Douglas A. Brush, GCFA, GCFE, GCIH, EnCE
3507 Ringsby Ct.
#106
Denver, CO 80216
dbrush@kivuconsulting.com
Tel: (702) 990-5390

2/14/18

DJI Research LLC
435 Portage Ave
Palo Alto, CA 94306

*Re: UAV Data Transmission & Storage*

For the past several months, my team and I have conducted a careful examination of several popular DJI drones to ascertain how data is collected, used, and stored through normal drone operation and use. Kivu's analysis of the drones and the flight control system (drone, hardware controller, GO 4 mobile app) concluded that users have control over the types of data DJI drones collect, store, and transmit. For some types of data, such as media files and flight logs, the drone user must affirmatively initiate transmission to any remote server. For other types, such as initial location checks or diagnostic data, the user may prevent transmission by deactivating settings in the GO 4 application and/or disabling the Internet connection.

## Methodology

For our analysis, Kivu was not provided drones directly from DJI. Instead, Kivu independently purchased and acquired DJI Spark, DJI Mavic, DJI Phantom 4 Pro, and DJI Inspire 2 model drones for testing and analysis. Kivu also obtained copies of the GO 4 mobile apps directly from the respective Apple and Android stores and installed the software on brand new, independently obtained, Apple iOS and Android devices. Kivu then employed various forensic analysis techniques to view and analyze the data collected on the drones as well as the GO 4 application. While operating the drones, Kivu captured all network data to collect any data transmitted by the GO 4 application to the Internet. Additionally, Kivu analyzed the servers utilized by DJI to store transmitted user data.

Kivu was also provided access to DJI engineers and managers in Palo Alto, California, and Shenzhen, China, and spent several days with the respective teams discussing the products, software development, and information security practices. DJI also provided Kivu access to the iOS and Android GO 4 code repositories, which Kivu analyzed to assist in its determination of what data is collected, stored, and transmitted by the drones and the flight control system.

## Data Storage and Transmission

The DJI drones and the flight control system have the capability to collect data such as videos, photos, and flight logs. Multimedia files are not created automatically, the user must choose to record video or to take pictures. Neither the drones nor the GO 4 application automatically upload or transmit multimedia files to any remote server. To transmit any of this data, a user must affirmatively authorize

the transmission. For example, users may use software provided by DJI to upload video and images to DJI's SkyPixel social media sharing platform. For users operating in the United States, any such multimedia files are uploaded to SkyPixel servers located in the United States.

### Audio

The drones Kivu analyzed do not have any onboard audio recording capabilities. Users have the option to record audio using the microphone on their mobile device, but this option is turned off by default. Any recorded audio data is stored within the GO 4 application on the respective mobile platforms and uploaded to remote servers only if the user affirmatively chooses to do so.

### Flight Logs

DJI drones record flight logs and store them on the drones themselves and within the GO 4 application. These files are stored in a proprietary format designed by DJI. Flight logs consist of GPS location, gimbal information, photo and video capture time, thumbnails of images or video taken during flight, detailed aircraft data, flight time, and battery information. Neither DJI drones nor the GO 4 application automatically upload or transmit flight logs to any remote server. Users must affirmatively choose to upload, or "sync," flight logs within the GO 4 application. For users operating in the United States, such flight logs are uploaded to servers in the United States.

### Diagnostic Information and "No Fly Zone" Data

By default, the drones transmit to DJI servers certain types of information such as diagnostic data (e.g. application performance and user experience information) and initial location check data, which is a generalized, or randomized, location within 10 km of the absolute operating location. This location is transmitted once after the drone is powered on to access nearby "No Fly Zone" ("NFZ") data, which helps users maintain safe drone operation and avoid flying in restricted airspace. However, users may prevent these transmissions by deactivating them within the GO 4 application and/or disabling the Internet connection. In addition, the DJI Pilot flight control application, available for Android, includes a Local Data Mode ("LDM") that the user may activate to prevent all Internet data transmissions.

### Personally Identifiable Information

Through normal use, users must input certain types of identifiable information, for example, at the time of product activation. This includes email addresses and/or phone numbers, but no other identifiable information. However, DJI does not validate this data, so users may enter any information they choose to anonymize themselves, with no impact on drone use or operation. This information is only stored within certain parts of the GO 4 application and is not easily accessible by a normal user or by the mobile device's operating system. There is no other Personally Identifiable Information ("PII") collected.

### DJI Servers

Any data transmitted by the GO 4 application is sent to secure DJI servers. The servers are hosted by Amazon Web Services ("AWS") in the U.S., except for multimedia files that users choose to upload to DJI's SkyPixel social media sharing forum, which is hosted on Alibaba Cloud servers which are also located in the U.S. Both AWS and Alibaba Cloud are widely used by global organizations and have the best in class security controls available to their customers. DJI maintains, manages, and accesses these server resources through their internal IT department.

Kivu reviewed the security policies in force on the AWS servers DJI uses, as well as the user accounts and security groups that have access privileges to these servers. As of the date of this report,

Kivu has confirmed that DJI's network access controls are in order and designed to prevent unauthorized access to information stored on DJI's AWS cloud servers.

### Facial Recognition

Kivu also analyzed the drones to determine whether they use facial recognition features capable of identifying individuals. Certain DJI drones do have the ability to use features called FaceAware and Gesture Control that enable users to control the drone by moving their arms a certain way to which the drone is programmed to respond. However, Kivu determined that the drones cannot identify individual faces or distinguish between them, and in fact do not utilize facial recognition software.

### Cloud Storage Security Audit

Kivu is aware that certain information stored on DJI's AWS cloud servers was recently and inadvertently made publicly available. Kivu has confirmed that DJI corrected this issue with the cloud server access and has complied with all notifications as required by law regarding this incident.

As part of its analysis, Kivu performed industry-standard data security audits and vulnerability scans on the GO 4 application and the AWS servers to identify any known software vulnerabilities. Kivu routinely performs such audits and scans for its customers, and it is common to find some potential vulnerabilities, particularly the first time the audits and scans are performed for a particular company. In DJI's case, Kivu identified certain potential vulnerabilities and immediately notified DJI, providing a full report and a prioritized list of potential vulnerabilities for immediate remediation and recommended steps for remediating them. Kivu worked with DJI to complete the recommended steps and then validated the remediation.

Sincerely,

Douglas A. Brush

Director, Cyber Security Investigations