EFF'S SURVEILLANCE SELF-DEFENSE

একটি প্রতিবাদে যোগদান

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

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

এখন, জনগণের আগের যেকোনো সময়ের চেয়ে অধিক পরিমাণে, ক্ষমতাধরদের জবাবদিহি করতে এবং প্রতিবাদের মাধ্যমে অন্যদের অনুপ্রাণিত করার সক্ষমতা থাকতে হবে।

আপনার ইলেকট্রনিক ডিভাইস এবং ডিজিটাল সম্পদগুলোকে প্রতিবাদের আগে, চলাকালীন এবং পরে সুরক্ষিত রাখা অত্যন্ত গুরুত্বপূর্ণ, যাতে আপনি নিজেকে এবং আপনার তথ্য সুরক্ষিত রাখতে পারেন, পাশাপাশি আপনার বার্তা ছড়িয়ে দিতে পারেন। চুরি, ক্ষতি, জব্দ, বা জোরপূর্বক মিডিয়া মুছে ফেলা আপনার মত প্রকাশ করার সক্ষমতাকে ব্যাহত করতে পারে। একই সাথে, প্রতিবাদে অংশগ্রহণকারীরা তল্লাশি, গ্রেপ্তার বা তাদের চলাচল ও সংযোগ পর্যবেক্ষণের শিকার হতে পারেন।

মনে রাখবেন, এই পরামর্শগুলো সাধারণ ডেটা সুরক্ষার জন্য প্রস্তাবনা মাত্র এবং এটি আইনি পরামর্শ বা উপদেশ নয়। আপনার যদি নির্দিষ্ট আইনি উদ্বেগ থাকে, তাহলে একজন লাইসেন্সপ্রাপ্ত আইনজীবীর পরামর্শ নিন।

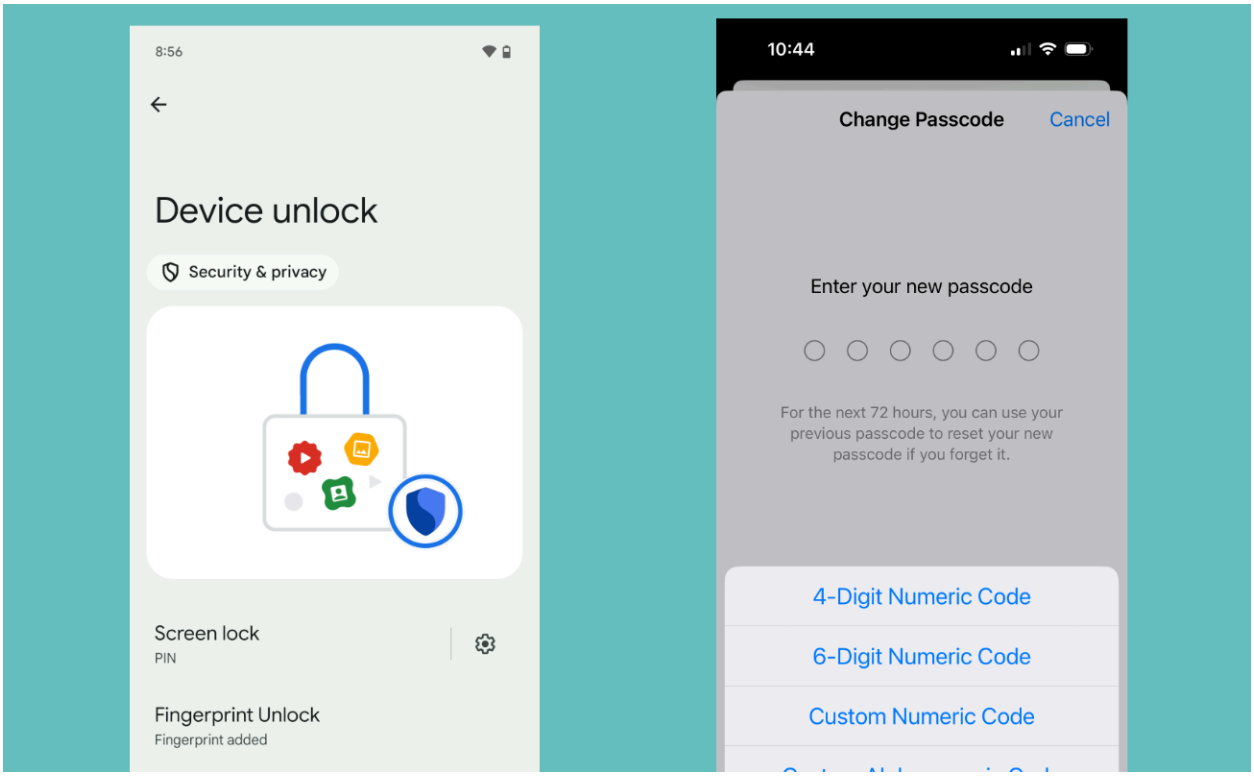
প্রতিবাদের আগে

আপনার ডিভাইসে শক্তিশালী এনক্রিপশন সক্রিয় করুন

ফুল-ডিস্ক এবং ফাইল-ভিত্তিক এনক্রিপশন ডিভাইস এনক্রিপশনের দুটি ধরণ, যা নিশ্চিত করে যে আপনার ডিভাইসের সমস্ত ফাইল অন্য কেউ অ্যাক্সেস করতে পারবে না। এগুলো এমন ধরনের এনক্রিপশন যা সংরক্ষিত ডেটা রক্ষা করে—যা "ইন-ট্রানজিট এনক্রিপশন" থেকে ভিন্ন, যা ইন্টারনেটের মাধ্যমে স্থানান্তরিত ডেটা রক্ষা করে। ফুল-ডিস্ক এবং ফাইল-ভিত্তিক এনক্রিপশন আপনার টেক্সট মেসেজের লোকাল ডেটাবেস থেকে শুরু করে ব্রাউজারে সংরক্ষিত পাসওয়ার্ড পর্যন্ত সবকিছু সুরক্ষিত রাখতে পারে। যদি আপনার ডিভাইস পুলিশ জব্দ করে, হারিয়ে যায়, বা চুরি হয়, তাহলে ডিভাইস এনক্রিপশন ডিভাইসে সংরক্ষিত ডেটা রক্ষায় সহায়ক হতে পারে। প্রতিবাদের পরিস্থিতি পূর্বানুমান করা কঠিন, তাই ফোন হারিয়ে ফেলার ঝুঁকিও অমূলক নয়।

iOS এবং বেশিরভাগ অ্যান্ড্রয়েড ডিভাইসে বিল্ট-ইন ডিভাইস এনক্রিপশন ক্ষমতা রয়েছে। এগুলো একটি শক্তিশালী পাসওয়ার্ড দ্বারা সুরক্ষিত হওয়া উচিত: ৮-১২টি এলোমেলো অক্ষরের সংমিশ্রণ যা সহজে মনে রাখা এবং ডিভাইস আনলক করার সময় টাইপ করা যায়। যদি ডিভাইস শক্তিশালী পাসওয়ার্ড দ্বারা সুরক্ষিত না হয়, তাহলে এই এনক্রিপশন ব্রুট-ফোর্স আক্রমণের মাধ্যমে সহজে ভেঙে ফেলা যেতে পারে। iPhone 5s এবং পরবর্তী মডেলগুলো, পাশাপাশি অনেক অ্যান্ড্রয়েড ডিভাইসে এই ধরনের আক্রমণ থেকে রক্ষা করার জন্য বিশেষ হার্ডওয়্যার থাকে। তবে এই সুরক্ষা বাইপাস করার পদ্ধতিও ক্রমাগত উন্নত হচ্ছে, তাই একটি জটিল ও শক্তিশালী পাসওয়ার্ড ব্যবহার করাই সর্বোত্তম। আপনার পাসকোড সক্রিয় বা পরিবর্তন করতে:

- **iPhone-**এ: সেটিংস খুলুন **>** ফেস আইডি এবং পাসকোড > এরপর পাসকোড চালু করুন অথবা পাসকোড পরিবর্তন করুন-এ ট্যাপ করুন > তারপর পাসকোড অপশনস-এ ট্যাপ করুন এবং আপনার পছন্দ অনুযায়ী পাসকোডের ধরণ বা দৈর্ঘ্য নির্বাচন করুন।
- অ্যান্ড্রয়েডে: সেটিংস খুলুন > সিকিউরিটি ও প্রাইভেসি > ডিভাইস আনলক > স্ক্রিন লক -এ যান এবং আপনার পছন্দ অনুযায়ী পাসকোডের ধরণ বা দৈর্ঘ্য নির্বাচন করুন।



পাসকোড সক্রিয়করণ প্রক্রিয়া অ্যান্ড্রয়েড (বামে) এবং আইফোন (ডানে)

আপনার ডিভাইস এনক্রিপ্ট করলেও সম্ভবত এটি এক্সটারনাল স্টোরেজ মিডিয়া, যেমন SD কার্ড বা ফ্ল্যাশ মেমোরি কার্ড এনক্রিপ্ট করবে না। এগুলো আলাদাভাবে এনক্রিপ্ট করতে হবে, এবং কখনও কখনও এগুলো এনক্রিপ্ট করা সম্ভব নাও হতে পারে। আপনার ডিভাইসে ফাইল কোথায় সংরক্ষিত হচ্ছে তা জানার জন্য একটি ফাইল ব্রাউজিং অ্যাপ ব্যবহার করতে পারেন, অথবা সম্পূর্ণভাবে এক্সটারনাল স্টোরেজ মিডিয়া বাদ দিতে পারেন।

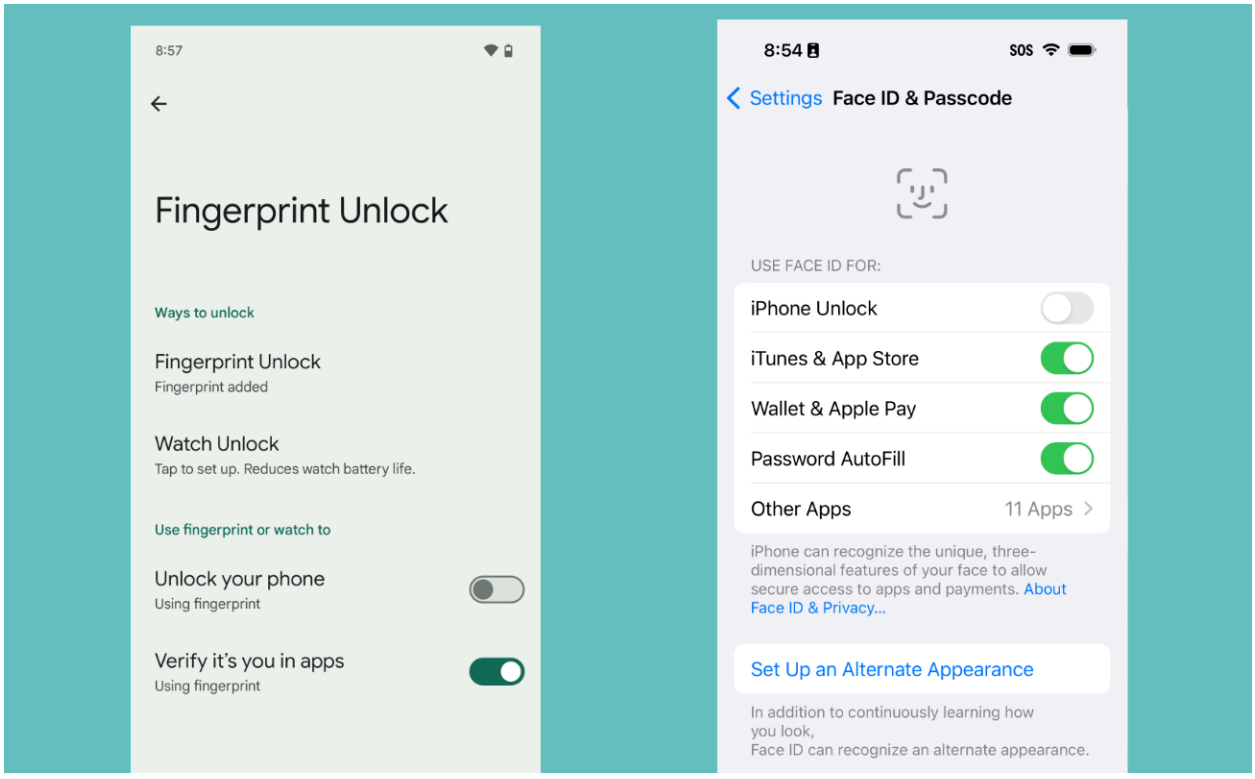
এছাড়াও, অনেক ডিজিটাল ক্যামেরায় এনক্রিপ্ট করার সক্ষমতা থাকে না। ধরে নেওয়াই নিরাপদ যে ডিজিটাল ক্যামেরায় তোলা ছবি এবং ভিডিওগুলো এনক্রিপ্ট করা থাকবে না, যদি না এটি স্পষ্টভাবে উল্লেখ করা থাকে।

ফিঙ্গারপ্রিন্ট বা ফেস আনলক বাতিল করুন

আপনার ফোন মডেলের উপর নির্ভর করে, iOS এবং Android উভয়ই ব্যবহারকারীদের ফিঙ্গারপ্রিন্ট বা ফেস রিকগনিশন ব্যবহার করে তাদের ডিভাইস আনলক (এবং ডিক্রিপ্ট) করার সুবিধা দেয়। যদিও এই সেটিংসগুলো ডিভাইস এনক্রিপশনের সুবিধা সহজভাবে উপভোগ করার জন্য আকর্ষণীয় মনে হলেও এগুলো সক্রিয় থাকলে কেউ আপনাকে বাধ্য করতে পারে আপনার ফিঙ্গারপ্রিন্ট বা চেহারা ব্যবহার করে ডিভাইসটি আনলক করতে। বিশেষত প্রতিবাদের পরিস্থিতিতে, বা এমন কোনো পরিস্থিতিতে যেখানে আপনার ফোন অনুসন্ধানের জন্য সরকারি হস্তক্ষেপের সম্ভাবনা বেশি (যেমন সীমান্ত অতিক্রম করার সময়), আমরা পরামর্শ দিই এই কার্যকারিতা বন্ধ করে রাখতে।

বাংলাদেশের প্রেক্ষাপটে, ফিঙ্গারপ্রিন্ট বা ফেস আনলক ব্যবহার ঠিক ততটাই ঝুঁকিপূর্ণ যতটা পাসওয়ার্ড ব্যবহার করলে হতে পারে। তবে আপনি পাসওয়ার্ড ব্যবহার করলে সেটি আপনি না বলা অব্দি তারা আপনার ডিভাইসে প্রবেশ করতে পারবে না। যদিও ইলেকট্রনিক ফ্রন্টিয়ার ফাউন্ডেশন মানুষকে তাদের ডিভাইস ডিক্রিপ্ট করতে বাধ্য করার বিরুদ্ধে আইনগত সুরক্ষাকে শক্তিশালী করার জন্য লড়াই চালিয়ে যাচ্ছে, বর্তমানে ফেস এবং ফিঙ্গারপ্রিন্ট দিয়ে আনলক করার ক্ষেত্রে বাধ্য করার বিরুদ্ধে সুরক্ষা পাসওয়ার্ড প্রকাশের ক্ষেত্রে বাধ্য করার বিরুদ্ধে সুরক্ষার চেয়ে কম।

- আইফোনে বায়োমেট্রিক আইডি নিষ্ক্রিয় করতে, ***Settings*** > ***Face (or Touch) ID & Passcode***এ যান এবং "iPhone Unlock" অপশনটি বন্ধ করুন, অথবা Reset Face ID অপশনে ট্যাপ করুন।
- অ্যান্ড্রয়েডে: বায়োমেট্রিকস নিষ্ক্রিয় করার প্রক্রিয়া আপনার ডিভাইস প্রস্তুতকারকের উপর নির্ভর করবে। অ্যান্ড্রয়েড ১৪ ভার্সনে চালিত পিক্সেল ডিভাইসের ক্ষেত্রে, ***Settings*** > ***Security & Privacy*** > ***Device Unlock > Fingerprint Unlock***এ যান এবং "Unlock your phone" অপশনটি বন্ধ করুন। যদি আপনার ফোন ভিন্ন প্রস্তুতকারকের হয়, তবে আপনার মডেলের নির্দিষ্ট নির্দেশনার জন্য অনলাইনে অনুসন্ধান করতে পারেন।



অ্যান্ড্রয়েড (বামে) এবং আইফোন (ডানে) এ বায়োমেট্রিক ফোন আনলক নিষ্ক্রিয় করা।

Signal ইনস্টল করা

[সিগন্যাল একটি নিরাপদে যোগাযোগের অ্যাপ, যা iOS এবং অ্যান্ড্রয়েড উভয় প্ল্যাটফর্মেই কাজ করে।](#) এটি শক্তিশালী এনক্রিপশন প্রদান করে, যা টেক্সট মেসেজ এবং ভয়েস কল উভয়কেই সুরক্ষিত রাখে। এই সুরক্ষার

ধরণটি "এন্ড-টু-এন্ড এনক্রিপশন" নামে পরিচিত, যা আপনার যোগাযোগের তথ্য আদান প্রদানের সময় নিরাপদ রাখে। অবশ্যই, অন্যান্য বিকল্পও আছে, তবে সেগুলোর কিছু সীমাবদ্ধতা রয়েছে। উদাহরণস্বরূপ, WhatsApp এন্ড-টু-এন্ড এনক্রিপ্টেড হলেও এটি সিগন্যালের তুলনায় বেশি মেটাডেটা সংগ্রহ করে। অ্যাপলের iMessages অ্যাপ এন্ড-টু-এন্ড এনক্রিপ্টেড, তবে কেবলমাত্র চ্যাটের সবাই যদি আইফোন ব্যবহার করে। সিগন্যাল সহজতম বিকল্প যা নিশ্চিত করে যে চ্যাটের সবাই ডিফল্টভাবে নিরাপদ।

একে অপরের সাথে যোগাযোগ এনক্রিপ্ট করার পাশাপাশি, সিগন্যাল এনক্রিপ্টেড গ্রুপ চ্যাটের সুবিধাও দেয়। এই অ্যাপ ব্যবহারকারীদের মেসেজ পড়ার পরে নির্দিষ্ট সময় অতিবাহিত হলে অদৃশ্য হয়ে যাওয়ার অপশন সেট করতে দেয়। স্ন্যাপচ্যাটের মতো অন্যান্য অ্যাপের সাথে তুলনা করলে, সিগন্যালের এই অস্থায়ী মেসেজগুলি কখনোই কোনো সার্ভারে সংরক্ষিত হয় না এবং অদৃশ্য হওয়ার পর আপনার ডিভাইস থেকেও মুছে ফেলা হয়।

২০১৬ সালে, ভার্জিনিয়ার ইস্টার্ন ডিস্ট্রিক্টের একটি গ্র্যান্ড জুরি সিগন্যাল অ্যাপের ডেভেলপার ওপেন উইস্পার সিস্টেমস-এর কাছে একটি সমন জারি করেছিল। সিগন্যালের আর্কিটেকচারের কারণে, যা কোম্পানির সার্ভারে ব্যবহারকারীর মেটাডেটা সংরক্ষণ সীমিত করে, তারা কেবলমাত্র "ব্যবহারকারী কখন সিগন্যালের জন্য রেজিস্টার করেছেন এবং সর্বশেষ কবে সিগন্যাল পরিষেবার সাথে সংযুক্ত হয়েছেন" এই তথ্য সরবরাহ করতে পেরেছিল। ২০২১ সালে একই ধরনের পরিস্থিতি ঘটেছিল, এবং ফলাফল একই রকম ছিল (দুইবার)।

প্রতিবাদে অংশগ্রহণকারীদের কখনও কখনও কিছু ছাড় দিতে হতে পারে। উদাহরণস্বরূপ, সিগন্যাল মেসেজ পাঠানোর একটি ভালো কারণ হতে পারে বন্ধুকে জানানো যে, আপনি প্রতিবাদে কী দেখছেন যাতে তারা অন্যদের সতর্ক করতে পারে বা গুরুত্বপূর্ণ ছবি এবং ভিডিও বন্ধুদের কাছে পাঠানো যাতে আপনার ফোন জব্দ করা হলে পরে সেই মিডিয়া পুনরুদ্ধার করা যায়। একইসঙ্গে, প্রতিপক্ষকে আপনার ফোন ব্যবহার করে প্রমাণ করতে বাধা দেওয়ার ভালো কারণ থাকতে পারে যে আপনি প্রতিবাদে উপস্থিত ছিলেন। এর জন্য ফোনের সংযোগ বিচ্ছিন্ন করা বা বাড়িতে রেখে যাওয়া প্রয়োজন, যেমনটি আমরা নিচে ব্যাখ্যা করেছি। দুর্ভাগ্যবশত, যদি আপনি একটি প্রতিবাদে অংশ নেন এবং সিগন্যাল ব্যবহার করার পাশাপাশি ফোনেও যোগাযোগ করেন, তবে ফোনের সংযোগ আপনার অবস্থান প্রকাশ করতে পারে।

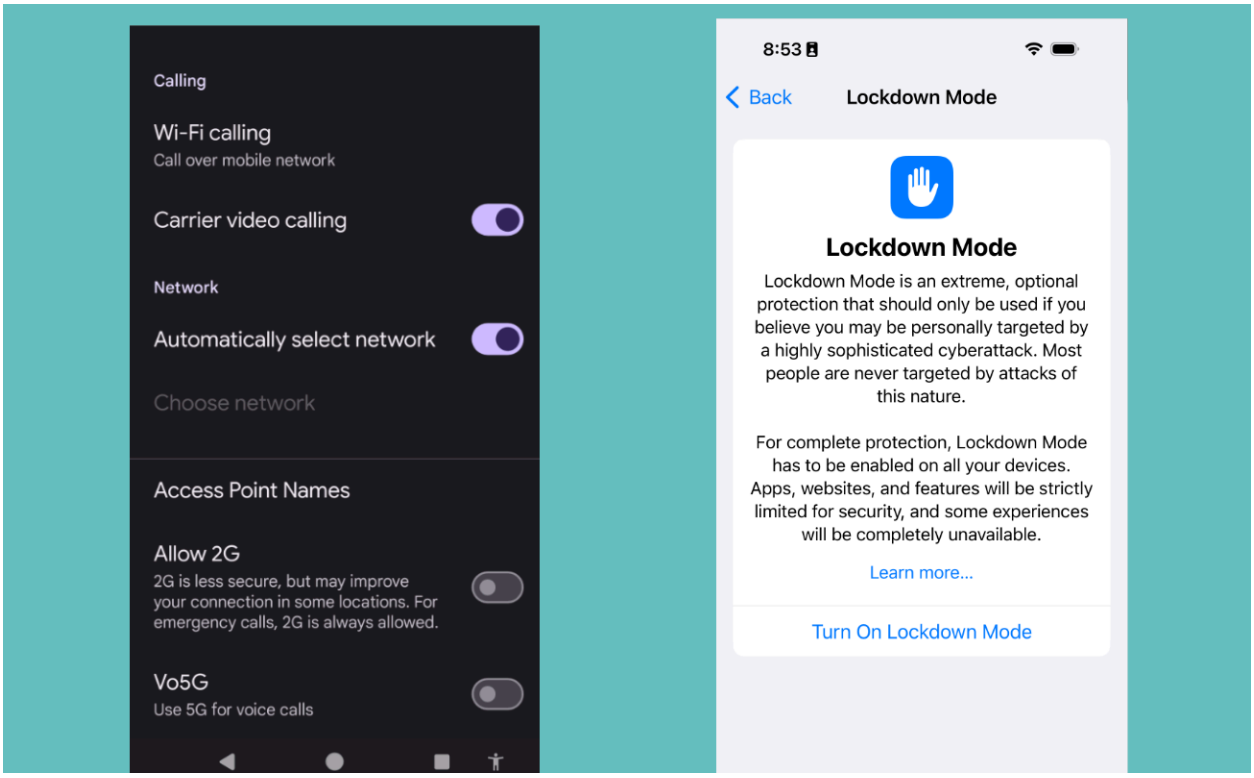
সেল-সাইট সিমুলেটর দ্বারা আপনার ফোন ট্র্যাক হওয়া প্রতিরোধ করুন

সেল-সাইট সিমুলেটর (CSS)—যা IMSI ক্যাচার এবং স্টিংরে নামেও পরিচিত— এমন একটি টুল যা আইন-শৃঙ্খলা বাহিনী এবং সরকার ফোনের অবস্থান ট্র্যাক করতে, যোগাযোগ বন্ধ বা ব্যাহত করতে, বিদেশি সরকারের ওপর গুপ্তচরবৃত্তি করতে, এমনকি ম্যালওয়্যার ইনস্টল করার জন্য ব্যবহার করে। CSS স্প্যাম পাঠানো এবং প্রতারণার জন্যও ব্যবহার করা যেতে পারে। CSS-এর একটি সাধারণ কৌশল হলো আপনার ফোনকে একটি নকল 2G সেল টাওয়ারে সংযুক্ত করতে প্রতারিত করা। আপনার ফোন যেন স্বয়ংক্রিয়ভাবে CSS-এর সঙ্গে সংযুক্ত না হয়, তার জন্য আপনি আপনার ফোনে 2G সংযোগ নিষ্ক্রিয় করতে পারেন।

- **iPhone-এ:** আপনাকে "Lockdown Mode" সক্রিয় করতে হবে, যা আপনার ফোনের একটি বিশেষ মোড এবং এটি তাদের জন্য ডিজাইন করা হয়েছে যারা স্পাইওয়্যার বা রাষ্ট্রীয় পর্যায়ের আক্রমণের শিকার হওয়ার বিষয়ে উদ্বিগ্ন। iOS 17 থেকে, এটি 2G মোডও নিষ্ক্রিয় করে। Lockdown Mode সক্রিয় করার পর এটি আপনার iPhone-এ বেশ কিছু ফিচার নিষ্ক্রিয় করবে, যেমন নির্দিষ্ট প্রকারের মেসেজ অ্যাটাচমেন্ট পাঠানো বা গ্রহণ করা (যেমন লোকেশন শেয়ার করা) এবং ইনকামিং FaceTime

কল ব্লক করা। আপনার ফোনে কী কী ফিচার বন্ধ হবে, সে সম্পর্কে আরও জানতে এখানে পড়তে পারেন।Lockdown Mode চালু করতে***: Settings >Privacy & Security > Lockdown Mode >*** Turn on Lockdown Mode অপশনে ট্যাপ করুন। প্রতিবাদ থেকে বাড়ি ফিরে আপনি চাইলে এই মোডটি বন্ধ করতে পারেন। একই নির্দেশনা অনুসরণ করে "Turn off Lockdown Mode" অপশনটি নির্বাচন করুন।

- **Android-**এ: আপনার অপারেটিং সিস্টেমের সংস্করণ, আপনার ফোনের প্রস্তুতকারক এবং আপনার ক্যারিয়ারের উপর নির্ভর করে, আপনি 2G নিষ্ক্রিয় করতে পারবেন, এনক্রিপ্টেড সেল সংযোগ ব্যবহার করতে বাধ্য করতে পারবেন, অথবা উভয়ই করতে পারবেন। এটি করতে: ***Settings > Network & Internet>*** SIMs [আপনার মোবাইল অপারেটরের নাম] "Allow 2G" অপশনটি খুঁজে বের করুন এবং এটি বন্ধ করে দিন, যাতে 2G সম্পূর্ণরূপে নিষ্ক্রিয় হয়ে যায়। আপনি যদি "Require Encryption" অপশনটি দেখতে পান, তবে এটি চালু করুন, যাতে আপনার ফোন টাওয়ার সংযোগের সময় "null cipher" ব্যবহার না করে ।যেহেতু মোবাইল কোম্পানির আর 2G নেটওয়ার্ক তেমন ব্যবহার করেনা, আপনি প্রতিবাদ শেষে এই সেটিংসগুলি যেমন ছিল তেমন রাখতে পারেন।



অ্যান্ড্রয়েডে 2G নিষ্ক্রিয় করা (বামে) এবং আইফোনে লকডাউন মোড সচল করা (ডানে)

আপনার ডেটা ব্যাকআপ রাখুন

আপনার ডিভাইসটি হারিয়ে গেলে, চুরি হয়ে গেলে, বা আইন প্রয়োগকারী কর্তৃপক্ষ কর্তৃক জব্দ করা হলে এর অ্যাক্সেস হারানোর সম্ভাব্য ক্ষতি সীমিত করতে সতর্কতা অবলম্বন করুন। আপনার ডেটা নিয়মিত ব্যাকআপ নিন এবং সেই ব্যাকআপটি একটি নিরাপদ স্থানে সংরক্ষণ করুন, যাতে পরবর্তীতে কোনও সমস্যার সম্মুখীন না

হন। যদি আপনি আপনার আইফোনের ব্যাকআপগুলি অনলাইনে সংরক্ষণ করেন, তবে আমরা দৃঢ়ভাবে পরামর্শ দিচ্ছি যে ঐচ্ছিক অ্যাডভান্সড ডেটা প্রোটেকশন অপশন সচল করুন, যা আইক্লাউডে সংরক্ষিত বেশিরভাগ ডেটার জন্য এন্ড-টু-এন্ড এনক্রিপশন চালু করে। অ্যান্ড্রয়েডের জন্য, আমরা একটি অনলাইন ব্যাকআপ পরিষেবা বেছে নেওয়ার পরামর্শ দিচ্ছি যা (সাধারণত) "জিরো নলেজ" প্রদান করে, আপনার ডেটা এমনকি ব্যাকআপ পরিষেবা প্রদানকারী থেকেও রক্ষা করে (দ্রষ্টব্য, কিছু পরিষেবা এই অপশনের জন্য আলাদা নাম ব্যবহার করে)।

ভার্চুয়াল সিম, ডিসপোজেবল ফোন কিনুন

যুক্তরাষ্ট্রে, ফেডারেল নিয়ম অনুযায়ী, আপনাকে প্রিপেইড সিম কার্ডকেনার জন্য আপনার আইডি প্রদর্শন করার প্রয়োজন নেই (কিন্তু আপনার দেশে এটি আবশ্যক হতে পারে)। বেশিরভাগ দেশে প্রিপেইড সিম কার্ড কেনার জন্য একটি আইডি প্রদানের প্রয়োজন হয়, যার মাধ্যমে সিম কার্ডটি আপনার পরিচয়পত্রের সাথে সংযুক্ত হয় এবং গোপনীয়তা অসম্ভব হয়ে পড়ে।

যদি আপনি আপনার ডিভাইসে সংরক্ষিত ডেটার সুরক্ষা নিয়ে উদ্বিগ্ন থাকেন, তাহলে সেটি প্রতিবাদস্থানে নিয়ে যাবেন না। তার পরিবর্তে, একটি প্রিপেইড মোবাইল ফোনঅথবা ভার্চুয়াল সিম এবং সাময়িক ডিভাইস কিনুন। আপনার বন্ধুদের আপনার অস্থায়ী নম্বরটি জানিয়ে দিন, এবং এটি ব্যবহার করে কার্যক্রম সমন্বয় করুন।

মনে রাখবেন যে, মোবাইল ডিভাইসগুলির অবস্থান তাদের সংযুক্ত সেল টাওয়ার দ্বারা নির্ধারিত হতে পারে। সুতরাং, যদি আপনি আপনার পরিচয় এবং অবস্থান জানাতে না চান, তবে বাড়ি ফিরে যাওয়ার আগে বা যেকোনো জায়গায় যাওয়ার আগে আপনার ডিভাইসটি বন্ধ করে দিন যা আপনার পরিচয় প্রকাশ করতে পারে। যেমনটি আমরা নীচে ব্যাখ্যা করেছি, আপনি আপনার ফোনের সেটিংস পরিবর্তন করতে পারেন যাতে সংযোগ বন্ধ হয় এবং এর ফলে অবস্থান ট্র্যাকিং ব্লক হয়ে যায়।

ফোনটি ব্যবহার শেষ হলে, এটি নিরাপদে ধ্বংস করতে পারেন বা এমন একটি স্থানে ফেলে দিতে পারেন যা আপনার সাথে সম্পর্কিত নয়। মনে রাখবেন, যদি আপনি আপনার নিয়মিত ডিভাইস এবং সাময়িক ডিভাইস উভয়ই সঙ্গে নিয়ে যান, তবে এই ডিভাইসগুলির অবস্থান প্রকাশ পেতে পারে এবং এটি আপনার গোপনীয়তা বিপন্ন করতে পারে।

গোপনীয়তা এবং নিরাপত্তার জন্য পোশাক পরা

বহু আইন প্রয়োগকারী সংস্থার কাছে এমন উন্নত পর্যবেক্ষণ প্রযুক্তি রয়েছে, যা প্রতিবাদে অংশগ্রহণকারীদের চিহ্নিত করতে ব্যবহার করা যেতে পারে। নিজের সুরক্ষা রক্ষার জন্য, আপনার গোপনীয়তা বজায় রাখতে এবং শারীরিক নিরাপত্তা সুরক্ষিত রাখতে উপযুক্ত পোশাক পরা গুরুত্বপূর্ণ।

আপনার দলের সবাই যেভাবে পোশাক পরবে, সেই একই পোশাক পরা আপনার পরিচয় লুকিয়ে রাখতে সাহায্য করতে পারে। প্রতিবাদ চলাকালে এবং পরে আপনাকে চিহ্নিত ও ট্র্যাক করা থেকে রোধ করতে পারে। কালো, একরঙা পোশাক পরলে আপনি ভিড়ের মধ্যে মিশে যেতে পারবেন। তবে মনে রাখতে হবে যে অন্ধকারে গাড়ি চালকের কাছে আপনি তেমন দৃশ্যমান নাও হতে পারেন, তাই রাস্তা পার হওয়ার সময় বা চলমান যানবাহনের কাছাকাছি হাঁটার সময় অতিরিক্ত সতর্কতা অবলম্বন করা উচিত।

যদি আপনার চোখে পড়ার মতো ট্যাটু বা উজ্জ্বল অস্বাভাবিক চুলের রঙ থাকে, তবে সেগুলো ঢেকে রাখুন। ট্যাটু দেখে আপনাকে চিহ্নিত করা যেতে পারে, এবং সেগুলো ট্যাটু চেনার ডেটাবেসে যোগ করা হতে পারে। কালো একরঙা টুপি, স্কার্ফ, দস্তানা, লম্বা হাতা এবং পূর্ণ দৈর্ঘ্যের পোশাক এসব চিহ্নিতকরণ বৈশিষ্ট্যগুলো ঢেকে রাখতে সাহায্য করবে, যাতে আপনি ভিড়ের মধ্যে সহজেই মিশে যেতে পারেন।

প্রতিবাদ চলাকালীন

আপনার ডিভাইস আনলক না করেই ছবি এবং ভিডিও তুলুন।

সঠিক ছবি তোলার জন্য আপনার প্রস্তুত থাকা জরুরী, এবং একটি ভালো ছবি আপনার উদ্দেশ্যকে সহায়তা করতে পারে। যদি আপনার একটি ডিজিটাল ক্যামেরা থাকে, এমনকি একটি সস্তা পয়েন্ট-এন্ড-শুট ক্যামেরাও, তা ছবি তোলার জন্য সেরা অপশন হতে পারে। তবে আপনার ফোনও একই কাজ করতে পারে। যদি আপনি একটি শক্তিশালী পাসওয়ার্ড সেট করে থাকেন, তবে ডিভাইসে প্রবেশ করতে বেশ সময় লাগবে, এবং আপনি ছবি তোলার জন্য গুরুত্বপূর্ণ মুহূর্তটি হারিয়ে ফেলতে পারেন। সৌভাগ্যবশত, iOS এবং Android আপনাকে আপনার ডিভাইস আনলক না করেই ছবি এবং ভিডিও তোলার সুযোগ দেয়।

- অ্যান্ড্রয়েড পিক্সেল ডিভাইসে, পাওয়ার বাটনে দুটি দ্রুত প্রেস করুন।
- আইফোনের লক স্ক্রিন থেকে, ক্যামেরা আইকনে জোরে প্রেস করুন বা স্ক্রিন বাম পাশে সোয়াইপ করুন। পুরানো আইফোন মডেলগুলিতে আপনাকে উপরে সোয়াইপ করতে হবে।

আপনার ফটো এবং ভিডিওগুলিতে অন্য প্রতিবাদকারীদের চেহারার বিষয়ে সচেতন থাকুন।

যদি আপনি প্রতিবাদে অংশগ্রহণকারী বা সাধারণ মানুষের ছবি বা ভিডিও তুলে থাকেন, তাহলে আপনি যা পোস্ট করছেন সে সম্পর্কে সচেতন থাকুন। যদি আপনি অনলাইনে এমন ছবি পোস্ট করেন যেখানে প্রতিবাদকারী বা দর্শকদের মুখ চিহ্নিত করা যায়, তাহলে আইন প্রয়োগকারী সংস্থা বা স্বেচ্ছাসেবকরা তাদের শনাক্ত করে আটক বা হয়রানি করতে পারে। ছবির মধ্যে থাকা সকলের মুখ ঢাকা বা আড়াল করুন। এটি করার জন্য কয়েকটি উপায় রয়েছে:

- আপনি ডিফল্ট Android বা iOS ফটো এডিটিং অ্যাপে ছবি সম্পাদনা করতে পারেন। নিশ্চিত হয়ে নিন যে, আপনি অন্য কোনো চিহ্নিত বৈশিষ্ট্য যেমন ট্যাটু বা বিশেষ পোশাক ব্লক বা ব্লার করেছেন (ব্লার করা ছবি ক্ষেত্রবিশেষ উদ্ধার করা যেতে পারে, তাই ব্লক করার বিকল্প থাকলে সেটি ব্যবহার করা ভালো)।
- যদি আপনি Signal ব্যবহার করেন, তাহলে এই অ্যাপে একটি ব্লারিং টুল রয়েছে। আপনি সহজেই ("Note to Self" নামে পরিচিত) একটি মেসেজ কনভার্সেশন তৈরি করতে পারেন, যার মাধ্যমে আপনি ছবি আপনার ফোনে সেভ করে শেয়ার করার জন্য তৈরি করতে পারবেন।
- Image Scrubberএকটি অনলাইন টুল যা মোবাইল বা ডেস্কটপ ডিভাইসে ব্যবহার করা যেতে পারে, ফেস ব্লার বা ব্লক আউট করার জন্য।

ছবি থেকে মেটাডেটা মুছে ফেলুন

যখন আপনি আপনার ছবি পোস্ট করতে চান, তখন আপনার উচিৎ ছবির ফাইলের মধ্যে থাকা মেটাডেটা মুছে ফেলা, যাতে আপনি ব্যক্তিগতভাবে পরিচয় শনাক্তকরণ তথ্য ফাঁস না করেন। ছবির মেটাডেটা নানা তথ্য ধারণ করতে পারে। যেমন ছবিটি যেই ক্যামেরা দিয়ে তোলা হয়েছে তার মডেল, ছবিটি তোলার সঠিক সময় এবং স্থান, এবং এমনকি আপনার নামও। এটি করার জন্য বেশ কিছু পন্থা রয়েছে:

- মুল ছবি থেকে যেকোনো মেটাডেটা মুছে ফেলতে, আপনি ছবিটি একটি ডেস্কটপ কম্পিউটারে ট্রান্সফার করতে পারেন, তারপর ছবিটির স্ক্রীনশট নিয়ে সেটি পোস্ট করতে পারেন, যাতে মূল ছবিটি পরিবর্তে স্ক্রীনশটটি শেয়ার হয়।
- আপনি আপনার মোবাইল ডিভাইসে ছবির স্ক্রীনশট নিয়ে মেটাডেটা মুছে ফেলতে পারেন, তবে এতে ছবির গুণগত মান হয়তো তেমন ভালো নাও হতে পারে। এরপর আপনি মূল ছবির পরিবর্তে সেই স্ক্রীনশটটি পোস্ট করতে পারেন।
- আপনি সিগন্যাল অ্যাপে ছবিটির একটি কপি নিজেকে পাঠাতে পারেন (যা ছবি পাঠানোর সময় মেটাডেটা মুছে ফেলে), তারপর পাঠানো ছবিটি ডাউনলোড করে পোস্ট করতে পারেন।

প্রতিবাদে যাওয়া এবং ফিরে আসার সময় যেসব বিষয় মনে রাখতে হবে

গাড়ি চালানোর সতর্কতা

অটোমেটেড লাইসেন্স প্লেট রিডার সিস্টেম (ALPRs) স্বয়ংক্রিয়ভাবে গাড়ির লাইসেন্স প্লেট রেকর্ড করে, এর সাথে সময়, তারিখ এবং স্থানও রেকর্ড করা হয়। এই প্রযুক্তিটি সাধারণত মার্কিন যুক্তরাষ্ট্রসহ অনেক দেশে আইন প্রয়োগকারী সংস্থা ব্যবহার করে, অথবা ভিজিলান্ট এবং MVTrac এর মতো বেসরকারি কোম্পানিগুলি ব্যবহার করে, যারা পরে আইন প্রয়োগকারী সংস্থা এবং অন্যান্য প্রতিষ্ঠানের সাথে লাইসেন্স প্লেটের তথ্য শেয়ার করে। বিশাল ডেটাবেসে জমা থাকা এই তথ্য সাধারণত দীর্ঘ সময়ের জন্য সংরক্ষিত থাকে। মূলত, আপনার নামে নিবন্ধিত যেকোনো গাড়ির ড্রাইভিং ইতিহাসের উপর ভিত্তি করে আপনার অবস্থান ট্র্যাক করা যেতে পারে,এবং কিভাবে এই ডেটা সংগ্রহ, অ্যাক্সেস, শেয়ার এবং সংরক্ষিত হবে তা নিয়ে খুব কম আইনগত সীমাবদ্ধতা থাকে।

গণপরিবহনে সতর্কতা

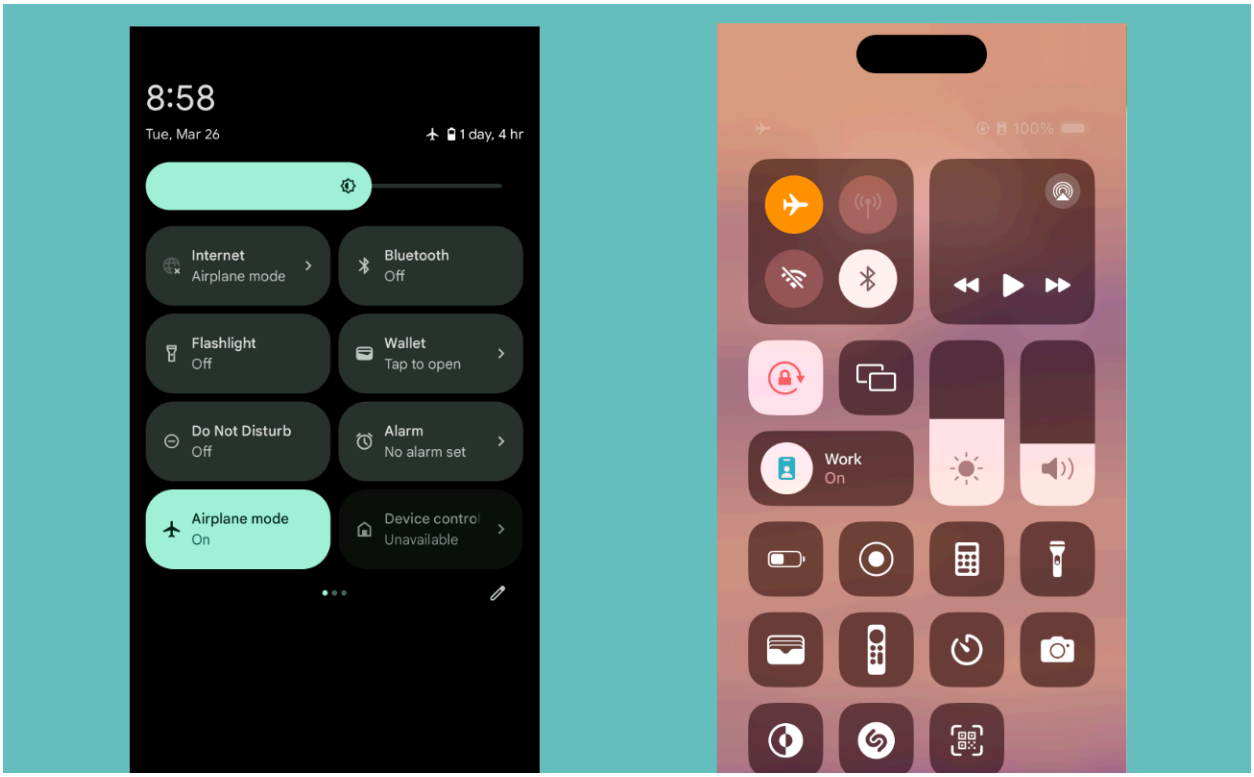
গণপরিবহন ব্যবহার করে প্রতিবাদস্থলে যাওয়া এবং ফিরে আসার সময় সতর্ক থাকুন। যদি আপনি এমন পেমেন্ট পদ্ধতি বা ট্রানজিট কার্ড ব্যবহার করেন যা আপনার পরিচয়ের সাথে যুক্ত থাকে, তবে আইন প্রয়োগকারী সংস্থাগুলি হয়তো আপনি প্রতিবাদে অংশগ্রহণ করেছিলেন এবং আপনার গতিবিধি ট্র্যাক করতে সক্ষম হবে। যদি আপনি চান যে আপনার গতিবিধি গোপন থাকবে তাহলে সম্ভব হলে নগদ টাকা ব্যবহার করুন, অথবা অন্য কোন পাবলিক ট্রান্সপোর্টেশন ব্যবহারের কথা ভাবুন।

যদি সম্ভব হয়, প্রতিবাদস্থলে যাওয়া এবং ফিরে আসার জন্য সাইকেল চালানো বা হাঁটা বিবেচনা করুন, যাতে এই ধরনের নজরদারি ঝুঁকি থেকে আপনার সম্মুখীন হবার সম্ভাবনা কমানো যায়।

ফোনের সেটিংস পরিবর্তন করুন

আপনার ফোনের মাধ্যমে কারো আপনার অবস্থান ট্র্যাক করার ঝুঁকি কমাতে, এর কিছু ফিচার বন্ধ করার কথা বিবেচনা করুন:

- আইফোনে: Settings খুলুন এবং "Airplane Mode" চালু করুন। এরপর, ***Wi-Fi*** এ ট্যাপ করুনএবং এটি বন্ধ করুন, আবার ***Settings*** এ ফিরে গিয়ে ***Bluetooth*** বন্ধ করুন। আবার ***Settings*** পৃষ্ঠায় ফিরে গিয়ে ***Privacy & Security*** > ***Location Services*** এ গিয়ে Location সেবা বন্ধ করুন। আপনি চাইলে Settings > Privacy & Security > Location Services > System Services (নিচে) > Significant Locations এ গিয়ে এটি বন্ধ করতে পারেন।
- অ্যান্ড্রয়েডে: স্ক্রিনের উপরের অংশ থেকে নিচে টেনে Notification Shade অ্যাক্সেস করুন। "Airplane Mode" এ ট্যাপ করুন এটি চালু করতে, তারপর "Internet" এ ট্যাপ করে "Wi-Fi" বন্ধ করুন। পরবর্তী, "Bluetooth" এ ট্যাপ করে এটি বন্ধ করুন। অবশেষে, Settings> Location এ গিয়ে "Use location" বন্ধ করুন। আপনার Google account এ গিয়ে Location History বন্ধ করুন। এটি নিশ্চিত করবে যে আপনার ডিভাইস প্রটেস্টের সময় পর্যন্ত কোন সিগন্যাল পাঠাচ্ছে না এবং আপনার অবস্থান ট্র্যাক হওয়া থেকে রক্ষা পাবে।



অ্যান্ড্রয়েডে এয়ারপ্লেন মোড চালু করা (বাঁ দিকে) এবং আইফোনে (ডান দিকে)।

তবে, এয়ারপ্লেন মোড চালু করা থাকেলে, লোকেশন সার্ভিস, Wi-Fi এবং ব্লুটুথ বন্ধ থাকেও অ্যাপসগুলি আপনার GPS লোকেশন সংরক্ষণ করতে পারে এবং পরবর্তীতে ইন্টারনেটের সাথে সংযুক্ত হলে তা প্রকাশ করতে পারে। এটি নিশ্চিত করার একমাত্র উপায় হল ফোনটি সম্পূর্ণরূপে বন্ধ করে দেওয়া।

এয়ারপ্লেন মোড চালু করা এবং Wi-Fi বন্ধ করলে আপনি আপনার বন্ধুদের মেসেজ বা কল করতে পারবেন না, তাই পরিকল্পনা অনুযায়ী প্রস্তুতি নিন। প্রতিবাদে যাওয়ার আগে, আপনি এবং আপনার বন্ধুদের জন্য একটি স্থান নির্ধারণ করুন যেখানে আপনি বিচ্ছিন্ন হলে পুনরায় মিলিত হতে পারেন।

যদি আপনাকে GPS ব্যবহার করে কোথাও যেতে হয়, তবে একটি অফলাইন ম্যাপ অ্যাপ যেমন Organic Mapsব্যবহার করুন। প্রতিবাদের এলাকার ম্যাপটি পূর্বে ডাউনলোড করে রাখুন।

আপনি যদি গ্রেপ্তার হন

যদি আপনাকে পুলিশ আটক করে এবং জিজ্ঞাসাবাদ করে, তাহলে আপনার নিশ্চুপ থাকুন। আপনার যে কোনো জিজ্ঞাসাবাদের আগে এবং চলাকালীন একজন আইনজীবীর সঙ্গে কথা বলার অধিকারও রয়েছে। আপনি বলতে পারেন, "আমি আমার আইনজীবী চাই এবং আমি নিশ্চুপ থাকতে চাই" এবং তারপর আপনি একটি আইনজীবীর সঙ্গে কথা বলার সুযোগ না পাওয়া পর্যন্ত কোনো প্রশ্নের উত্তর না দেওয়ার সিদ্ধান্ত নিন।

যদি আপনি প্রশ্নের উত্তর দেওয়ার সিদ্ধান্ত নেন, তবে নিশ্চিত হয়ে সৎ উত্তর দিন। পুলিশ অফিসারকে মিথ্যা বলা অপরাধ হতে পারে, এবং আপনি যদি আইনশৃঙ্খলা রক্ষাকারী বাহিনীকে মিথ্যা বলেন, তাহলে হয়তো আপনি প্রথমে যেটি সম্পর্কে কথা বলতে চেয়েছিলেন তার চেয়ে আরও বড় সমস্যায় পড়ে যাবেন।

যদি পুলিশ আপনার ফোন দেখতে চায়, তবে তাদের জানিয়ে দিন যে আপনি আপনার ডিভাইসের তল্লাশি করার জন্য সম্মতি প্রদান করছেন না। পুলিশ হয়তো আপনার ফোনটি বাজেয়াপ্ত করতে পারে এবং পরে সেটি তল্লাশি করার চেষ্টা করবে, তবে অন্তত এটা পরিষ্কার থাকবে যে আপনি তাদের এ কাজ করার জন্য অনুমতি দেননি।

যদি পুলিশ আপনার ডিভাইস আনলক করার জন্য পাসওয়ার্ড চায় (অথবা সরাসরি আপনাকে আনলক করতে বলে), আপনি এটি অস্বীকার করতে পারেন। আপনি পাসওয়ার্ড বা বায়োমেট্রিক কী দিতে অস্বীকার করলে আইন প্রয়োগকারী কর্তৃপক্ষ থেকে নেতিবাচক ফলাফল ভোগ করতে পারেন—এতে আপনার ফোন বাজেয়াপ্ত হওয়া বা গ্রেফতার হওয়ার মতো ঘটনা ঘটতে পারে। তবে প্রতিটি গ্রেফতার পরিস্থিতি আলাদা, এবং আপনাকে আপনার নিজস্ব ঝুঁকির মডেল বিবেচনা করতে হবে।

প্রতিবাদের পরে

যদি আপনার ডিভাইস জব্দ করা হয়, তাহলে কী করবেন

যদি আপনার ডিভাইস জব্দ করা হয়, আপনি এটি ফিরিয়ে পাওয়ার জন্য আইনি পদক্ষেপ নিতে পারেন। যুক্তরাষ্ট্রে, যদি এটি প্রমাণ হিসেবে একটি চলমান মামলায় জমা না থাকে, তবে আপনার আইনজীবী আপনার ডিভাইস ফেরত পাওয়ার জন্য একটি আবেদন করতে পারেন। যদি পুলিশ মনে করে যে আপনার ডিভাইসে কোনো অপরাধের প্রমাণ পাওয়া গেছে, যেমন আপনার ছবি বা ভিডিওতে, তাহলে পুলিশ এটি প্রমাণ হিসেবে রেখে দিতে

পারে। তারা আপনার ডিভাইসের মালিকানা পরিবর্তন করার চেষ্টা করতে পারে, তবে আপনি আদালতে এই ধরনের সম্পত্তি বাজেয়াপ্তের বিরুদ্ধে চ্যালেঞ্জ করতে পারেন।

আপনি আপনার ডিভাইসে লগ ইন করা কিছু সার্ভিস অন্য একটি ডিভাইস থেকে লগ আউট করতে পারেন। উদাহরণস্বরূপ, X (পূর্বে Twitter) এ, যদি আপনি ***Settings and privacy*** > ***Apps and devices*** এ যান, আপনি আপনার X অ্যাকাউন্টে সংযুক্ত থাকা ডিভাইসগুলো থেকে এক্সেস প্রত্যাহার করতে পারেন।

অন্যান্য সার্ভিসের জন্য, আপনার পাসওয়ার্ড বা পাসফ্রেজ পরিবর্তন করলে অ্যাপটি লগ আউট হয়ে যাবে। তবে সতর্ক থাকুন, কারণ আইন প্রয়োগকারী সংস্থাগুলোর কাছে এক্সেস প্রত্যাহার করলে আপনি ন্যায়বিচারের প্রতিবন্ধকতা বা প্রমাণ ধ্বংসের ঝুঁকির মধ্যে পড়তে পারেন। আপনি কীভাবে এগিয়ে যাবেন সে বিষয়ে সিদ্ধান্ত নেওয়ার আগে সর্বদা আপনার আইনজীবীর সাথে পরামর্শ করুন। অনলাইন সার্ভিসগুলো আপনার অ্যাকাউন্টের সাম্প্রতিক লগ-ইনগুলোর লগ সরবরাহ করতে পারে। যদি আপনি উদ্বিগ্ন হন যে, আপনার ডিভাইসটি আপনার সম্মতি ছাড়াই অ্যাকাউন্ট অ্যাক্সেস করার জন্য ব্যবহৃত হচ্ছে, তবে এটি আপনার জন্য সহায়ক হতে পারে। এই ধরনের লগ আছে কিনা তা দেখুন এবং সেগুলো মনিটর করুন।

যদি আইন প্রয়োগকারী সংস্থা আপনার ডিভাইসটি বাজেয়াপ্ত করে, তারা আপনার ডিভাইস থেকে ডেটা যেমন ছবি, কন্টাক্ট, মেসেজ এবং অবস্থান বের করতে "ফোরেনসিক" টুল যেমন Cellebrite ব্যবহার করতে পারে। আপনার ফোন যদি পুরানো বা এনক্রিপ্ট করা না থাকে তবে এটি আরও সহজ হতে পারে। এই কারণে, এটি গুরুত্বপূর্ণ যে আপনি ঝুঁকিপূর্ণ পরিস্থিতিতে যেমন একটি প্রতিবাদে যাওয়ার সময়, আপনার সাথে অত্যন্ত কম তথ্য বহন করবেন এবং শক্তিশালী এনক্রিপশন ব্যবহার করবেন।