ryanohoro
Nov 11, 2024 · 3 min read

Spotting Flock Safety's Falcon Cameras

Updated: Mar 20

This article includes my own security engineering informed analysis / opinion.

Surveillance as a Service Part 2

Read Part 1 for background on Flock Safety

Flock Safety says Falcon cameras provide 24/7 day-or-night detection of license plates, vehicle model, color, even aftermarket parts and bumper stickers. Flock says still images plus “vehicle fingerprint” metadata, are processed locally, and sent back to Flock over a cellular connection. No need to stream bulky live video, which economizes on network infrastructure. A solar panel and batteries forego the need for hardwired power.

Given the nature of what these devices do, and the fact that they are designed to blend into the environment, it may be advantageous to make people aware of where they're located.

Falcon V2 cameras are composed of the following hardware, mentioned in a press release by Lantronix about their partnership with Flock Safety:

Lantronix Open-Q™ 624A System-On-Module (SOM)
Android™ 8.1 Oreo
Qualcomm® Snapdragon™ 624 processor

A Falcon camera label lists the following FCC registered components:

FCC ID N7NRC76B Sierra Wireless Inc. RC76B RC7611 IoT (LTE Cat-4)FCC ID WCBN3510A LiteOn 802.11 a/b/g/n/ac 2T2R+BT V4.2LE LTE

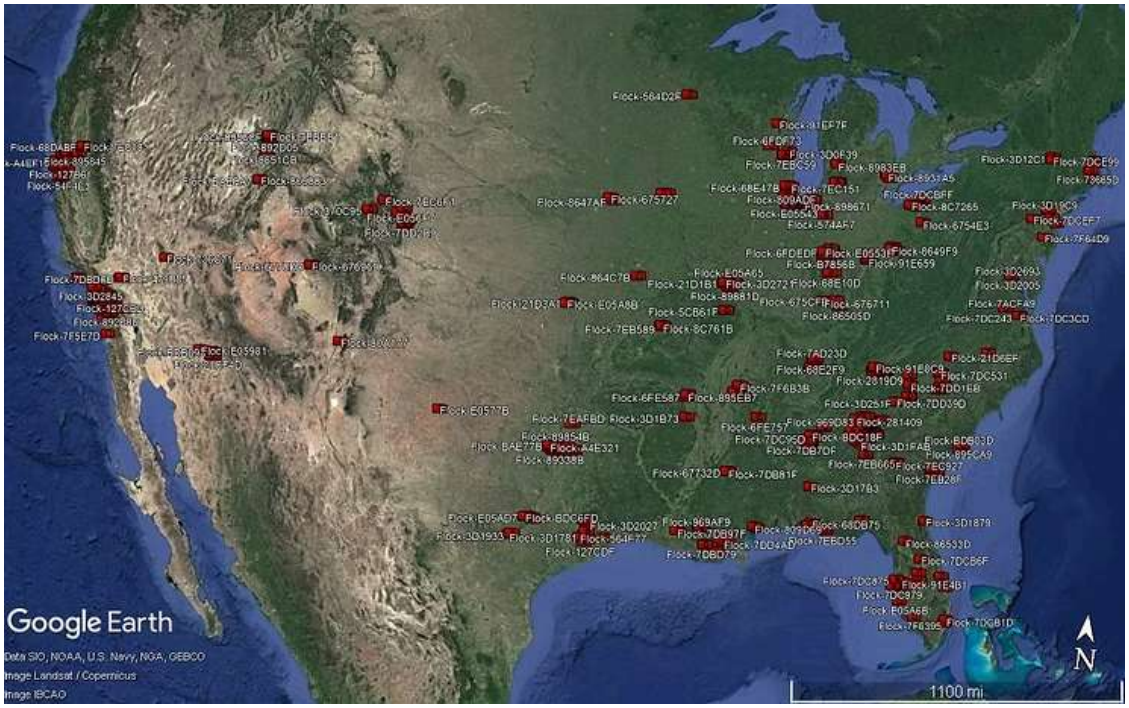
Each Flock device has a QR code sticker that encodes data about the devices. Here are some codes from Flock Safety devices available on Ebay, decoded below.

```
Raven {"pn":'703-
00005',"imei":'864351059169203',"mac":'EC62606B024C',"sim":'89883070000030222390',"fsn":'23071370067'}
Falcon {'pn':'701-
```

00161','imei':'014697000764750','mac':'744CA168DA63','sim':'89014103272872397886','fsn':'21062126FF3'}
Falcon {'pn':'701-
00203','imei':'358026260461440','mac':'9C2F9D6F45A7','sim':'89148000008319644666','fsn':'221013201E0'}

It's interesting these cameras have Bluetooth and WiFi radios. WiFi does not appear to be used in the field for normal operations.

If you wanted to try to locate cameras with WiFi you might use a tool like WiGLE.net, which catalogs such access points using crowdsourced data. Because we know the devices use a fairly niche Lite-On chipset specific to IoT devices, it was easy to find that the cameras have an obvious common WiFi name scheme: Flock-[partial MAC address].



Google Earth image mapping 700+ WiGLE.net WiFi identified Flock devices

Let's manually confirm that these hits are real, installed Flock devices. Castle Rock, CO PD is one of the customers with a Transparency Page, and some of the cameras in that city are in the WiGLE.net WiFi data.

Google Maps Satellite and Streetview images of Castle Rock, CO Flock Safety cameras

Google Maps Satellite and Streetview images of Castle Rock, CO Flock Safety cameras

Google Maps Satellite and Streetview images of Castle Rock, CO Flock Safety cameras

It appears that WiFi being enabled on a camera is an irregularity, since on-site investigations did not show WiFi available near some known Flock Safety devices. What seems to make sense is Wifi being enabled for the installation and initial setup, or field troubleshooting.

This mLive photo gallery includes a photo of a Flock Safety technician looking at a phone in close proximity to a camera, giving the impression he's using it to set up the camera. This WiFi function presents a webcam-like web interface which seems to help the installer put the camera in the optimal position.

Flock Safety likely has tens of thousands of devices in the field though. Can we do any better? We can with Bluetooth.

Every Flock device with an external battery uses Bluetooth to communicate health and safety data back to the camera. The Bluetooth radios use predictable naming schemes.

```
Penguin-NNNNNNNNNN (N = decimal digit)
FS Ext Battery
```

UPDATE 2025-03-19:

The Penguin battery firmware has been updated to remove "Penguin-" from the Bluetooth name, which is now simply:

```
NNNNNNNNNN (N = decimal digit)
```

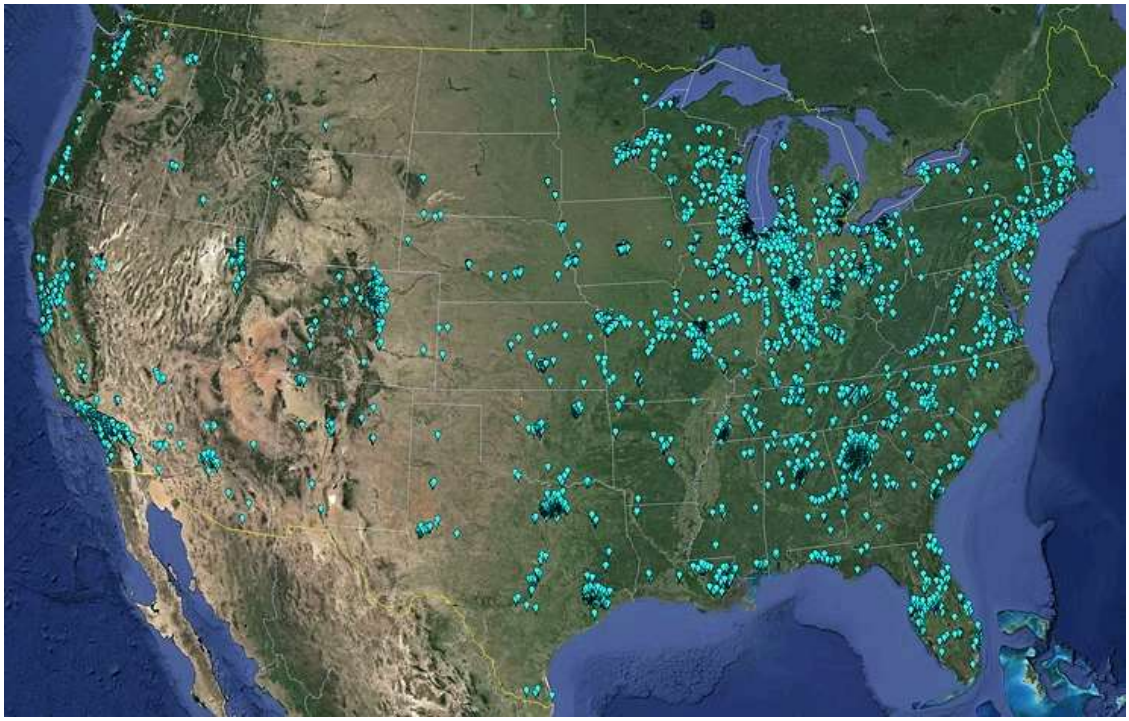
To validate a specific device is a Penguin battery, look for a BTLE advertising packet with a Manufacturer Specific advertising data for XUNTONG (0x09C8), the data will include a serial number e.g. TN72023022000771

```
Packet Header: 0x2444 (PDU Type: SCAN_RSP, TxAdd: Random)
    .... 0100 = PDU Type: 0x4 SCAN_RSP
    ...0 .... = Reserved: 0
    ..0. .... = Reserved: 0
    .1.. .... = Tx Address: Random
    0... .... = Reserved: 0
    Length: 36
Advertising Address: d8:a0:d8:9f:4a:5e (d8:a0:d8:9f:4a:5e)
Scan Response Data: 1dffc809d8a0d89f4a5e2030502a544e373230323330323232303030373731
    Advertising Data
        Manufacturer Specific           Length: 29
            Type: Manufacturer Specific (0xff)
            Company ID: XUNTONG (0x09c8)
            Data: d8a0d89f4a5e2030502a544e373230323330323232303030373731
```

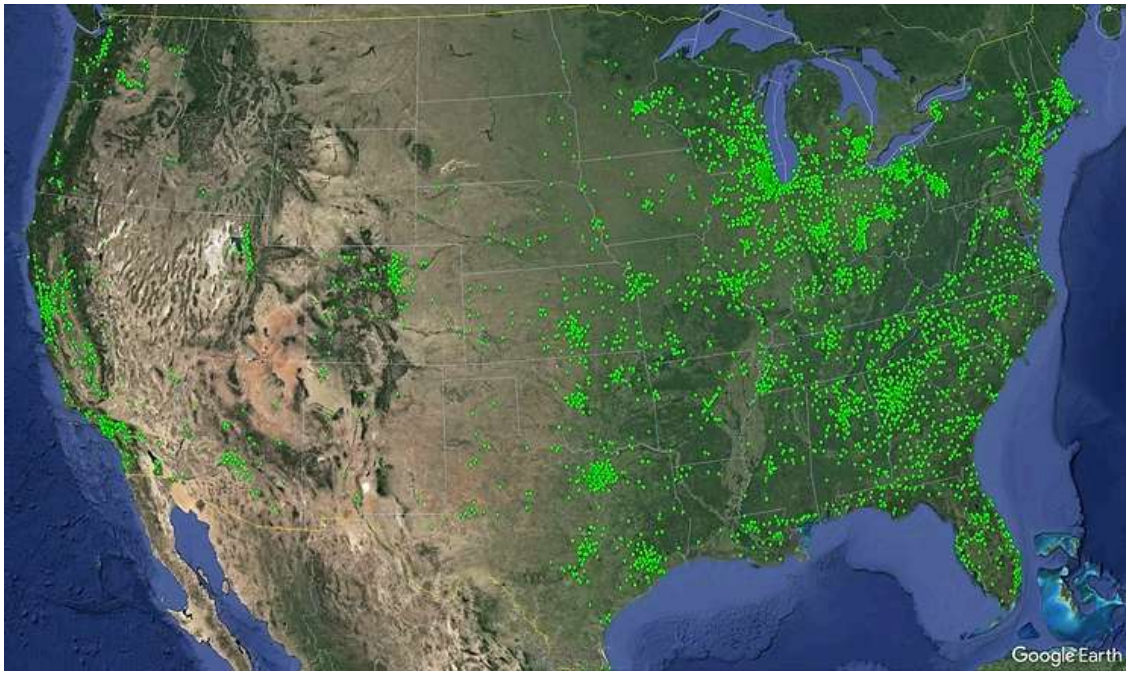
Using these patterns to search the WiGLE.Net data nets many more hits, 18,000+ in fact.

Some cameras have multiple external batteries. Some (very few) cameras are hardwired and have no external batteries. WiGLE.Net relies on citizen reported data, so not all cameras will be identified in this dataset.

Mapping this data shows us what is potentially the real extent of Flock device deployments across the country, that line up a lot better with we know about Flock customers from the Transparency Portals.



Map of Flock devices from WiFi and Bluetooth WiGLE.Net data



Map of Flock customers based on Transparency Portal data