Kent S. Jackson
Contributing Editor
kjackson@jetlaw.com

Who Is Watching You?

ADS-B raises **aircraft tracking issues (again)**

THERE IS A GROWING AWARENESS AND CONCERN THAT THOSE WHO have asked that ATC tracking data be blocked from dissemination on the Internet are now subject to exposure through growing networks that capture their Automatic Dependent Surveillance-Broadcast (ADS-B) transmissions. Today, there are thousands of tracking capture sites receiving data from unwitting operators.

Flightradar24 and FlightAware appear to be the biggest players in the ADS-B tracking world and they have endeavored to be good citizens. Both have voluntarily blocked tail numbers. Flightradar24 has assisted with accident investigations, for instance.)

Flightradar24 states: "Privacy advocates will be pleased to know that Flightradar24 charges no fees to block the tail numbers of business jets based on an internal list of aircraft types the company put together, as well as the FAA's list of blocked tail numbers, and direct requests from operators."

For its part, FlightAware states that it "is subject to a number of government laws and regulations surrounding the distribution of flight data. In many cases, sensitive [*e.g.,* military] flights are not available for tracking as well as private aircraft whose owners have opted out of public flight tracking." However, it goes on to say that its "users and customers who share data with FlightAware may be able to track these flights on their own equipment, independent of FlightAware."

If you know enough about the technology, you can get completely unfiltered aircraft data without the aid of FlightAware or Flightradar24. Several websites for the truly techno-savvy explain how to "track planes for $20 or less." If you happen to be a "Linux kernel developer" you can indeed create your own ADS-B tracking device for $20, and have control over how you filter the information for your own curiosity. In other words, without a filter, the tracker will not only see all of the ADS-B-equipped business aircraft that have requested "blocking" of their tail numbers, but you also will see military aircraft movements, and presumably even Air Force One. With the same $20 gadget, you also can receive weather balloon data, decode digital voice communications and do budget radio astronomy.

In fact, the blocked tail number aircraft can be tracked even if its operator hasn't yet installed ADS-B. Flightradar24's website explains: "In some regions with coverage from several FR24-receivers we also calculate positions of non-ADS-B equipped aircraft with the help of Multilateration (MLAT), by using a method known as Time Difference of Arrival (TDOA). By measuring the time it takes to receive the signal from aircraft with an older Mode S transponder, it's possible to calculate the position of these aircraft."

MLAT already covers most of North America and Europe. There is also some MLAT coverage in Mexico, Brazil, South Africa, India, China, Japan, Taiwan, Thailand, Malaysia, Indonesia, Australia and New Zealand.

So, aircraft tracking is an issue again, but this time, the source(s) of the problem is very different, and therefore the solution(s) will be very different.

When the industry first dealt with radar tracking websites, those websites solely relied on the FAA for their data feeds. That unwelcome problem was solved once the industry got the agency to put controls on its data.

This time, the data is available directly to the techno-savvy, and there are "crowd-sourced networks" of amateur and not-so-amateur data collectors.

Can't we simply make it illegal? Ironically, the FAA Reauthorization bill passed by the U.S. Senate contains a section titled "Aircraft Tracking and Flight Data" but does not address the security and privacy issues of private tracking sites. Instead, the section is aimed at improving aircraft tracking and flight data recovery. There is specific language regarding underwater locating. The irony is that the Flightradar24 team has previously shown that the amateur tracking network can aid in flight data recovery after an accident.

So, the amateur tracking network has already proven that it can aid in accident investigations. Will the public demand laws that attempt to abolish these networks in the name of corporate security? It seems unlikely, but even if we could craft a law that insisted that amateurs respect blocking requests, U.S. laws can't really stop worldwide networks of aviation geeks, among others.

From my legal perspective, there is no legal solution that will effectively stop someone from finding and tracking your blocked aircraft. The crowd-sourced tracking information networks are incredibly diverse and global. And even if every country passed laws, how would those statutes be enforced? From my limited understanding of the technology, the people tracking you are merely listening. They are not transmitting. If laws are passed to prohibit the sale of the gadgets used to track aircraft, then the sellers can ask the buyers to confirm that the gadgets will only be used for "budget radio astronomy."

The FAA and the aviation associations have discussed several technology solutions to keep aircraft identity from the amateur trackers. There have been a number of alternatives discussed, but given the advent of MLAT, it is clear that the trackers are incredibly adaptive.

A recent exchange with ATC was instructive: A pilot asked the controller if the controller was seeing his new ADS-B output correctly. The controller said: "Uh, no, we have that turned off." The pilot said that he had spent a lot of money on the equipment and really wanted to know if it worked. Could ATC turn the equipment on for a few minutes? The controller said he would check, then reported no, we can't turn it on, it has to be fixed. Meanwhile, dozens of $20-$100 amateur-built units were accurately reporting the aircraft's ADS-B information in real time to their respective networks.

I don't think that the government can beat the amateurs with law or technology. **BCA**