EFF'S SURVEILLANCE SELF-DEFENSE

လက်ဗွေ အသုံးပြုခြင်းဆိုတာ ဘာလဲ။

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

လက်ဗွေ အသုံးပြုခြင်းဆိုတာ ဘာလဲ။

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ- ၂၇/၀၆/၂၀၂၁

လက်ဗွေ အသုံးပြုခြင်း ဆိုတာ ဘာလဲ။

ဒီဂျစ်တယ် လက်ဗွေ အသုံးပြုခြင်းဆိုတာက ဆိုက်တစ်ခု (သို့မဟုတ်) ဝန်ဆောင်မှုတစ်ခုမှ အသုံးပြုသူ၏ စက်ရှိ အချက်အလက်အပိုင်းအစများကို စုစည်းပြီး အဲဒီစက်အတွက် သီးသန့်ဖြစ်သောပုံစံ (သို့မဟုတ်) လက်ဗွေ "fingerprint"ကို ထုတ်ပေးတဲ့ ဖြစ်စဉ်တစ်ခု ဖြစ်ပါတယ်။ ဒီဂျစ်တယ်လက်ဗွေ အသုံးပြုနိုင်တဲ့ ပုံစံ နှစ်မျိုးရှိပါတယ်။ ဘရောက်ဇာ လက်ဗွေအသုံးပြုခြင်း မှာဆိုရင် အသုံးပြုသူက ဆိုက်များအတွင်း ဝင်ရောက်တဲ့အခါ အချက်အလက်များကို ဘရောက်ဇာမှတဆင့် ပေးပို့ပါတယ်။ စက်ပစ္စည်း လက်ဗွေအသုံးပြုခြင်းမှာတော့ စက်အတွင်းသိမ်းဆည်းထားတဲ့ အက်ပ်များကတဆင့် အချက်အလက်များကို ပေးပို့ပါတယ်။

များသောအားဖြင့် လက်ဗွေအသုံးပြုမှုမှာ ဆိုက်များ (သို့မဟုတ်) အက်ပ်များကို ဝန်ဆောင်မှု ပေးသူများက တိုက်ရိုက်ထုတ်ပေးခြင်းထက် တတိယပါတီက ဝန်ဆောင်မှု ပေးလေ့ရှိပါတယ်။ စက်ပစ္စည်းတစ်ခု အတွင်းမှာရှိတဲ့ အက်ပ်များနှင့် ဆိုက်များအတွက် တတိယပါတီတစ်ခုရဲ့ ခြေရာခံစက်ကို ထည့်သွင်းထားမယ်ဆိုရင် အဲဒီခြေရာခံစက်က လူတစ်ဦးအသုံးပြုတဲ့ ဆိုက်တွေ၊ အက်ပ်တွေကို ခြေရာခံမှတ်သားပေးပါတယ်။ ဒီလိုမှတ်သားထားခြင်းအားဖြင့် လူတစ်ယောက်ရဲ့ နေ့စဉ် အသုံးပြုမှုကို တိတိကျကျ မှတ်တမ်းတင်ထားနိုင်ပါတယ်။ ဘယ်လောက်တိကျသလဲဆိုရင် လူတစ်ယောက်က ဘယ်အချိန်မှာ ဘာလုပ်နေသလဲဆိုတာနဲ့ ဘယ်နေရာမှာလဲဆိုတာကို စက်ပစ္စည်းကို ခြေရာခံပြီး သိနိုင်ပါတယ်။

လက်ဗွေ အသုံးပြုခြင်းနှင့် ပစ်မှတ်ထားခြင်း

လက်ဗွေအသုံးပြုခြင်းကို ခြေရာခံဝန်ဆောင်မှုပေးတဲ့ ကုမ္ပဏီတွေအများဆုံး အသုံးပြုပါတယ်။ ရလာ တဲ့ အချက်အလက်တွေကို အသုံးပြုသူအကြိုက် ကြော်ငြာထိုးဖို့သုံးတာ (သို့မဟုတ်) ဒေတာ ပွဲစားတွေဆီရောင်းချပါတယ်။ ဒီဂျစ်တယ်ကြော်ငြာလုပ်ငန်းဟာ ဘီလီယံရာပေါင်းများစွာ တန်တဲ့ စျေးကွက်ဖြစ်ပါတယ်။ ဆိုက် (သို့မဟုတ်) အက်ပ်ကို ထပ်မံ ဝင်ရောက်သူ တွေကို ပစ်မှတ်ထားခြင်းနဲ့ ဘရောက်ဇာဝင်ရောက်မှုမှတ်တမ်းကို အခြေခံပြီး အရောင်းမြှင့် တင်ရေး လုပ်ခြင်း စတာတွေဟာ အရောင်းမြှင့်တင်သူတွေအတွက် ကလစ်ထောက် ဝင်ရောက်ကြည့်ရှုမှုနှုန်း မြင့်လာဖို့နဲ့ ရောင်းအားတက်လာဖို့အတွက် အလွန်အရေးပါတဲ့ နည်းလမ်းတွေဖြစ်ပါတယ်။

ပစ်မှတ်ထားကြော်ငြာရာမှာ ဝက်ဘ်ဆိုဒ်အတွက်ဆိုရင် ဘရောက်ဇာ ကွတ်ကီးများ cookies နဲ့ အက်ပ်အတွက်ဆိုရင် iOS နဲ့ Android က ပေးတဲ့ ကြော်ငြာသူအိုင်ဒီနည်းလမ်းတွေကို အများဆုံး သုံးပါတယ်။ ဒါပေမဲ့ အသုံးပြုသူအနေနဲ့ ကွတ်ကီးတွေနဲ့ ကြော်ငြာသူအိုင်ဒီတွေကို ဖျက်လိုက်မယ်ဆို ရင် မိမိနဲ့ ဘရောက်ဇာ (သို့မဟုတ်) အက်ပ်ကြား ချိတ်ဆက်ထားတဲ့ သီးသန့်အမှတ်အသား (persistent identifier) ကို ဖျောက်နိုင်ပါတယ်။ သင့်ရဲ့ ဘရောက်ဇာဝင်ရောက်မှုမှတ်တမ်းဆိုတာကို ဘုတ်ပြားတစ်ခုပေါ်မှာထိုးထားတဲ့ ပင်အပ်လေးတွေကို ကြိုးတစ်ချောင်းနဲ့ ချိတ်ဆက်ထားတာလို့ မြင်ယောင်ကြည့်ပါ။ ပင်အပ်လေးတွေက သင်ဝင်ရောက်ခဲ့တဲ့ ဆိုက်တွေဖြစ်ပြီး ခြေရာခံစက်ကတော့ ကြိုးစကို ခြေရာကောက်ပြီး သင်ဘယ်နေရာတွေကို ဝင်ရောက် ခဲ့လဲဆိုတာကို သိနိုင်ပါတယ်။ ကွတ်ကီးတွေကိုဖျက်လိုက်ခြင်းအားဖြင့် ပင်အပ်တစ်ခုနဲ့တစ်ခုအကြားကကြိုးအပိုင်းလေးတွေကို တစ်စစီလိုက်ဖြတ်တာနဲ့တူပါတယ်။ ကွတ်ကီးများများဖျက်လေလေ ကြိုးအပိုင်းတိုလာလေလေပါပဲ။ နောက်ဆုံးတော့ သင်ဘယ်နေရာတွေကို ဝင်ရောက်ကြည့်ရှုခဲ့လဲဆိုတာကို ခြေရာမခံ နိုင်တော့ အထိဖြစ်သွားပါလိမ့်မယ်။

လက်ဗွေအသုံးပြုခြင်းကတော့ မြဲမြံတဲ့ အမှတ်အသားအသစ်နဲ့ အစားထိုးပြီး ဖျက်လို့မရတဲ့ ကြိုးကို ဖန်တီးထားပါတယ်။ လက်ဗွေက သင့်ဘရောက်ဇာ (သို့မဟုတ်) စက်ပစ္စည်းရဲ့ အဓိက ပုံစံတွေနဲ့ ဆန့်ကျင်တဲ့နည်းလမ်းကို သုံးထားပါတယ်။ သီးသန့်အမှတ်အသားကတော့ သင့်ဘရောက်ဇာနဲ့ စက်ပစ္စည်းမှာရှိတဲ့ ပုံစံတွေအားလုံးကို ပေါင်းထားတာပါ။ လက်ဗွေအသုံးပြုခြင်း ရှိနေရတဲ့ အကြောင်းရင်းတစ်ခုကတော့ အသုံးပြုသူတွေပုံမှန်သုံးနေကျဖြစ်တဲ့ ဘရောက်ဇာထိန်းချုပ်ခလုတ်တွေရဲ့ လုပ်ဆောင်မှုတွေကို ကျော်လွှားပြီးခြေရာခံနိုင်ဖို့ဖြစ်ပါတယ်။ ဘရောက်ဇာနဲ့ မိမိတို့ရဲ့စက်ပစ္စည်းတွေ ကို ကိုယ့်ရဲ့ထိန်းချုပ်မှုအောက်မှာပဲရှိစေဖို့ဆိုရင်တော့ လက်ဗွေအသုံးပြုခြင်းကို ခုခံနိုင်တဲ့ နည်းလမ်းတွေ အသုံးပြုဖို့ လိုလာပါတယ်။

လက်ဗွေအသုံးပြုခြင်းကို ခြေရာခံစနစ်အဖြစ်အသုံးပြုခြင်း၏ ထိရောက်မှု

ခြေရာခံစက်တွေအတွက် လက်ဗွေအသုံးပြုမှု ထိရောက်စေဖို့အတွက် အချက်နှစ်ချက်လိုပါတယ်။

ပထမအချက်က fingerprint လက်ဗွေဟာ တသမတ်တည်းဖြစ်ဖို့လိုပါတယ်။ အသုံးပြုသူရဲ့ လက်ဗွေက ခဏခဏပြောင်းနေမယ်ဆိုရင် တစ်ကြိမ်နဲ့တစ်ကြိမ်ဝင်ရောက်ကြည့်ရှုနေတာကို ခြေရာခံဖို့ ခက်ပါမယ်။ ဝက်ဘ်ဆိုက် (သို့မဟုတ်) အက်ပ်တွေကို တူညီတဲ့ အသုံးပြုသူက ဝင်ရောက်နေ လားဆိုတာကို ဆုံးဖြတ်နိုင်ဖို့အတွက် ဝင်ရောက်တဲ့အကြိမ်တိုင်းကို ချိတ်ဆက်နိုင်စွမ်းက အရေးကြီးပါတယ်။ မြဲမြံတဲ့အမှတ်အသားဟာ ကွတ်ကီးအစားထိုးသုံးတာဖြစ်ပြီး အသုံးပြုသူက အလွယ်တကူ ဖျက်လို့ရပါတယ်။ လက်ဗွေကို တော့ အလွယ်တကူဖယ်လို့မရပါဘူး၊ ဘာလို့လဲဆိုတော့ အသုံးပြုသူရဲ့ စက်ထဲမှာ သိမ်းထားတာမဟုတ်လို့ပါ။

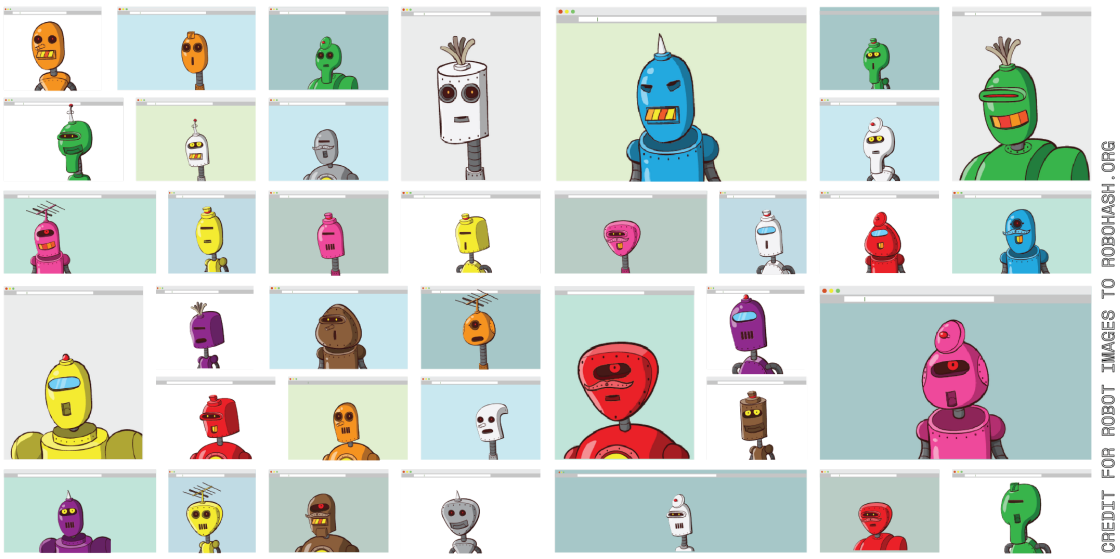
ဒုတိယအချက်ကတော့ အများနဲ့မတူ တမူထူးခြားနေဖို့ လိုပါတယ်။ လူနှစ်ယောက် (သို့မဟုတ်) လူအများကြီးအတွက် တူညီတဲ့ လက်ဗွေတွေရှိနေရင်တော့ ခြေရာခံစက်က လူနဲ့ လက်ဗွေကို တွဲပြီး မှတ်သားနိုင်စွမ်းမရှိတော့ပါဘူး။ ခြေရာမခံနိုင်တော့တဲ့အတွက် လူတစ်ယောက်က "မုန့်ဖုတ်ဝါသနာရှင်" ဒါမှမဟုတ် "လေယာဉ်များကို စိတ်ဝင်စားသူ" စသည်ဖြင့် ခွဲခြားမပေးနိုင်တော့လို့ ပစ်မှတ်ထားအရောင်းမြှင့်တင်တာမျိုး မလုပ်နိုင်တော့ပါဘူး။ ကျွန်ုပ်တို့ရဲ့ ၂၀၁၀ တုန်းက လုပ်ခဲ့တဲ့ ဘရောက်ဇာ အသုံးပြုသူများကို လေ့လာတဲ့ Panopticlick သုတေသနမှာဆိုရင် ဘရောက်ဇာအများစုမှာ အခုရှင်းပြတဲ့ အချက်နှစ်ချက်ရှိနေတာကို တွေ့ရပါတယ်။

လက်ဗွေအသုံးပြုခြင်းကို ပြန်လည်ခုခံနိုင်သည့် ဗျူဟာများ

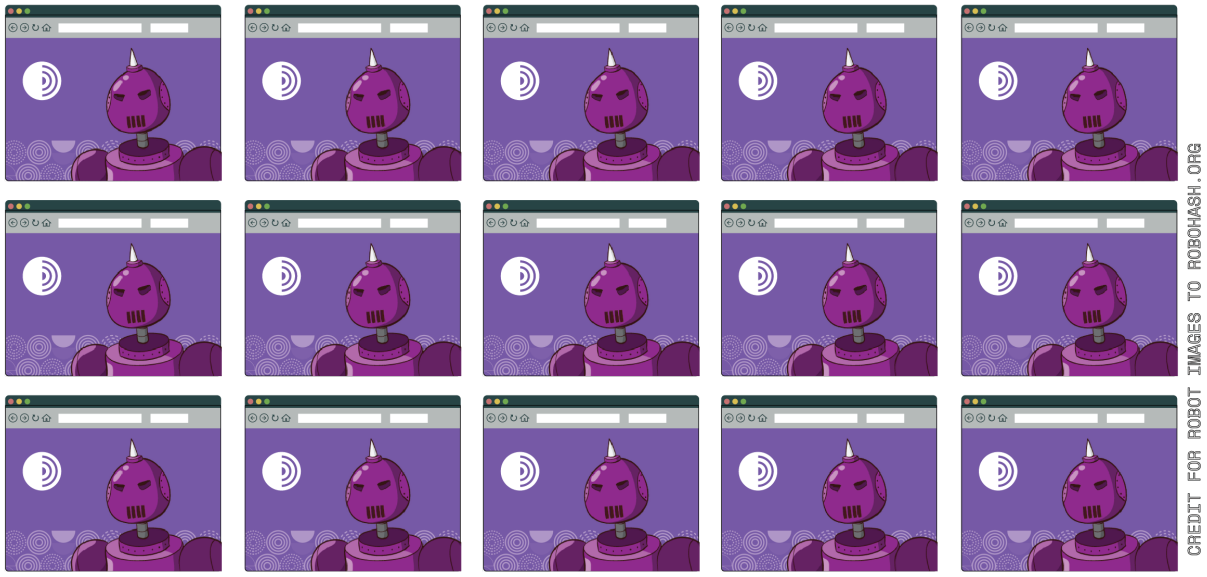
လက်ဗွေအသုံးပြုခြင်းကို ထိထိရောက်ရောက် ပြန်လည်ခုခံဖို့အတွက် အောက်မှာဖော်ပြထားတဲ့ ဗျူဟာတွေကို သုံးလို့ရပါတယ်။ ပထမဆုံးအနေနဲ့ အထက်မှာဖော်ပြခဲ့တဲ့ အချက်နှစ်ချက်ကို ဖယ်ရှားနိုင်ပါတယ်။ ဒုတိယအချက်အနေနဲ့ ခြေရာခံစက်တွေကိုစာရင်းလုပ်ပြီး ဘရောက်ဇာ (သို့မဟုတ်) မိုဘိုင်းစက်ထဲမှာ အလုပ်မလုပ်နိုင်အောင် ပိတ်ပင်နိုင်ပါတယ်။

လက်ဗွေတွေရဲ့ ကြာရှည်စွာတည်ရှိမှုကို ဖျက်ဆီးနိုင်တဲ့ နည်းလမ်းများစွာရှိပါတယ်။ ဥပမာ- canvas fingerprint and AudioContext fingerprinting တို့ကိုသုံးပြီး လက်ဗွေထဲမှာရှိတဲ့ အချို့ ကိန်းဂဏန်း ပုံစံတွေကို အစီအစဉ်တကျမဟုတ်ဘဲ ပြောင်းပစ်တာမျိုးဖြစ်ပါတယ်။ ဒီနည်းလမ်းက လက်ဗွေရဲ့ကြာရှည် စွာတည်ရှိမှုကို ဖျက်ဆီးနိုင်ပေမမယ့် အစီအစဉ်တွေကိုပြောင်းပစ်တဲ့နည်းလမ်းကို သုံးတယ်ဆိုတာကို ခြေရာခံစက်က သိရှိနိုင်ပါသေးတယ်။ ခြေရာခံစက်တွေကို ပိတ်ပင်နိုင်ဖို့အတွက် ဒီနည်းလမ်းကို အသုံးပြုတဲ့အခါ အသုံးဝင်/မဝင်ကို သေချာစဉ်းစားဖို့လိုပါတယ်။

ဘရောက်ဇာနံပါတ်တွေအားလုံးကို တူညီအောင်လုပ်တဲ့နည်းကလည်း လက်ဗွေအသုံးပြုပြီး ခြေရာခံတာကို ပိတ်ပင်နိုင်တဲ့နည်းလမ်းဖြစ်ပါတယ်။ ဘရောက်ဇာနံပါတ်တွေမှာပေါ်နေတဲ့ လက်ဗွေကိန်းဂဏန်း ပုံစံတွေအားလုံးကို တူညီအောင်လုပ်ထားခြင်းအားဖြင့် ဘရောက်ဇာတွေကို သီးခြားခွဲထုတ်ခြေရာခံလို့ မရတော့ပါဘူး။ ဒီနည်းလမ်းကို ဘယ်သူသုံးမှန်းမသိအောင် ခြေရာဖျောက်ထားတဲ့ Tor Browser မှာသုံးထားပါတယ်။



ဘရောက်ဇာတစ်ခုချင်းစီက ထူးခြားတဲ့ဝိသေသတွေကို ခြေရာခံစက်က တောက်လျှောက် ခြေရာခံပါတယ်။



ဘရောက်ဇာတွေ အားလုံးက တူညီနေတာမို့ ခြေရာခံစက်တွေက သီးခြားလက်ဗွေ fingerprint တွေ မထုတ်ပေးနိုင်တော့ ပါဘူး။

ဒီနည်းလမ်းကို မှန်မှန်ကန်ကန်အသုံးပြုမယ်ဆိုရင် လက်ဗွေခြေရာခံမှုမလုပ်နိုင်အောင် ထိထိရောက် ရောက်တားဆီးနိုင်ပါတယ်။ Tor ဘရောက်ဇာက ဘရောက်ဇာတွေအားလုံးကို အတူတူဖြစ်အောင်

လုပ်နိုင်တဲ့ အစိတ်အပိုင်းတွေကို ဖော်ထုတ်အသုံးပြုထားနိုင်ပါတယ်။ ဒီအချက်က အရေးကြီးပါတယ်။ ဘာလို့လဲဆိုတော့ တခါတလေမှာ ကိုယ့်ကိုခြေရာမခံမိအောင်လုပ်ရင်းနဲ့ ခြေရာခံဖို့ပိုလွယ်သွားတတ်တာကြောင့်ပါ။

နောက်ဆုံးနည်းလမ်းကတော့ ခြေရာခံစက်စာရင်းပြုစုပြီး တိုက်ရိုက်ပိတ်ပင်တဲ့ နည်းလမ်းပါ။ ဒီနည်းလမ်းကိုတော့ ဘရောက်ဇာတွေရဲ့ addons (သို့မဟုတ်) extensions တွေမှာတွေ့ရပါတယ်။ ဥပမာ- EFFs ရဲ့ ကိုယ်ပိုင် Privacy Badger လိုပေါ့။ ဘရောက်ဇာတွေပေါ်ရောက်လာတဲ့ လက်ဗွေခြေရာခံစေက်တွေကို အစုလိုက်အပြုံလိုက် ဖယ်ရှားတဲ့ နည်းလမ်းနဲ့ ခြေရာခံစက်ကတွေကို ပိတ်ပင်ခြင်း blocking တာဖြစ်ပါတယ်။ ဒီနည်းလမ်းကြောင့် လက်ဗွေနည်းလမ်းကို အများစုသုံးထားတဲ့ ခြေရာခံစက်တွေဟာ ဘရောက်ဇာအသုံးပြုသူတွေကို ခြေရာခံလို့မရတော့ပါဘူး။

ဘယ်လောက်ပဲထိရောက်တဲ့နည်းလမ်းဖြစ်ပါစေ လက်ဗွေအသုံးပြုခြင်းကို လုံးဝပိတ်ပင်ပစ်လိုက်လို့ မရပါဘူး။ စာရင်းမပေါက်တဲ့ ခြေရာခံစက် (သို့မဟုတ်) တတိယပါတီက မဟုတ်ဘဲ ဆိုက်ကနေ တိုက်ရိုက်ခြေရာခံတာမျိုး ကတော့ တားလို့ရမှာမဟုတ်ပါဘူး။ ဒီလိုအခြေအနေမှာတော့ မိမိရဲ့ ကိုယ်ရေးလုံခြုံမှုကို အပြည့်အဝ အာမခံလို့မရဘူးပေါ့။

လက်ဗွေအသုံးပြုခြင်းကို ဖယ်ရှားဖို့အတွက် မိမိရဲ့စက်တင်တွေကို စိတ်ကြိုက်မပြောင်းလဲပါနဲ့

လက်ဗွေကို ပြောင်းလဲဖို့ ကိုယ့်စက်တင်တွေကို ပြောင်းလဲတာ အလုပ်ဖြစ်လေ့ မရှိပါဘူး။

ဥပမာအားဖြင့် သင့်အနေနဲ့ သင်အသုံးပြုတဲ့ဘရောက်ဇာနဲ့ ဗားရှင်းကို ခြေရာခံတဲ့ အသုံးပြုသူ-ဝန်ဆောင်မှုချိတ်ဆက်ကြိုးကို လူအများဆုံးအသုံးပြုတဲ့ကြိုးပုံစံဖြစ်အောင် ပြောင်းလဲဖို့ ကြိုးစားကောင်းကြိုးစားမိပါလိမ့်မယ်။ လူအများဆုံးအသုံးပြုတဲ့ပုံစံမို့ လက်ဗွေရာကို ခြေရာခံရအခက်ဆုံးလို့ ထင်ကောင်းထင်ပါလိမ့်မယ်။ ဒါပေမဲ့ အဲဒီအထင်က တချို့အခြေအနေတွေအတွက်တော့ မမှန်ပါဘူး။ တခါတရံမှာ ပိုလို့တောင်ခြေရာခံလို့ကောင်းတဲ့ လက်ဗွေဖြစ်လာနိုင်ပါတယ်။ ဘာကြောင့်ပါလိမ့်။

ဒီမေးခွန်းအတွက် အဖြေကတော့ သင့်ဘရောက်ဇာမှာရှိတဲ့ အခြားလက်ဗွေထုတ်နိုင်တဲ့မက်ထရစ်တွေကနေ သင့်ရဲ့ အသုံးပြုသူ-ဝန်ဆောင်မှုချိတ်ဆက်ကြိုးက ဘယ်လောက်အမှီအခိုကင်းသလဲအပေါ်မူတည်ပါတယ်။ ဥပမာအားဖြင့် iOS ရဲ့ Safari ဘရောက်ဇာဟာ ဟာ့ဒ်ဝဲလ်၊ ဆော့ဖ်ဝဲလ်နဲ့ ဒရိုင်ဘာတွေဟာ ဘယ်စက်မှာသုံးသုံးခပ်ဆင်ဆင်ဖြစ်နေတာမို့ လက်ဗွေအသုံးပြုဖို့ခက်တဲ့ ဘရောက်ဇာ ဖြစ်ပါတယ်။ ဆိုလိုတာက iOS ရဲ့ Safari အသုံးပြုသူအတော်များများက ပုံစံတူတွေဖြစ်နေတာပါ။

ဒါပေမဲ့ iOS ရဲ့ Safari က အသုံးအများဆုံး အသုံးပြုသူ-ဝန်ဆောင်မှု ချိတ်ဆက်ကြိုး မဟုတ်ပြန်ပါဘူး။ Windows မှာရှိတဲ့ Chrome နောက်ဆုံးဗားရှင်းက အသုံးအများဆုံး အသုံးပြုသူ-ဝန်ဆောင်မှု

ချိတ်ဆက်ကြိုးဖြစ်မယ်ဆိုပါစို့။ တခြားဘယ်စက်တင်မှမပြောင်းဘဲ iOS ရဲ့ Safari ရဲ့ ချိတ်ဆက်ကြိုးကို Windows မှာရှိတဲ့ Chrome ချိတ်ဆက်ကြိုး အသွင်ပြောင်းလိုက်မယ်ဆိုရင် အဲဒီကြိုးက ထူးခြားတဲ့ကြိုးဖြစ်သွားပါလိမ့်မယ်။ canvas လက်ဗွေအတွက် iOS ရဲ့ Safari ဖြစ်ပြီး အသုံးပြုသူ-ဝန်ဆောင် မှုချိတ်ဆက်ကြိုးအတွက် Windows ရဲ့ Chrome ဖြစ်နေတဲ့ တစ်ယောက်တည်းသောသူ ဖြစ်နေပါလိမ့်မယ်။

ဒါ့ကြောင့်မို့ လက်ဗွေခြေရာခံမှုကို ရှောင်ရှားလိုသူတွေအနေနဲ့ သတိကြီးကြီးထားဖို့လိုပါတယ်။ အသုံးမတတ်ရင် ကိုယ့်ကိုခြေရာခံဖို့ ပိုလွယ်သွားတတ်ပါတယ်။ ကိုယ့်ချည်းသီးခြားမဖြစ်ဘဲ အားလုံးနဲ့ ရောနှောသွားဖို့အတွက် ကိုယ်နဲ့ လက်ဗွေချင်းတူတဲ့ အခြားသူတွေရဲ့ “privacy pool” ကို ဝင်ရောက်ထားဖို့လိုပါတယ်။ အဲဒါကို အကောင်းဆုံးလုပ်နိုင်တဲ့ နည်းလမ်းကတော့ စက်တင်ကို ကိုယ့်အတွက်သီးခြား စက်တင်မလုပ်ဘဲ ဘရောက်ဇာ နံပါတ်တွေကို သူလိုကိုယ်လို တူအောင်လုပ်ထားတဲ့ ဘရောက်ဇာ တွေဖြစ်တဲ့ Tor browser, Brave သို့မဟုတ် Firefox တို့ကို ရွေးချယ်ဖို့ပါဘဲ။