# Research Note

## The Airline Industry's Internet of Things Risks

**Kyle Simpson**

*Published: March 2018*
*Written: November 2017*

Keywords: Internet of Things; IoT; Airline Industry; Innovation

*Abstract: There is not sector left untouched by the creeping application and presence of the Internet of Things (IoT). Despite its historic reputation for driving innovation in its sector, the airline industry has been unusually slow to implement widespread use of devices connected to the Internet to drive business needs. In defense of this caution, this research paper outlines some potential areas of innovation leveraging the IoT for the airline industry, while highlighting the corresponding risks.*

### Introduction

The broad aviation industry has long been absorbed in innovation, from jet manufacturers working tirelessly to produce top quality and efficiency airbuses, to airline companies constantly reworking customer experiences and interactions. The industry consistently adopts new technologies and methodologies to improve user experience, but where does it stop? At what point do industry operators slow innovation in order to ensure customer safety, rather than releasing new, potentially insecure technology? Lately, the answer to this question has come to focus on the area of the Internet of Things (IoT). The Internet of Things Global Standards Initiative defines IoT as "the network of physical objects or 'things' embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data."[1] There has been noticeable hesitation on the part of airlines when it comes to implementing sensors and other small devices to collect user data; at the same time, impatient industry experts have increasingly demanded progress in this space. One such industry expert, Raj Dalal, wrote in October 2016 heavily pressuring the aviation industry to roll out more connections to the IoT in order to improve passenger experience; however, the argument completely avoided the subjects of passenger information security and cloud integration.[2] This research paper outlines some of the possible implementations of the IoT in the airline industry, and highlight some risks associated with each implementation in defense of the airline industry's hesitations.

### The Internet of Things

The definition of what the IoT encompasses is incredibly broad, leaving a lot of room for innovation and potential risks. The Online Trust Alliance (OTA) recognizes the incredible breadth IoT has the potential to manifest itself in, and seeks to understand best practices companies can follow to maximize customer satisfaction. In short, the OTA outlines "security, privacy, and sustainability" as the three pillars upon which businesses should build their IoT platform.[3] Meanwhile, for the purposes of this research paper, the definition of IoT will be restricted to include only physical electronics and sensors that collect and exchange data, in order to narrow the field of view and give opportunity to focus more on the OTA's pillars. It will also be necessary to distinguish the two categories for which IoT could be applied within the airline industry – airline employees and consumers. When examining use cases for both groups, it becomes evident each have very different needs which would equate to very different solutions. As a

brief example, an airline employee might be interested in a piece of physical technology that could track a passenger through check-in and TSA to consider delaying a flight; while a passenger might be interested in a piece of software they could integrate into their existing hardware that could look up on-flight menus or track their luggage on the way to the baggage claim. Each of these solutions would require a different IoT device and measurement, and would have varying security access controls, entailing nuanced risks for each service. Keeping this in mind, it is important to delineate which category a service would fall under to fairly consider the risk involved and to be able to recommend appropriate controls and procedures.

### Airline Employees

From the perspective of an airline employee in the role of checking passengers in for flights, they use a physical computer and a scanner to read passenger's QR codes and check them into the system. From the employee's perspective, this can be a slow and clunky process since they are connected to large, physical hardware and must always be in the same place, often causing congestion for other passengers trying to move through a space. A potential innovation for this role could be a small, handheld scanner to replace the physical computer, similar to devices many retail stores have adopted. These small devices would only be accessible to airline employees, and as such would need to consider the following controls in implementation. First, they would need appropriate access to passenger data, primarily needing flight numbers, seat numbers, passenger names. This information would provide enough for airline employees to efficiently check-in passengers, while also not providing access to passenger payment information. Having the mobile handheld devices may also allow for increased efficiency and decreased cost. Since the smaller hardware would be cheaper than a typical computer, airline companies could afford to have more of them, speeding up the check-in process, while also allowing for the existing mobile check-in systems.

Although having a more efficient and dynamic check-in system seems nice, it is important to consider the risks associated with new, smaller hardware. The primary risk associated with this potential implementation would be the information security risk.[4] The potential of a passenger with malicious intents stealing one of these readers is moderate-to-high considering the number of passengers traveling through an airport at any given time. Given this risk, it would be incredibly important for the handheld device to have automated controls built in, only granting access to airline employees who are registered with a username and password.[5] In addition to automated controls, it would be import to only provide necessary information about passengers on the device so that even if a malicious party got access to the device, they would not get highly protected information about every passenger.

Since this implementation of IoT relates to aviation employees, rather than passengers, there is greater feasibility for preventative control establishment.[6] In this case, a preventative control could look like an employee training on how to use the new device, a training on what passenger data they have access to and what data they should not have access to, or registration of usernames and passwords. Whatever the form the preventative control takes, the main point is to inform employees of the functions of their new hardware, and train them on proper uses and access.

### Flight Attendants

Moving on to the role of the flight attendant. The place of highest probability for innovation would be food and drink service. Currently, flight attendants slowly move through the aisle with large, clunky carts, asking each passenger if they would like to purchase anything, so to innovate in this position, one idea would be another small handheld device distributed to each passenger or built into each seat that performs a similar function. This device would need a small display, most likely a touch pad, along with a card reader so passengers could look through options and purchase what they want. On the receiving end, there could be a panel for flight attendants to see what passengers order, and distribute individual orders, rather than blocking the aisle for 20-30 minutes at a time. Similar to the check-in handheld device, the devices passengers use would need very specific access to items available on-flight, and restrict access to items on other flights, or access to other passengers' information. Meanwhile, the panel

for flight attendants would need automated controls to access only seat and order information, to prevent similar malicious passengers from stealing passenger's private data while attendants were away from the panel. In this case, preventative controls would be appropriate for the flight attendants, but inappropriate for passengers, since having some form of training for each passenger is not typically a feasible option for most airlines.[7]

### Airline Passengers

Transitioning to the consumer side of airline industry IoT, this is the category of aviation IoT where there is the most opportunity for innovation, and the most opportunity for risk. Consumers of IoT products can be wildly unpredictable in what they accidentally access, so it is very important to heavily structure access to data. Meanwhile, hackers are notorious for wanting to breach important databases, and any database related to aviation would be a high target. There are three primary implementations the industry could develop: 1) sensors to track traffic conditions around airport and in parking garages, 2) sensors to track luggage from the airplane to baggage claims, and 3) sensors and trackers to locate lost luggage. For each, it is critical to note the potential control failures in implementation, as well as the associated risks, beginning with traffic conditions and parking garages.

#### Traffic Conditions

Cameras noting traffic conditions have been sparsely implemented in and around large metropolitan areas. These existing cameras are used primarily for news sources to report on conditions for television and radio listeners to get an idea of what their morning commute looks like. This system has been effective in the past, but relies on qualitative measures, and is open for interpretation from whomever is reporting. A new system that could be implemented is a system where sensors track motion, in this case around airports, and use quantitative measures to more accurately report the traffic conditions. A similar system could be used in parking garages, tracking the number of open parking spaces and congestion in parts of the garage, and reporting this information in a similar manner. The most probable form of reporting would be some mobile application users could download to receive the information, primarily allowing them to better plan for their trip.

The primary risks associated with sensors tracking traffic are system failures, information security, and processing errors.[8] A system failure has the potential to occur when a sensor improperly categorizes data and causes a data center failure. An easy solution to this problem would be to instantiate automated controls, and test the device thoroughly enough to ensure that a miscategorization would not occur. An information security failure could occur if a hacker tried to breach the network where the sensors transmitted data, or if someone damaged or stole the sensor itself. To prevent hackers from breaching the system, automated controls and strong firewall protection would be the best solutions, doing everything possible to protect and segment the system. A processing error would look very similar to a system failure, in that a miscategorization of data has the highest potential of causing such an event. Similarly, automated controls could solve this problem, ensuring that data would not be miscategorized.[9]

Another issue to bring up surrounding the implementation of sensors is the potential for users to be tracked over long periods of time. If the sensor system used some form of machine learning to track cars, there is the potential for the system to begin noticing long-term patterns and accidentally track someone's long-term behaviors. If this were the case, the network would become a larger target for hackers since it has the power to track users and note patterns. To address this issue, whoever operates the sensor system would need to implement strong directive and corrective controls, in the case of a breach.[10]

#### Luggage Tracking

Switching over to the two IoT implementations regarding luggage, these are the two most feasible IoT innovations the aviation industry could make, since both are already currently in existence in other applications. Small GPS tags already exist in the realm of tracking cell phones and car keys, so transferring this feature into aviation is entirely

probable. The brand Tile already sells such a product, so the industry could very easily integrate Tile's hardware into their software.[11] Both locating lost luggage, and tracking luggage progress towards a baggage claim could be achieved with the integration of Tile or a similar product, and the most challenging task for airlines would be third-party coordination. The highest risk associated with third-party integration is the opportunity for hackers to breach either system. If airlines chose to create their own system and simply partner with Tile, rather than relying entirely on Tile's service, then the opportunity for hackers to breach the system is doubled. The Equifax breach in June 2017 demonstrated the challenges associated with third-party cloud integration, and the importance of having proper controls in place to restrict access to data is crucial. Consequently, cloud integration would need to be a major consideration for any airline planning to make third-party partnerships.

## Conclusion

To summarize the potential implementations of consumer IoT in the aviation industry, the most probable form of information synthesis would be a mobile application. The traffic and parking garage sensors, and the luggage tracking would all have to be aggregated somewhere, and for current consumers, mobile applications tend to be the best option. Mobile applications of course have their own risks and control needs, namely information security and system failure risks and automated controls, so these applications would need frequent monitoring and updates.[12] Many airlines already have their own mobile applications for passengers to check-in, get boarding passes, and pay for checked bags, so adding these features to their current systems seems like a feasible goal.

The final area to address in implementing IoT within the airline industry is how everything will actually be developed. When it comes to creating a system as complex as the one described, there needs to be an appropriate amount of time dedicated to ensuring the system is designed well and will not bring about too many negative risks. When in development, the tone at the top will heavily influence the developer's priorities, and will dictate whether they focus on speed of implementation, or strength of the system. A study conducted by the Ponemon Institute found that "the tone at the top … has a trickle-down effect on all employees of the organization," and as a results "risks such as insider negligence and third party risk are minimized."[13] If executives are more focused on spitting out a flimsy system that only works some of the time, then developers will respond with mediocre work. However, if the executives truly want the system to be effective, efficient, and durable, then they must take the time to emphasize the importance of secure networks. The hope is that the current caution of the airline industry to implement IoT is due to executives demanding strong networks, and that when the industry is ready to deploy IoT features, that these will be well-developed, secure and highly functional. Assuming that a positive tone at the top is the reason why the industry has been slow in implementing IoT, industry experts should reduce their pressure on airlines as this may encourage sloppiness over dependability. "Security, privacy, and sustainability," should continue to be top priorities for any company looking to integrate IoT into their business and the airline industry is no exception.[14]

---

[1] Mann, Jason. "The Internet of Things: Opportunities and Applications Across Industries." *International Institute for Analytics*. Dec. 2015. Accessed Nov. 2017 <www.sas.com>.

[2] Dalal, Raj. "Why The Aviation Industry Needs to Hurry Up With IoT Implementation." *Data Science Central*. 27 Oct. 2016. Accessed Nov <www.datasciencecentral.com>.

[3] "About Us." *Online Trust Alliance*. N.D. Accessed Oct. 2017 <www.otalliance.org>.

[4] Searle, Annie. "Enterprise Risk Management." Informatics 312. Information School, University of Washington, Week #3B Oct. 2017, Seattle, WA. Lecture Slides.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] "About Us." Tile Inc. N.D. Accessed Nov. 2017 <www.thetileapp.com>.

[12] Searle, Annie.

[13] "Tone at the Top and Third Party Risk." *Ponemon Institute*. 19 May 2016. Accessed Nov. 2017 <www.ponemon.org>.

[14] "About Us." *Online Trust Alliance*.