



## RESTRICTIONS ON USE OF COMMUNICATIONS SYSTEMS BY COMMERCIAL AIRPLANE PASSENGERS

The use of communications technologies by passengers (excepting designated law enforcement officers) on commercial airplanes raises a serious security risk: the potential to facilitate terrorist activities. Of particular concern are systems that provide wireless or wired access to passenger-owned devices for access to the Internet, cellular telephone networks, or onboard in-flight entertainment systems. The potential for terrorists to use such systems to communicate and coordinate tactics, both within the airplane and to team members on the ground and even on other airplanes, is a grave concern to aviation security experts, and one that has been discussed relative to the in-flight use of cellular telephones by the U.S. Departments of Justice and Homeland Security and the Federal Bureau of Investigation in comments to the Federal Communications Commission.<sup>1</sup> Footnote 18 of the DOJ/FBI document states:

As documented in the 9/11 Commission Report, the hijackers/terrorists involved in the September 11, 2001 attacks utilized existing telecommunications options from within the terminals at Boston's Logan Airport to communicate and coordinate the planned attacks. See *The 9/11 Commission Report* at 1, 451 n. 3 (noting that while checking in for American Airlines Flight 11, hijacker Mohammed Atta reportedly received a call on his cell phone from fellow hijacker Marwan al Shehhi, which was placed by Shehhi from a payphone located in Terminal C of Logan Airport between the screening checkpoint and the boarding gate for United Airlines Flight 175). Although the communications were effectuated on the ground using existing communications facilities, it is not difficult to conclude what additional/further coordination could have occurred if other options – such as in-flight cell phone use – had been available.

Passenger electronic devices pose additional potential threats to airplane software and hardware systems. These threats include, for example, laptop computers that could be used to plant viruses through the wireless network, or music/video players plugged into hard-wired ports that could be used to send electrical pulses into airplane electronic systems, with the potential to disrupt operations.

To minimize the risks to aviation safety and security from the use of onboard communications systems by passengers, the Association of Flight Attendants-CWA, AFL-CIO (AFA) recommends that the appropriate government security agencies, in consultation with the communications industry, immediately conduct rigorous threat evaluations and develop appropriate performance standards for hardware, software and operations. As a further measure to ensure national security, AFA recommends that all wireless communications systems for use by commercial airplane passengers be kept off during periods of high or severe risk for terrorist attacks (as defined by the Department of Homeland Security).

---

<sup>1</sup> *Comments of the Department of Justice, Including the Federal Bureau of Investigation, and the Department of Homeland Security, In the Matter of Amendment of the Commission's Rules to Facilitate the Use of Cellular Telephones and Other Wireless Devices Aboard Aircraft, FCC WT Docket No. 04-435, Dated May 26, 2005.*

