EFF'S SURVEILLANCE SELF-DEFENSE

Metadata က ဘာကြောင့် အရေးပါတာလဲ

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

LOCALIZATION LAB

Metadata က ဘာကြောင့် အရေးပါတာလဲ

Last reviewed:
2015-08-10

ဒစ်ဂျစ်တယ်ဆက်သွယ်ရေးသဘောသဘာဝတွေမှာ metadata (အချက်အလက်အကြောင်းပြောပြတဲ့ အချက်အလက်) ဆိုတာကတော့ စာအိတ်သဘောနဲ့ တူပါတယ်။ ဆိုလိုတာက သင်ပို့လိုက်တာနဲ့ လက်ခံရရှိတဲ့ သတင်းအချက်အလက်တွေအကြောင်းပဲ ဖြစ်ပါတယ်။ အီးမေးလ်ရဲ့ အကြောင်းအရာ၊ စကားကြာကြာ ပြောထား၊ မပြောထားစတာနဲ့ ဆက်သွယ်နေတဲ့အချိန်မှာ သင့်ရဲ့ တည်နေရာ ပြီးတော့ ဘယ်သူနဲ့ ဆိုတာတွေက metadata အမျိုးအစားတွေပဲ ဖြစ်ပါတယ်။ Metadata ကို သင်ဆက်သွယ်တဲ့အခါမှာ ဘာအကြောင်းအရာပြောတယ်ဆိုတာကလွဲလို့ ကျန်တဲ့ အချက်အလက်တွေအကုန်လုံးလို့လည်း ပြောကြလေ့ရှိပါတယ်။

သမိုင်းကြောင်းအရတော့ U.S. အပါအဝင် တစ်ချို့နိုင်ငံတွေမှာ တစ်ယောက်နဲ့တစ်ယောက် ဆက်သွယ်တဲ့အကြောင်းအရာတွေအပေါ် ကာကွယ်ပေးမှုထက် metadata တွေကို ကာကွယ်ပေးတာက တော်တော်ကို နည်းပါတယ်။ ဥပမာပြောရရင် သင် ဘယ်သူတွေနဲ့ ဘာအကြောင်းအရာတွေ ပြောတယ်ဆိုတဲ့ အသေးစိတ်ကို ကြားဖြတ်နားထောင်ဖို့ စီစဉ်တာထက် သင် ဘယ်သူတွေနဲ့ ဖုန်းပြောထားတယ်ဆိုတဲ့ စာရင်းကို ရဲတွေက ပိုပြီးလွယ်လွယ်ကူကူ ရနိုင်ပါတယ်။

ဒီ metadata တွေကို စုဆောင်းတာ ဒါမှမဟုတ် တောင်းတဲ့ သူတွေဖြစ်တဲ့ အစိုးရတို့ ဆက်သွယ်ရေးဆိုင်ရာ ကုမ္ပဏီတွေကတော့ metadata ကို ထုတ်ဖော်တာ၊ စုဆောင်းတာဟာ သိပ်ပြီး ပြဿနာမရှိပါဘူးလို့ ငြင်းကြလေ့ရှိပါတယ်။ ဒါပေမယ့်လည်း အဲဒီလို ငြင်းချက်တွေက မမှန်ပါဘူး။ Metadata သေးသေးမွှားမွှားလေးကတောင်မှ သင့်ဘဝရဲ့ အတွင်းကျကျကိစ္စရပ်တွေကို သူများသိသွားအောင် ထုတ်ဖော်နိုင်ပါတယ်။ metadata တွေကို စုဆောင်းတဲ့ အစိုးရနဲ့ ကုမ္ပဏီတွေက metadata တွေကို သုံးပြီး ဘယ်လောက်တောင် ထင်သာမြင်သာရှိစေတယ်ဆိုတာကို တစ်ချက်ကြည့်လိုက်ကြရအောင်။

- သူတို့က မနက် ၂ နာရီ ၂၄ မိနစ်မှာ သင် လိင်ကျန်းမာရေးကိစ္စ တိုင်ပင်ဆွေးနွေးပေးတဲ့ ဖုန်းကို ဆက်ပြီး ၁၈ မိနစ်လောက် စကားပြောခဲ့တယ်ဆိုတာကို သူတို့ သိတယ်။ ဒါပေမယ့် သင် ဘာအကြောင်းတွေ ပြောတယ်ဆိုတာကိုတော့ မသိဘူး။
- သူတို့က မိမိကိုယ်ကို သတ်သေမှုတားဆီးပေးတဲ့ ဖုန်းကို ဆက်တယ်ဆိုတာ သူတို့ သိတယ်။ ဖုန်းပြောတဲ့ အတောအတွင်း ဘာတွေ ပြောတယ်ဆိုတာကိုတော့ မသိဘူး။
- HIV စစ်ပေးတဲ့ ဝန်ဆောင်မှုကနေ အီးမေးလ်တစ်စောင်ကို သင် လက်ခံရရှိတယ်၊ ပြီးတော့ သင့်ဆရာဝန်ကို ဖုန်းခေါ်တယ်၊ နောက်ကျတော့ HIV ရှိသူတွေကို အကူအညီပေးတဲ့ ဝဘ်ဆိုဒ်ကို နာရီပိုင်းအတွင်း ဝင်တယ်ဆိုတာကို သူတို့ သိတယ်။ ဒါပေမယ့် အီးမေးလ်မှာ ဘာအကြောင်းအရာတွေ ပါပြီး ဖုန်းထဲမှာ ဘာတွေ ပြောတယ်ဆိုတာကိုတော့ မသိဘူး။

- “ပုဂ္ဂလိကဆိုင်ရာ လွတ်လပ်လုံခြုံခွင့်ဥပဒေကို တားဆီးဖို့အတွက် ၅၂ နာရီပဲ ကျန်တော့တယ်" ဆိုတဲ့ အကြောင်းအရာနဲ့ အီးမေးလ်တစ်စောင်ကို ဒစ်ဂျစ်တယ်အခွင့်အရေး လှုပ်ရှားသူတွေကနေ သင် လက်ခံရရှိတယ်ဆိုတာကို သူတို့သိတယ်။ ဒါပေမယ့် အီးမေးလ်ထဲမှာ ပါတဲ့ အကြောင်းအရာတွေကိုတော့ မသိဘူး။
- သင် သားဖွားမီးယပ်ဆရာဝန်တစ်ယောက်နဲ့ ဖုန်းပြောတာ နာရီဝက်လောက် ကြာတယ်၊ ပြီးတော့ ကလေးဖျက်ချပေးတဲ့ ဆေးခန်းရဲ့ ဖုန်းနံပါတ်ကို အွန်လိုင်းမှာ ရှာတယ်ဆိုတာကို သူတို့ သိတယ်။ ဒါပေမယ့် ဘာတွေပြောတယ်ဆိုတာကို မသိဘူး။

နည်းပညာအားဖြင့်တော့ metadata ကို ပြင်ပကနေ ရယူစုဆောင်းတာကို ကာကွယ်ဖို့ဆိုတာ ခက်ခဲပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ သင့်ရဲ့ ဆက်သွယ်ရေးတွေ အောင်မြင်ဖို့အတွက် metadata ကို တခြားပါဝင်ပတ်သက်သူ (third parties) တွေက ရယူနိုင်ဖို့ လိုအပ်လို့ပါပဲ။ စာအိတ်ပေါ်က လိပ်စာကို အပြင်လူဖြစ်တဲ့ စာပို့သမားက ဖတ်နိုင်မှ စာကို လိပ်စာအမှန်ကို ပို့ပေးနိုင်တာလိုမျိုး ဒစ်ဂျစ်တယ် ဆက်သွယ်ရေးတွေမှာလည်း ဂိတ်စနဲ့ ဂိတ်ဆုံးကို အမှတ်အသားလုပ်လိုက်ပေးဖို့ လိုပါတယ်။ သင် ဖုန်းခေါ်တဲ့အခါမှာ ချိတ်ပေးနိုင်ဖို့အတွက် မိုဘိုင်းကုမ္ပဏီတွေက သင့်ဖုန်း ဘယ်မှာ ရှိနေတယ်ဆိုတာ အကြမ်းဖျင်း သိဖို့တော့ လိုပါတယ်။

Tor၊ စမ်းသပ်နေဆဲ ပရောဂျက်ဖြစ်တဲ့ Ricochet တို့လိုမျိုး ဝန်ဆောင်မှုတွေက အွန်လိုင်းဆက်သွယ်ရေး သာမန်နည်းလမ်းတွေမှာ ထုတ်လုပ်လိုက်တဲ့ metadata တွေရဲ့ ပမာဏကို အတတ်နိုင်ဆုံး လျှော့ချပေးဖို့ ရည်ရွယ်ပါတယ်။ metadata တွေကို ကာကွယ်ဖို့အတွက် ကောင်းမွန်တဲ့ ဥပဒေတွေ မပြဋ္ဌာန်းရသေးခင်နဲ့ metadata ထုတ်လုပ်တဲ့ ပမာဏကို လျှော့ချပေးနိုင်တဲ့ နည်းပညာတွေကို ကျယ်ကျယ်ပြန့်ပြန့် အသုံးမပြုလာသေတဲ့အချိန်မှာ သင် အကောင်းဆုံး လုပ်နိုင်တာကတော့ ဆက်သွယ်တဲ့အခါမှာ ဘာ metadata တွေကို သင်က ထုတ်လုပ်နေတယ်ဆိုတာကို သတိထားပြီး ဘယ်သူတွေက သတင်းအချက်အလက်တွေကို ရယူနိုင်နေပြီး ဘယ်လိုမျိုး အသုံးချခံရနိုင်တယ်ဆိုတာကို သတိထားဖို့ လိုအပ်ပါတယ်။