AIRPORT BIOMETRICS OPPORTUNITIES & RISKS

As air passengers reach a projected 1.28 billion by 2038, the need for airports to process each passenger through airport entry and exit presents a major challenge that has made the consideration of biometric screening technologies an imperative. In March 2017, the U.S. Department of Homeland Security (DHS) made the use of facial recognition identification a mandate for international passengers, including American citizens, in the top 20 U.S. airports by 2021. Through the U.S. Customs and Border Protection's (CBP) biometric entry/exit program with the TSA, facial-matching services are now being used for air passenger entry into the U.S. at 16 locations, including pre-clearance processes at several international airports, and for air passenger exit at 26 U.S. airports.

Biometric technologies are tools that sense and compare a person's unique biological characteristics, such as their fingerprints, retina, face, speech or biological matter (e.g., DNA) in order to identify and authenticate their identity in a reliable and fast way. Biological characteristics are unique, nearly impossible to falsify and inseparable from a person, and thus, they offer the ultimate identity verification platform. The efficacy of biometric technology for identity authentication is typically used to enable or restrict access of sensitive information and physical spaces, or the use or control of a vital operation, to only designated individuals. A facial recognition screening system, for example, can scan and verify a passenger's identity in seconds. This has already been proven successful through common usage in countless applications for organizations with high-security protocols.

Despite rapid adoption, skeptics of the technology and critics of Federal mandates have raised many questions which remain insufficiently addressed. They suggest that the rush to adopt new technology has occurred despite the fact that its costs, benefits and other implications have not yet been fully vetted or considered by industry participants, policymakers, and especially the general public. Even proponents of biometrics have suggested the need to exercise due caution. Technology deployments are never easy and investment costs are always steep. For the deployment of biometric solutions, as the ever-present threat of cybersecurity and terrorist attacks attests, the cost of failure is even higher. Further, the fragmented vendor landscape raises questions about technical efficacy and legacy system interoperability. Other issues that require greater discussion include questions around:

>> Privacy implications for the collection of highly personal and personally identifiable information;

>> Data protection and ownership given the potential for commercial exploitation;

>> Cybersecurity or potential exploitation by bad actors who steal, modify and abuse data; and

>> Threats to civil liberties, given numerous suspected and confirmed cases of misuse of biometric technologies by foreign governments and authoritarian regimes.

Despite the rush to deploy biometric technologies, in order to maintain the confidence of airport operators, aviation industry stakeholders, government agencies, privacy advocates, civil libertarians, and the traveling public, it is clear that airports should first carefully consider how to approach this new and innovative technology with a full understanding of its potential use cases and corresponding benefits, costs and risks. As airport operators see greater use of biometrics and as they consider exploring the technology, research is needed to help airport operators and their stakeholders understand the uses and considerations of biometric technology.

Global Dynamic Group, LLC
40 Wall Street, 28th Floor
New York, NY 10005

GDG

+1 (347) 767-5453
info@GDGIoT.com
www.GDGIoT.com