယ်ပြီးဖြစ်လိမ့်မည်။</p>
<p>[IMAGE] The 3-2-1 file backup principle.</p>	<p>3-2-1 backup အရန်သိမ်းခြင်း အခြေခံမူ</p>
<p>Check out the final post in this series, “File Sharing and Communication During an Internet Shutdown.”</p>	<p>ဒီစီးရီးရဲ့ နောက်ဆုံးပိုစ်စ်ဖြစ်တဲ့ “အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဖိုင်ဝေမျှခြင်းနှင့် ဆက်သွယ်ခြင်း” ကိုကြည့်ပါ။</p>

File Sharing and Communication During an Internet Shutdown

Documenting During Internet Shutdowns series

By [Yvonne Ng](#)

With contributions by [Arul Prakkash](#)

This post is part of a series on [Documenting During Internet Shutdowns](#).

Last reviewed: 31 January 2020

The ongoing internet shutdown and crackdown in Kashmir, the longest internet shutdown ever imposed in a democracy, has had a [catastrophic impact](#) on the lives of people in the region. Adding insult to injury, in December 2019, Kashmiris' [WhatsApp accounts started being revoked](#) due to users' 120 days of inactivity as per WhatsApp policies.

အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဖိုင်ဝေမျှခြင်းနှင့် ဆက်သွယ်ခြင်း

အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

ရေးသားသူ - [Yvonne Ng](#)

ပံ့ပိုးသူ - [Arul Prakkash](#)

ဒီပို့စ်သည် “[အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း](#)” စီးရီး၏ အပိုင်းဖြစ်သည်။

နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်

ကက်ရှုမီးယားဒေသမှာ ဆက်လက်ဖြစ်ပွားနေဆဲဖြစ်တဲ့ အင်တာနက် ဖြတ်တောက်ခြင်းနှင့် ဖြိုခွဲနှိမ်နင်းခြင်းသည် ဒီမိုကရေစီစနစ်တွင်းတွင် အကြာရှည်ဆုံးသော အင်တာနက်ဖြတ်တောက်မှုဖြစ်ပြီး ဒေသတွင်းရှိ ပြည်သူများ၏အသက်ကို [ပြင်းထန်ထိခိုက်သောသက်ရောက်မှု](#) ဖြစ်စေခဲ့သည်။ ထိခိုက်ဒဏ်ရာပေါ်တွင် ရိုင်းပြောစာကားခြင်းဆင့်၍ ဒီဇင်ဘာ ၂၀၁၉တွင် WhatsApp၏ ရက် ၁၂၀ သုံးစွဲသူ မူဝါဒအရ ကက်ရှုမီးယား၏ [WhatsApp အကောင့်များသည် စတင်၍](#)

	<p>ပိတ်သိမ်းခြင်းခံခဲ့ရသည်။</p>
<p>At the time of this writing in January 2020, the Indian Supreme Court ruled that the indefinite shutdown in Kashmir is illegal and an abuse of power. Limited broadband and mobile internet has been restored in some areas, but only to select “whitelisted” websites.</p>	<p>ယခုစာရေးသားသောအချိန် ဇန်နဝါရီ ၂၀၂၀ တွင် ကက်ရှုမီးယားဒေသ၏ အကန့်အသတ်မဲ့ အင်တာနက်ဖြတ်တောက်ခြင်းသည် တရားမဝင်သော အာဏာအလွဲသုံးစားမှု ဖြစ်သည်ဟု အိန္ဒိယနိုင်ငံ၏ နိုင်ငံတော်တရားရုံးချုပ် တရားဝင်ဆုံးဖြတ်ခဲ့သည်။ ကန့်သတ်ထားသော မြန်နှုန်းမြင့်အင်တာနက် ဘရော့ဘင်နှင့် မိုဘိုင်းအင်တာနက်ကို အချို့နေရာများတွင် ပြန်လည်ရရှိသော်လည်း ခွင့်ပြုသောစာရင်း သန့်ရှင်းသောစာရင်း ဝက်ဘ်ဆိုက်များကိုသာ ရွေးချယ်ခွင့်ရှိသည်။</p>
<p>Internet shutdowns are designed to block people from sharing information and communicating (and also push people into less secure forms of communication such as mobile phone and SMS, which are easier for authorities to intercept and monitor). There are not always good workarounds during complete shutdowns. During the strictest periods of the shutdown in Kashmir, for example, people resorted to using handwritten notes and couriers to get messages to their loved ones.</p> <p>We don't have sure-fire ways to circumvent all blockages, but through conversations with activists and peers, we have learned some methods and approaches for offline sharing and communication that may work for you, depending on the circumstances. Note that some of these options require internet to initially set up (e.g. to download apps, etc).</p>	<p>အင်တာနက်ဖြတ်တောက်ခြင်းများသည် လူအများအား သတင်းအချက်အလက်မျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းအား ပိတ်ဆို့ထားဆီးရန် ဒီဇိုင်းလုပ်ထားပြီး (လူများအား မိုဘိုင်းဖုန်းနှင့် SMS အချက်ပို့ခြင်း စသဖြင့် လုံခြုံမှုနည်းသော ဆက်သွယ်ရေးပုံစံစနစ်များကိုသာ သုံးရန် တွန်းပို့ခြင်းဖြင့် အာဏာပိုင်များအနေဖြင့် ကြားဖြတ်နားထောင်ခြင်း လေ့လာစောင့်ကြည့်ခြင်းများကို လွယ်ကူစေသည်) ။</p> <p>ကက်ရှုမီးယားဒေသ၏ အတင်းကြပ်ဆုံးအင်တာနက်ဖြတ်တောက်ချိန်များ အတွင်းတွင် လူများစုသည် လက်ရေးစာများသုံးခြင်း စာပို့စာယူစနစ်များ သုံးခြင်းကိုသာ ယင်းတို့၏ချစ်ခင်သူများနှင့် သတင်းစကားပါးရန် အခြားရွေးချယ်စရာမရှိ၍ ရွေးချယ်စရာအဖြစ်သတ်မှတ်ခဲ့ရသည်။</p> <p>ပိတ်ဆို့ထားဆီးခြင်းအားလုံးကိုရှောင်တိမ်းနိုင်ရန် သေချာပေါက်နည်းလမ်း မရှိသေးသော်လည်း တက်ကြွလှုပ်ရှားသူနှင့် မိတ်ဆွေတို့၏ စကားလက်ဆုံ</p>

	<p>များမှတစ်ဆင့် ကျွန်ုပ်တို့လေ့လာခဲ့သည်မှာ အချို့သော နည်းလမ်းများနှင့် ချဉ်းကပ်နည်းများသည် အော်ဖ်လိုင်းမျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းများ အခြေအနေပေါ်မူတည်ပြီး သင့်အတွက် အလုပ်ဖြစ်နိုင်မည်။</p> <p>မှတ်ချက်ပြုရန်မှာ အချို့ရွေးချယ်နိုင်သောလမ်းများသည် စတင်ပြင်ဆင် setup လုပ်ရန်အတွက် အင်တာနက်လိုအပ်သည်။</p> <p>(app ဒေါင်းလုပ်လုပ်ခြင်း စသဖြင့်)</p>
<p>Share files directly with Bluetooth, Wifi Direct, or NFC</p>	<p>အနီးကပ်ဆက်သွယ်မှုစနစ် NFC, Bluetooth ကြိုးမဲ့အနီးကပ်ဆက်သွယ် Wifi Direct မှတစ်ဆင့် ဖိုင်မျှဝေခြင်း</p>
<p>You don't need to have an internet connection to connect your phone with another nearby device via Bluetooth, Wifi Direct, or Near Field Communication (NFC) (sometimes called Android Beam on older devices). Bluetooth and Wifi Direct are both wireless technologies that can "pair" two devices without another router or access point in between. WiFi Direct provides a wider range and faster data transfer than Bluetooth, but uses up a lot more power. Meanwhile, NFC has a much shorter range (~4cm) and much slower transfer speeds than either Bluetooth or WiFi Direct, but connects faster and uses less power, so can be useful for small transfers when have both devices in your hands.</p>	<p>သင်ဖုန်းနဲ့ နီးရာတွင်ရှိသော ဖုန်းသို့မဟုတ် device တစ်ခုကိုဆက်သွယ်ရန် အင်တာနက်ဆက်သွယ်မှုမရှိရန် မလိုအပ်ပါ။ Bluetooth, Wifi Direct, Near Field Communication NFC/နီးစပ်ရာကွင်းပြင်ဆက်သွယ်စနစ် အင်တာနက်မလိုအပ်ပါ။ (တခါတရံ အင်ဒရိုက်ဘ်နန်းဟုလည်းခေါ်သည်)။</p> <p>Bluetooth နှင့် Wifi Direct နှစ်ခုစလုံးသည် ကြိုးမဲ့ဆက်သွယ်နည်းပညာ ဖြစ်ပြီး ဖုန်းသို့မဟုတ် device နှစ်ခုကို ချိတ်ဆက်ပွိုင့် သို့မဟုတ် ကွန်ယက်ဖြန့်ချိစက် မရှိဘဲ “စုံတွဲဆက်သွယ်” နိုင်ပါသည်။ Wifi Direct က ပိုမိုကျယ်ဝန်းသော အကွာအဝေးကို Bluetooth ထက်ပို၍ လျင်မြန်သော ဒေတာလွှဲပြောင်းမှု ပံ့ပိုး နိုင်ပါသည်။</p>

	<p>သို့သော်ပါဝါကိုအလွန်တရာပိုသုံးသည်။ တချိန်တည်းမှာ NFC သည် ပိုမိုတိုတောင်းသော အကွာအဝေးကို Bluetooth or Wifi Direct ထက်နှေးသော လွှဲပြောင်းနှုန်းဖြင့် သို့သော် ပိုမိုမြန်ဆန်စွာချိတ်ဆက်ပြီး ပါဝါသုံးနှုန်းနည်းသည်။ ထို့ကြောင့် ပမဏာနည်း လွှဲပြောင်းခြင်းဖြစ်မယ် စက်နှစ်ခုလုံးလက်ထဲရှိမယ်ဆို အသုံးဝင်သည်။</p> <p>Wifi Direct ကတော့ ဘလူးတုထက်စာရင် ဝေးဝေးရောက်ပြီး ဒေတာတွေကို မြန်မြန်ပြောင်းရွှေ့နိုင်စွမ်းရှိပေမယ့် ပါဝါသုံးတာ အရမ်းများပါသည် တချိန်တည်းမှာ NFC အနီးကပ်ဆက်သွယ်မှု လေးစင်တီမီတာ ပိုပြီးနီးနီးအကွာအဝေးနဲ့ ပြောင်းရွှေ့ချိန်လည်းပိုနှေးကွေးပါသည် သို့သော် သူက ဆက်သွယ်မှုပိုမြန်ပြီး ပါဝါသုံးတာပိုနည်းတာမို့ ခပ်မြန်မြန်နဲ့ နည်းနည်းပဲ ပြောင်းရွှေ့မယ် စက်နှစ်ခုလုံးလက်ထဲမှာရှိမယ်ဆို အသုံးဝင်ပါတယ်</p>
<p>[IMAGE] Built-in Bluetooth, WiFi Direct and Android Beam features.</p>	
<p>You likely have Bluetooth, WiFi Direct, and NFC features built into your phone that show up in your sharing options. In addition, apps with file sharing features, like Files By Google,</p>	<p>သင့်ရဲ့ဖုန်းမှာBluetooth, Wifi Direct or NFC features အင်္ဂါရပ်များက</p>

<p>also integrate these technologies.</p>	<p>တပါတည်းပါလာပြီး မျှဝေဖို့နည်းလမ်းများကိုလည်း ပြသထားနိုင်ချေရှိပါသည်။ ဒါ့အပြင် ဖိုင်းတွေကိုမျှဝေတဲ့ အင်္ဂါရပ်မျိုးဖြစ်တဲ့ Files by Google app ကဲ့သို့နည်းပညာများလည်း ပေါင်းစပ်ထားမှာပါ။</p>
<p>[IMAGE] Offline sharing in Files by Google.</p>	
<p>Important: the downside to the ease of connection provided by these services is that they are not secure. Bluetooth and wifi beacons/scanners can be used to trace your location or probe your device for information. Infiltrators may try to pair with your device, send you unwanted files, or even gain control of your device if it is vulnerable. To be safer, turn these services off when you are not using them and only turn them on when you're in safe locales, limit app permissions to only what/who you need, and practice good phone security like running updates and having a strong passcode.</p>	<p>အရေးကြီးမှတ်ချက်။ ဒီဝန်ဆောင်မှုတွေကတော့ ဆက်သွယ်ဖို့လွယ်ကူပြီး အားနည်းချက်ကတော့ လုံခြုံမှုမရှိပါ။ Bluetooth and wifi များသည် တည်နေရာဒေသကို ခြေရာခံခြင်း သင့်ဖုန်းdeviceအချက်အလက်တွေကို စုံစမ်းစစ်ဆေးလို့ရနိုင်ပါသည်။ ကြားဖြတ်ဖောက်ထွင်းသူများကလည်း သင့်ဖုန်းdevice ကို စုံတွဲဆက်သွယ်ဖို့ ကြိုးပမ်းတာမျိုး မလိုချင်တဲ့ဖိုင်တွေကို ပို့လိုက်တာမျိုး သို့မဟုတ် ထိခိုက်လွယ်တဲ့အခြေအနေမှာ သင့်ဖုန်းdeviceကို ထိန်းချုပ်တာမျိုးတွေ လုပ်နိုင်ပါသည်။ ပိုပြီးလုံခြုံမှုရှိဖို့ဆိုရင် စက်တွေကို မသုံးတဲ့အချိန်မှာ ဝန်ဆောင်မှုတွေအားလုံးကိုပိတ်ထားပြီး လုံခြုံသောနေရာမှ ပြန်ဖွင့်တာမျိုး app တွေကို လိုအပ်တာဘဲ ဘာလဲ/ဘယ်သူလဲခွင့်ပြုချက် ကန့်သတ်ထားတာမျိုး ဖုန်းလုံခြုံရေးစနစ် ကိုလေ့ကျင့်ပြီး update အမြဲလုပ်နေတာမျိုး ခိုင်မာသောလျှို့ဝှက်နံပါတ် passcode ထားတာမျိုးလုပ်ရမှာဖြစ်သည်။</p>

<p>Share files with a wireless drive or via a Wireless Local Area Network (WLAN)</p>	<p>ကြိုးမဲ့စနစ်ဖြင့်ဖိုင်များကိုမျှဝေခြင်း ကြိုးမဲ့ဆက်သွယ်မှုဧရိယာကွန်ယက်</p>
<p>A wireless hard drive or flash drive can be used to share files among a team, or multiple people at one time. The wifi drive will typically come with instructions and/or an app for connecting your phone to the drive, and is relatively easy to use. Remember to set a password on the drive for security.</p>	<p>ကြိုးမဲ့hard drive သို့မဟုတ် flash drive များကို အဖွဲ့တွင်း သို့မဟုတ် လူများစုကို တပြိုင်နက်တည်း ဖိုင်မျှဝေရာတွင် သုံးနိုင်သည်။ Wifi driveသည်များသောအားဖြင့် ညွှန်ကြားချက်များနှင့်အတူ သို့မဟုတ် drive ဆက်သွယ်ရန် app များပါပြီး သုံးစွဲရန် လွယ်ကူသည်။ လုံခြုံရေးအတွက် drive ကို လျှို့ဝှက်နံပါတ်လုပ်ရန် သတိရပါစေ။</p>
<p>[IMAGE] Users can connect to a wireless drive to share files.</p>	<p>သုံးစွဲသူများသည် ကြိုးမဲ့စက်ကို ဆက်သွယ်ပြီး ဖိုင်များမျှဝေနိုင်သည်။</p>
<p>If you don't have a wireless drive, you can also share files on a regular USB drive by plugging it into a wireless router. A travel router with a USB port, for example, is relatively inexpensive and very portable. Users can connect to the USB drive through a local network (no internet required). To access files on the connected USB drive on your phone, you will need to use a file manager app that can connect to networked storage, such as Solid Explorer. The IP address of your router can usually be found in your phone's advanced wifi settings.</p>	<p>ကြိုးမဲ့drive မရှိဘူးဆိုရင် ပုံမှန် USB drive ကို ကြိုးမဲ့ကွန်ယက်ဖြန့်ချိကိရိယာ မှာ ပလပ်ထိုးပြီး သုံးလို့ရပါသည်။ USB အပေါက်ပါသော ခရီးသွားကွန်ယက်ဖြန့်ချိကိရိယာသည် ဈေးသက်သာပြီး သယ်ယူရန်လွယ်ကူသည်။ သုံးစွဲသူသည် USB drive ကို အင်တာနက်မလိုဘဲ ဒေသတွင်းဧရိယာကွန်ယက်မှတစ်ဆင့် ဆက်သွယ်နိုင်သည်။ ဖုန်းထဲမှာရှိသောဖိုင်များကို USB drive နှင့် ဝင်ရောက်ချိတ်ဆက်ရန် ဖိုင်မန်နေဂျာ app ကို သုံးစွဲပြီး Solid Explorer ကဲ့သို့ကွန်ယက်တွင်းရှိ သိုလှောင်ခန်းများကို ဆက်သွယ်နိုင်သည်။ ကွန်ယက်ဖြန့်ချိကိရိယာ၏ အိုင်ပီလိပ်စာကို သင့်ဖုန်း၏ advanced wifi settings တွင် တွေ့ရှိနိုင်သည်။</p>

<p>[IMAGE] Users can connect to a USB drive plugged into a wireless router to share files over a LAN.</p>	<p>သုံးစွဲသူသည် USB drive ကို ကြိုးမဲ့ကွန်ယက်ဖြန့်ချိကိရိယာတွင် ပလပ်ထိုးပြီး ဒေသခံရိယာကွန်ယက်မှတစ်ဆင့် ဖိုင်များကို မျှဝေနိုင်သည်</p>
<p>[IMAGE] Use a file manager app (Solid Explorer shown here) to connect to the network on your phone.</p>	<p>ဖိုင်မန်နေဂျာ app ကိုသုံး၍ (Solid Explorer ပြထားသည်) ဖုန်းထဲရှိကွန်ယက်များနှင့် ဆက်သွယ်ခြင်း</p>
<p>Meanwhile, another option is PirateBox, a do-it-yourself project that provides freely licensed software. Users can share files as above, but Piratebox lets them do so anonymously, and also includes chat and messaging features. Setting up a Piratebox requires downloading, installing, and setting up a few pieces of software. Instructions are on the Piratebox website.</p>	<p>နောက်တစ်ခုသုံးနိုင်တဲ့ နည်းလမ်းတစ်ခုက PirateBox လို့ခေါ်တဲ့ ကိုယ်တိုင်လုပ် ပရောဂျက်ဖြစ်ပြီးတော့ လိုင်စင်ရှိဖရီးဆော့ဖ်ဝဲဖြစ်သည်။ အပေါ်မှာပြထားသလိုပဲ ဖိုင်တွေကို မျှဝေနိုင်ပြီး PirateBox ကအမည်မသိမျှဝေခွင့် ပေးမှာဖြစ်တဲ့အပြင် ချက်နဲ့ မတ်ဆွေပို့နိုင်တဲ့ အင်္ဂါရပ်များလည်းပါဝင်ပါသည်။ PirateBox ကိုပြင်ဆင်ခြင်း setup လုပ်ဖို့အတွက် ဆော့ဖ်ဝဲ အပိုင်းအစအနည်းငယ်ကို download, install နဲ့ setup လုပ်ရမှာဖြစ်ပါသည်။ ညွှန်ကြားချက်များကို Pirate Box ဝက်ဘ်ဆိုက်တွင် ကြည့်ပါ။</p>
<p>[IMAGE] PirateBox</p>	<p>PirateBox</p>
<p>Communicate via peer-to-peer chat</p>	<p>မိတ်ဆွေချင်းချက်လုပ်ပြီးဆက်သွယ်ခြင်း</p>
<p>Two new-ish peer-to-peer messaging apps that we have become aware of through activist networks are Briar and Bridgefy. We haven't tried them yet, but we know others who</p>	<p>တက်ကြွလှုပ်ရှားသူကွန်ယက်များမှတစ်ဆင့် သတိပြုမိလာတဲ့ အသစ်ကဲ့သို့</p>

<p>are testing them.</p>	<p>မိတ်ဆွေချင်းအချက်ပို့ဆက်သွယ်တဲ့ app များတွင် Briar and Bridgefy တို့ဖြစ်သည်။ ကျွန်ုပ်တို့ သုံးစွဲဖူးခြင်းမရှိသေးသော်လည်း စမ်းသပ်သုံးစွဲဖူးသူများကို သိရှိပါသည်။</p>
<p>Briar is an open-source, end-to-end encrypted messaging app that doesn't rely on a central server, but instead syncs messages between users' devices (so content lives on each user's device). It can sync even when there is no internet using Bluetooth or WiFi (when there is internet, the app syncs devices over the Tor network). Briar also features private groups, public forums, and blogs. When using offline, your range is limited by your Bluetooth or WiFi range (maximum ~ 100 meters).</p>	<p>Briar သည် ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီး နှစ်ဖက်လုံးလျှို့ဝှက်ထိန်းသိမ်းသောစနစ်ဖြင့် အချက်ပို့သော app ဖြစ်ပြီး ဗဟိုဆာဗာကို အားကိုးခြင်းမရှိဘဲ သုံးစွဲသူများ၏ဖုန်း(device) များကို syncs ဆွဲယူခြင်း (သုံးစွဲသူတိုင်း၏ device တွင် အကြောင်းအရာများကို အသက်ဝင်နေမည်။ အင်တာနက်မသုံးဘဲ Bluetooth or Wifi သုံးရုံဖြင့်လည်း ဆွဲယူနိုင်သည်။ (အင်တာနက်ရချိန်တွင် Tor ကွန်ယက်ကိုသုံးပြီး ဆွဲယူနိုင်သည်) Briar သည် ကိုယ်ပိုင်အုပ်စုဖွဲ့ခြင်း အများသုံးဖိုရမ်များ ဘလော့များလည်း တည်ဆောက်နိုင်သော အင်္ဂါရပ်များပါသည်။ အော်ဖ်လိုင်သုံးချိန်တွင် သင်၏အကွာအဝေးသည် Bluetooth or Wifi အကွာအဝေးကဲ့သို့ ကန့်သတ်ချက်ရှိသည်။ (အများဆုံး တရာမီတာ)</p>
<p>Meanwhile, Bridgefy is an end-to-end encrypted (except when using "broadcast" feature) messaging app that uses Bluetooth to send messages. Unlike Briar, messages can travel longer distances by hopping along a mesh network of other Bridgefy users (only the intended recipient can read the message). Bridgefy lacks Briar's private groups, forums, and blog features, but it does have a Broadcast mode through which you can send a message to up to 7 Bridgefy users within range, who do not need to be your contacts (Broadcast messages are by necessity</p>	<p>တချိန်တည်းတွင် Bridgefy သည် နှစ်ဖက်လုံးလျှို့ဝှက်လိုခြံသော (တိုက်ရိုက်အသံလွှင့်သော အင်္ဂါရပ်သုံးခြင်းမှအပ) အချက်ပို့သော app ဖြစ်ပြီး Bluetooth ကိုသုံးပြီး အချက်ပို့သည်။ Briarနဲ့မတူသောအချက်က မတ်ဆွေသည် အကွာအဝေးရှည်ရှည် ခရီးရောက်နိုင်သည်။ အခြား Bridgefy သုံးစွဲသူများ၏ ပိုက်စိတ်တိုက်ထားသောကွန်ယက်မှ ခုန်ဆွဲခြင်း (ရည်ရွယ်ပြီးပို့သူသာဖတ်လိုရမည်ဖြစ်သည်)။ Bridgefy သည် Briar ကဲ့သို့</p>

<p>encryption protocol. While we haven't tried it ourselves, we have heard that others have used it. Both the sender and recipient need to have it installed and exchange keys with each other. Since SMS messages necessarily go through your telecom's servers, even with Silence the fact that you are sending an encrypted message and the metadata about your message will be accessible to the telecom company.</p>	<p>လျှို့ဝှက်ထိန်းသိမ်းထားသော SMS ဖြစ်သည်။ ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီး Signal ၏လျှို့ဝှက်ထိန်းသိမ်းခြင်းလုပ်ထုံးလုပ်နည်းကို သုံးထားသည်။ ကျွန်ုပ်တို့ကိုယ်တိုင်စမ်းသပ်ဖူးခြင်းမရှိသော်လည်း အခြားသူများသုံးသည်ကို ကြားဖူးသည်။ ပေးပို့သူရော လက်ခံသူပါ install လုပ်ထားရမှာဖြစ်ပြီး လဲလှယ်သောသော့ချက်ရှိရမှာဖြစ်သည်။ SMS သည် သင့်ရဲ့တယ်လီကွန်း ဆာဗာကိုဖြတ်ပြီးမှသွားမှာဖြစ်တဲ့အတွက် Silence ကိုသုံးရင်တောင်မှ လျှို့ဝှက်သောမတ်ဆွေကိုပို့မှာဖြစ်သော်လည်း မတ်ဆွေရဲ့metadata တွေကိုတော့ တယ်လီကွန်း ကုမ္ပဏီတွေကနေ အချက်အလက်ရှာဖွေနိုင်မှာ ဖြစ်ပါသည်။</p>
<p>Partial shutdowns: Circumvent blocked sites</p>	<p>တစ်စိတ်တစ်ပိုင်းဖြတ်တောက်ခြင်း ပိတ်ပင်တားဆီးထားသောဆိုက်ဒ်များကိုရှောင်တိမ်းခြင်း</p>
<p>An "internet shutdown" often does not mean total internet blackout, but rather blocking access to specific websites or social media platforms. Governments, via internet service providers (ISPs), can block sites based on IP address, content, or via DNS lookups. Unsure if a site is being blocked? Organizations like Open Observatory of Network Interference and Netblocks monitor and measure internet disruptions and censorship around the world.</p> <p>Fortunately, as long as you have internet access, there are some ways to try to get around the partial blocks. As with</p>	<p>မကြာခဏအားဖြင့် အင်တာနက်ဖြတ်တောက်ခြင်းသည် အင်တာနက်တစ်ခုလုံး ပြတ်အောင်ပိတ်ခြင်းမဟုတ်ဘဲ အချို့သီးခြားဝက်ဘ်ဆိုက်ဒ်နှင့် ဆိုရှယ်မီဒီယာများကိုသာ ပိတ်ပင်ခြင်းလည်းဖြစ်နိုင်သည်။ အာဏာပိုင်အစိုးရသည် အင်တာနက်ဝန်ဆောင်မှုပေးသူ ISP များမှတစ်ဆင့် အိုင်ပီလိပ်စာပေါ်အခြေခံသောပိတ်ပင်ခြင်း အကြောင်းအရာသို့မဟုတ် DNS lookups ဒီမိုင်းအမည်စနစ်ရှာဖွေခြင်းစနစ်ကတစ်ဆင့် ပိတ်ပင်နိုင်သည်။</p>

<p>encryption, keep in mind that circumventing blocked sites may be criminalized in your country.</p>	<p>ဆိုက်ဒ်တစ်ခုကပိတ်ပင်ထားခြင်းခံရသလားဆိုတာမသေချာဘူးလား အဖွဲ့အစည်းများဖြစ်သော Open Observatory of Network Interference and Netblocks စသောအဖွဲ့အစည်းများက လေ့လာစောင့်ကြည့်ချင်း အင်တာနက်ပြတ်တောက်မှုနဲ့ ပတ်သက်ပြီး တိုင်းတာခြင်း ဆင်ဆာဖြတ်ခြင်းကို ကမ္ဘာနှင့်တဝန်းတွင် လုပ်ဆောင်သည်။ ကံကောင်းထောက်မသည်မှာ သင့်တွင် အင်တာနက်ဝင်ရောက်ချိတ်ဆက်ခွင့် ရှိသမျှ ကာလပတ်လုံး တစ်စိတ်တစ်ပိုင်းပိတ်ဆို့ခြင်းကို ကျော်ဖြတ်နိုင်သော နည်းလမ်းများရှိသေးသည်။ လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption နှင့်အတူ ပိတ်ဆို့ထားသောဆိုက်ဒ်များကို ရှောင်တိမ်းပြီးအသုံးပြုခြင်းသည်လည်း သင့်နိုင်ငံတွင် ရာဇဝတ်ပြစ်မှုအဖြစ်သတ်မှတ်နိုင်ကြောင်း သတိပြုပါ။</p>
<p>VPN</p>	<p>ဗီပီအန် ခေါ် လျှို့ဝှက်ဆက်သွယ်ကွန်ယက်</p>
<p>One way to bypass IP-based and content-based blocking is to use a virtual private network or VPN, such as ProtonVPN or TunnelBear. When you connect through a VPN, your internet traffic is encrypted and routed through a VPN server in another location, such as in another country, thus concealing the true destination and the content of your traffic to your ISP.</p> <p>Keep in mind that some governments ban VPN usage or may try to detect and block VPN connections. It is also important to use a trustworthy VPN provider, and preferably one that does not store data or logs, since the provider will be able to see your</p>	<p>အိုင်ပီအခြေခံနှင့် အကြောင်းအရာကို အခြေခံသော ပိတ်ပင်တားဆီးခြင်းကို ရှောင်ကွင်းကျော်ဖြတ်ရန်နည်းလမ်းတစ်ခုမှာ Proton VPN or TunnelBear ကဲ့သို့ လျှို့ဝှက်ကွန်ယက်စနစ် ဗီပီအန်သုံးခြင်းဖြစ်သည်။ ဗီပီအန်မှတစ်ဆင့် ဆက်သွယ်သောအခါ အင်တာနက်အသွားအလာ လမ်းကြောင်းသည် လျှို့ဝှက်လုံခြုံပြီး ဗီပီအန်ဆာဗာမှတစ်ဆင့် တခြားအရပ်ဒေသ၊ အခြားနိုင်ငံအစရှိသဖြင့် ပြောင်းသွားပြီး အမှန်တကယ်ရည်ရွယ်ရာအရပ်နှင့် သင့်အင်တာနက်အသွားအလာလမ်းကြောင်း အကြောင်းအရာကို</p>

<p>internet activity. Be aware of what country the VPN provider is based in, and what legal processes they may be subject to based on their jurisdiction. Also consider that government-approved VPNs may actually enable surveillance and inspection of your data.</p>	<p>သင့်အင်တာနက်ဝန်ဆောင်မှုပေးသူအား ဖုံးကွယ်သည်။</p> <p>ဖြတ်သန်းသွားသောကြောင့် တကယ်နေရာအစစ်အမှန်နဲ့ ပါဝင်မှုများကို လမ်းကြောင်းပြောင်းပေးသည်။ တချို့နိုင်ငံအစိုးရများက ဗီပီအင်သုံးစွဲမှုကို ပိတ်ပင်ခြင်း သို့မဟုတ် ပိတ်ထားသော ဗီပီအင်မှ တဆင့်သုံးစွဲမှုကို ခြေရာခံခြင်းများ လုပ်နိုင်သည်။ အရေးကြီးသည်မှာ စိတ်ချရသော ဗီပီအင်ကိုသုံးစွဲခြင်း အချက်အလက်များကို မစုဆောင်းသော တခုကို သုံးစွဲခြင်းကို ပြုသင့်သည်။ မည်သည့်နိုင်ငံတွင် ဗီပီအင်ကရှိနေသလဲ သူတို့ရဲ့ ဆုံးဖြတ်သုံးသပ်မှုများသည် တရားဆိုင်ရာလမ်းကြောင်းများရှိမရှိ တချို့ အစိုးရသည် ဗီပီအင်ကို ခွင့်ပြုသော်လည်း သင့်အချက်အလက်များကို စုံစမ်းထောက်လှမ်းခြင်း လေ့လာစစ်ဆေးခြင်းများလုပ်ဆောင်သည်။</p>
<p>DNS servers</p>	<p>DNS ဆာဗာ ဒိုမိန်းအမည်စနစ်</p>
<p>DNS (“domain name system”) servers work by translating the domain names or URLs that a user types into a browser into the numerical IP addresses that the internet uses to identify webpages. An ISP can modify the DNS servers it controls to block certain queries, or to return an incorrect page saying that the website doesn’t exist. In 2014, Turkish Prime Minister Recep Tayyip Erdoğan attempted to block Twitter during Turkish elections using this technique. The ban was quickly thwarted by activists who shared step-by-step tips on how to use VPNs and</p>	<p>DNS (ဒိုမိန်းအမည်စနစ်) ဆာဗာတွေဟာ ဒိုမိန်းအမည်တွေကို ဘာသာပြန်ပြီး အလုပ်လုပ်တဲ့ သို့မဟုတ် သုံးစွဲသူအနေနဲ့ နံပါတ်ပါသော အိုင်ပီလိပ်စာများကို ရိုက်ထည့်ပြီး အင်တာနက် ဝက်ဘ်စာမျက်နှာတွေကို ခွဲခြားသတ်မှတ်တဲ့ URL တွေ ဖြစ်ပါသည်။</p> <p>ISP အင်တာနက်ဝန်ဆောင်မှုပေးသူသည် ဒိုမိန်းအမည်စနစ် DNS ဆာဗာများကို ပြုပြင်ပြီး အချို့မေးမြန်းချက်များကို ထိန်းချုပ်ခြင်း ဝက်ဘ်ဆိုက်ဒ်မရှိပါ ဟူ၍ မမှန်သောစာမျက်နှာများကို ပြန်ပို့ခြင်းလုပ်သည်။</p>

<p>change DNS servers.</p>	<p>၂၀၁၄ ခုနှစ် တူရီကီရွေးကောက်ပွဲကာလအတွင်း တူရကီဝန်ကြီးချုပ် Recep Tayyip Erdogan က တွစ်တာကို ပိတ်ရန်ကြိုးစားတုန်းက ထိုနည်းကိုသုံးခဲ့သော်လည်း ပိတ်ပင်ခြင်းကို တက်ကြွလှုပ်ရှားသူများက လျင်မြန်စွာ ဖောက်ထွင်းပြီး ဗီပီအင်သုံးရန်နှင့် ဒိုမိန်းအမည်စနစ် DNS ဆာဗာပြောင်းရန် အသုံးဝင်သည့်အချက်များကို တဆင့်ပြီးတဆင့် တဆင့်ချင်း တားဆီးနိုင်ခဲ့သည်။</p>
<p>You can change the default DNS server in your phone's network or wifi settings. Instead of the default DNS server, you can use alternative DNS servers such as Google Public DNS or CloudFlare to get around DNS-based blocks. Cloudflare also has an app called 1.1.1.1 that allows users to switch to a Cloudflare DNS server through a simple app interface.</p>	<p>မူလDNSဆာဗာကို ဖုန်းရဲ့network သို့မဟုတ် wifi setting မှာ ပြောင်းလိုရပါသည်။ ဆာဗာသုံးတဲ့အခါ မူလDNSဆာဗာ တမျိုးတည်းမသုံးဘဲ အပြောင်းအလဲဆာဗာတွေဖြစ်တဲ့ Google Public DNS or CloudFlare တွေကို ပြောင်းလဲသုံးခြင်းဖြင့် DNSကို အခြေခံပြီး ပိတ်ဆို့တာတွေကို လှည့်ပတ်သွားနိုင်မှာဖြစ်ပါသည်။ CloudFlare တွင်လည်း 1.1.1.1 ဟုခေါ်သည့် app ရှိပြီး သုံးစွဲသူအား ရိုးရှင်းသော app မှ တဆင့် CloudFlare DNS ဆာဗာသို့ပြောင်းလဲရန် ခွင့်ပေးသည်။</p>
<p>[IMAGE] You can change DNS addresses in advanced wifi settings (note down or take a picture of your old settings first).</p>	<p>DNSလိပ်စာပြောင်းရန် advanced wifi setting ဆက်တင်ကိုသွားပါ။ (ဆက်တင်အဟောင်းကို အရင်ရေးမှတ်ပါ သို့မဟုတ် ဓာတ်ပုံရိုက်ထားပါ)</p>
<p>These are just two ways to circumvent the most common blocking techniques. Check out helpful guides from Internet Society, Access Now, Security-in-a-Box, and EFF for more in-</p>	<p>ပိတ်ပင်ခြင်းကိုရှောင်တိမ်းနိုင်သောအသုံးများသည့် နည်းလမ်းနှစ်မျိုးသာ ရှိသည်။ အတွင်းကျကျအချက်အလက်များကို လေ့လာလိုလျှင် “Internet Society, Access Now, Security-in-a-Box and EFF” တွင် အတွင်းကျကျ</p>

depth information.

အချက်အလက်များကိုရရှိနိုင်ပါသည်။