Cryptoparty 26

Introduction

Welcome to the Cryptoparty! This session is about building a resilient and secure digital life. We’ll explore practical tools and techniques to protect your data and privacy.

Choose Your Own Adventure

We're here to help you.
You'll pick the topics that benefit you and your community.

Who Am I?

Justin McAfee, Ericsson,
Head of Business Enterprise
Wireless Systems: IT Security
Formerly Psychological
Operations Specialist

Pick A Path

- Secure Messaging
- Secure Operating Systems
- Resilient Communications
- Mutual Aid
- Alternative App Stores

Secure Messaging

Signal Messenger

Signal offers end-to-end encryption for secure messaging, file transfer, video and voice messaging. Open-source, independently audited.

Signal Messenger

Limitations

Requires Phone number for sign-up

Central Point of Failure

Date Registered, Phone No., Date last used

WhatsApp

Uses Signal's tech to offer end-to-end encryption for secure messaging.

WhatsApp

Limitations

Owned by Facebook (Meta)…Eww

Requires Phone number

Central Point of Failure

Collects Metadata…lots (location, social graph, use frequency)

Delta Chat

Encryption over Email

Decentralyzed

Resilient

Delta Chat

Limitations

Slower

Requires pre-planning (sign up now!)

Signal Contingency Plan

iMessage

Encrypted

iMessage

Limitations

Apple Owns Keys (Subpoenas!)

Only works on 50% of Phones

Encryption Before and After First Unlock

Encryption transforms data into an unreadable format. Unlocking a device (phone, computer) often removes this protection. Understanding this is the first step to security.

Before First Unlock

BFU state refers to a device that has been powered off or reset and has not been signed back into using the screen lock passcode.

Limited Features - No Camera, WiFi, etc...

After First Unlock

A device that is in the AFU state is that of any device that has been unlocked at least once since the device has been reset or completely powered off.

AFU States

This applies to:

- Apple Computers
- Windows Computers
- Linux Computers
- Apple Cellphones
- Android Cellphones
- Smart Watches

BFU Forensics

This type of extraction is small, and a majority of the information is either system/application data, as well as cached images and videos that are not user-generated.

AFU Forensics

Contains a vast majority of all user-generated data, which can be seen as about 95% of a Full Filesystem extraction

Including user-generated chats, images, videos, web-browsing data, and much more.

Defenses

Samsung LockDown Mode

Apple Advanced Data Protection

Secure Operating Systems

TailsOS

Tails is a secure operating system designed for anonymity and privacy. It routes all internet traffic through Tor, masking your IP address.

Qubes OS

Qubes OS isolates different tasks and applications into separate virtual machines, limiting the impact of a security breach.

Resilient Messaging

Meshtastic

Meshtastic enables decentralized encrypted communication using a mesh network – even without internet access.

But Easily Tracked and requires special hardware

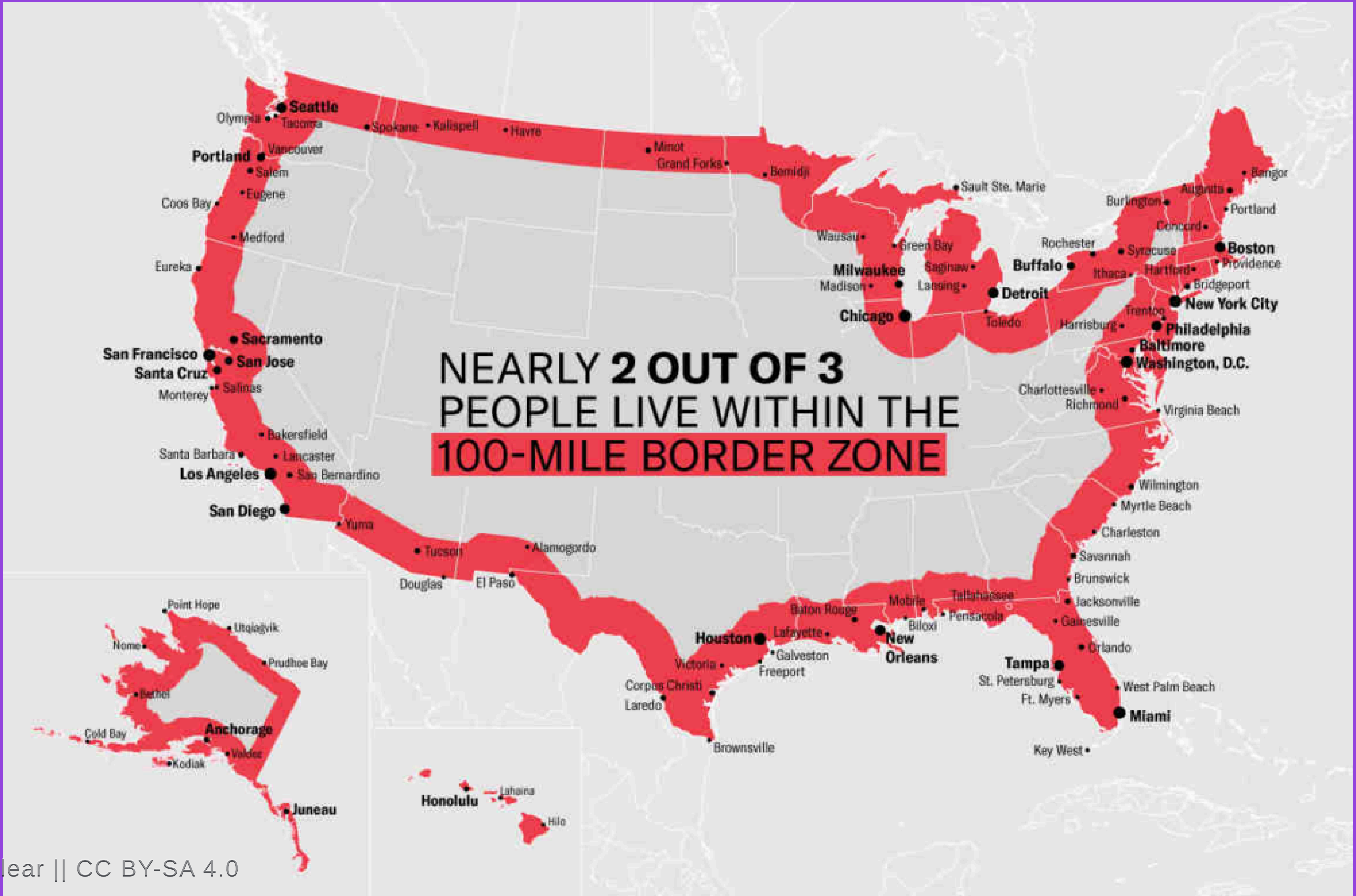
Ham Radio

- Cheap, Easy, Illegal?
- FRS/GMRS Bands
- Easily Tracked

Briar
Meshenger

- Allows Asynchronous messaging
- Huge Meshes
- Blog Publishing
- Android Only

Immigration Issues


NEARLY **2 OUT OF 3**
PEOPLE LIVE WITHIN THE
100-MILE BORDER ZONE
Seattle
Olympia
Tacoma
Spokane
Kalispell
Havre
Minot
Grand Forks
Bemidji
Portland
Vancouver
Salem
Eugene
Coos Bay
Medford
Eureka
Sacramento
San Francisco
San Jose
Santa Cruz
Monterey
Salinas
Bakersfield
Santa Barbara
Lancaster
Los Angeles
San Bernardino
San Diego
Yuma
Tucson
Douglas
El Paso
Alamogordo
Sault Ste. Marie
Wausau
Green Bay
Milwaukee
Madison
Saginaw
Lansing
Chicago
Detroit
Toledo
Rochester
Buffalo
Syracuse
Ithaca
Burlington
Augusta
Bangor
Portland
Concord
Boston
Providence
Hartford
Bridgeport
New York City
Trenton
Harrisburg
Philadelphia
Baltimore
Washington, D.C.
Charlottesville
Richmond
Virginia Beach
Wilmington
Myrtle Beach
Charleston
Savannah
Brunswick
Jacksonville
Gainesville
Orlando
Tampa
St. Petersburg
Ft. Myers
West Palm Beach
Miami
Key West
Tallahassee
Pensacola
Mobile
Biloxi
New Orleans
Baton Rouge
Lafayette
Houston
Galveston
Freeport
Victoria
Corpus Christi
Laredo
Brownsville
Point Hope
Utqiagvik
Nome
Prudhoe Bay
Bethel
Anchorage
Cold Bay
Valdez
Kodiak
Juneau
Honolulu
Lahaina
Hilo

Red Cards

The ILRC's red cards give examples of how people can exercise their rights.

Immigrant Legal Resource Center:Red Cards

Mutual Aid

Mutual aid networks offer a way to build resilient communities and support those in need.

- Can't do everything
- Unique skills and abilities
- Don't Wait!

Flock Cameras

- Automated License Plate Readers
- #7 Top Donator to Trump Campaign
- Top Awardee for DHS Contracts

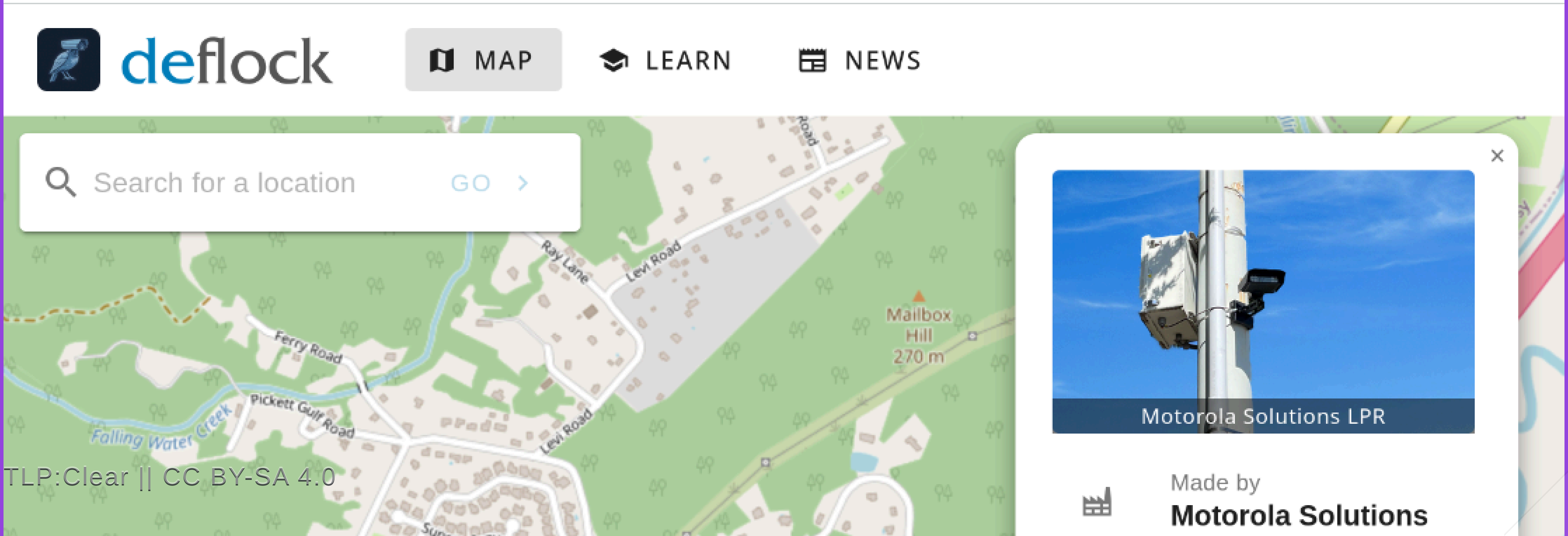
FlockYou

Uses ESP32 to identify and alert on Flock and other surveillance tech

Github:ColonelPanichaks

Deflock.org

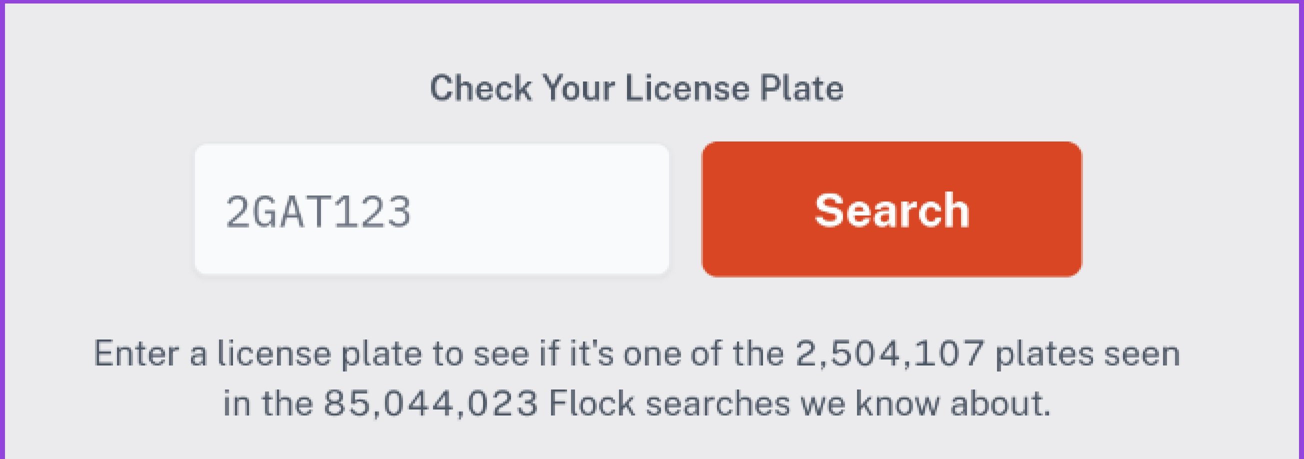
- Real Time map of all Flock known locations
- Crowdsourced
- Contribute via the App or Website



Motorola Solutions LPR

Made by
Motorola Solutions

HaveIBeenFlocked?



Check Your License Plate

Enter a license plate to see if it's one of the 2,504,107 plates seen in the 85,044,023 Flock searches we know about.

Check if your 4th Amendment has been violated.

IMSI Catcher

Cell-site simulators or "Stingrays" can also log IMSI numbers, (International Mobile Subscriber Identifiers) unique to each SIM card, of all mobile devices within an area. Others have advanced features allowing law enforcement to intercept communications.

RayHunter

Rayhunter works by intercepting, storing, and analyzing the control traffic between the mobile hotspot and the cell tower its connected to. It analyzes the traffic in real-time to find suspicious events, incluling unusual requests like the cell tower trying to downgrade your connection to 2G or the tower requesting your IMSI under suspicious circumstances.

Threat Models

- What are you protecting?
- From who?
- What tools do you have to prevent it?

Alternative App Stores

- F-droid
  - Guardian Project
  - Izzy On Droid Repo
- Aurora (Google Play Proxy)

Outro

Thank you for attending! Remember, protecting your privacy is an ongoing process. Keep learning, stay vigilant, and build resilient communities.

Contact US

Mastodon: DigitalDarkAge.cc/@Iaintshootinmis

Signal Messenger: DigitalDarkAge.98

Sources

AFU/BFU Lock States

Android Advanced Protection