

Massport's claim that a WiFi antenna installed by Continental Airlines poses a significant security risk, while Massport's WiFi backbone does not lack any merit:

1. Interoperability of WiFi antennas with a variety of potential WiFi consumers demands a high degree of conformance on the part of the WiFi antenna and sender. Thus, the technology used in modern WiFi equipment is extremely uniform over a broad range of different equipment vendors and practically identical for similar or identical models of antennas. There is no technical reason to assume a higher security risk potential for a Continental controlled WiFi antenna. It should be noted that most modern WiFi antennas and senders can limit their power output, thereby restricting the range (and thus impact) of operation.

2. Any argument claiming that Internet access through non-Massport controlled access channels would pose an organizational risk is also invalid, since all major cell phone providers provide Massport-independent Internet access through their cellular network. Furthermore encryption and cloaking techniques can also prevent Massport from sniffing potentially security relevant communications.

Overall, Massport's actions suggest a barely veiled attempt to monetize their monopoly for wireless ethernet communication at Logan airport to the detriment of Continental airlines and consumers.