Travel and Tourism Research Association: Advancing Tourism Research Globally

2011 ttra International Conference

Opportunities and Challenges for Biometric Systems in Travel: a Review

Cristian Morosan
Cameron School of Business, University of St. Thomas

Opportunities and Challenges for Biometric Systems in Travel: a Review

Cristian Morosan
Cameron School of Business
University of St. Thomas

ABSTRACT

As biometric technology provide superior levels of accuracy, security, and convenience, it is important to understand the extent to which they are applicable in travel. This research reviews the applicability of biometric technology in travel, emphasizing the most critical opportunities and challenges. The opportunities offered by biometric systems in travel can materialize in superior identity management, increased convenience, and better human resource management. Such opportunities can be achieved through specific biometric applications, such as identity management and immigration systems, registered traveler programs, biometric passports, hotel access systems, and payment/retail systems in hotels/restaurants/resorts. Although biometric applications are promising in travel, their large-scale deployment by organizations and adoption by travelers is hindered by a number of challenges. Such challenges include privacy, fear of harm resulting from using the system, and general user anxiety, which need to be addressed before large-scale deployment of biometrics in travel, to guarantee adoption and its associated benefits.

Keywords: *biometric systems, identity management, registered traveler programs, travel industry.*

INTRODUCTION

Within the array of current technologies, one in particular – biometric technology – promises remarkable applicability beyond today's travel industry solutions (i.e., identity management, registered traveler programs). As travel is an information-intensive industry, biometric technology can provide superior levels of accuracy, security, and convenience, therefore optimizing the interactions between travelers and travel organizations. Despite an intense recent scholarly effort aimed at understanding both technical (i.e., enrollment, matching) (Jain & Ross, 2008) and consumer-related aspects (i.e., system adoption, data ownership) (Maio, Maltoni, Capelli, Wayman, & Jain, 2002; Murphy & Rottet, 2009), many issues associated with the applicability of biometric technology to specific industrial settings such as travel, remain, to date, unexplained. Thus, the purpose of this research is to review the applicability of biometric technology in travel, emphasizing the most critical opportunities and challenges. To this end, three specific objectives are followed: (1) discuss the most important opportunities offered by the biometric technology, (2) examine the challenges associated with the use of biometric technology, and (3) provide suggestions to travel organizations about the possible integration of biometric technology with the existing systems to achieve synergies and derive important benefits for their stakeholders.

BIOMETRIC SYSTEM ARCHITECTURE

Biometrics are unique human characteristics that rarely or never change (Inskeep & Claypole, 2007). The literature recognizes two types of biometrics: (1) *physiological*, which allow no control by owner (i.e., fingerprint, face, retina, iris, voice), and (2) *behavioral*, which allow some control by owner (i.e., signature pattern, handwriting, gait) (Chollet, Dorizzi, Petrovska-Delacrétaz, 2009). The information technology applications of various biometrics are referred to as “modalities”. While certain modalities are relatively superior to others (i.e., 3D face recognition is believed to be superior to fingerprinting), no biometric modality is unequivocally recognized as the best for all types of applications (Schouten & Jacobs, 2009). Moreover, specific settings require certain modalities, such as recognition of an individual located away from the sensor, which usually calls for the use of behavioral biometrics (Sarkar & Liu, 2008). To date, the most commonly utilized modalities include fingerprint, face, iris, voice, signature, and hand geometry, while other modalities are still in developmental stages.

A biometric system is a computerized system that allows a user to be recognized based on his/her biometrics. It is based on four components: (1) a *sensor module*, which includes a reader/scanner used to acquire a raw biometric image from a user; (2) a *feature extractor module*, which extracts a feature set from the raw biometric image and creates a template for the user; (3) a *matching and decision-making module*, which compares a feature set extracted from the user with the ones existing in the database and makes a decision to either validate a claimed identity or classify the enrolled identities to identify a user; and (4) a *database module*, which is a repository of templates for users (Jain & Ross, 2008).

Biometric systems function in two stages: (1) *enrollment*, and (2) *recognition*. In enrollment, a user provides a sample image of his/her biometric (i.e., fingerprint, iris) via the sensor module. Then, the feature extractor module extracts features of the user’s biometric and stores a unique template of that user’s biometric into a database. Upon enrollment, newly extracted features are compared against templates stored in the database to create a match score (Jain & Ross, 2008). Recognition is performed in two ways: identification and verification. In identification, a user offers to provide a sample of a biometric that is not necessarily known by the system. The system extracts a feature set, which is then compared to existing samples in a database (Schouten & Jacobs, 2009). In verification, when a user claims an identity, the system compares a newly extracted feature set with that user’s own biometric template already stored in the database (Jain & Ross, 2008). If there is sufficient similarity, the system makes a decision to accept the user (Schouten & Jacobs, 2009).

Given biometrics’ uniqueness to each individual (Bolle, Connell, Pakanti, Ratha, & Senior, 2004), they are believed to be superior to any other recognition alternative (Jain, 2007). Even though biometrics obtained from the same individual may slightly differ due to the nature of the reading/acquisition process, they are considered extremely accurate (Jain & Ross, 2008). The functionality of biometric systems differs from that of other systems, especially in terms of matching, due to the variability in sensing conditions (i.e., a perfect match is necessary in a password-based recognition system, while an imperfect match is appropriate for biometric systems) (Jain & Ross, 2008). Moreover, in biometric systems, a perfect match could indicate a system flaw or even an attack. Thus, it is normal to find two feature sets to vary, even when they belong to the same individual. The variation within the feature set of the same individual is called “intra-class variation”, while the variation of feature sets belonging to different individuals is called “inter-class variation”. Thus, a good feature set should be characterized by low intra-class variation and high inter-class variation (Jain & Ross, 2008). To reach an accept or reject decision, biometric systems compare/match feature sets and express the difference between feature sets in terms of similarity scores, which are further compared with a predetermined threshold. There are two types of similarity scores: (1) authentic scores, obtained by matching two feature sets belonging to the same user, and (2) impostor scores, obtained by comparing two feature sets belonging to different users (Jain & Ross, 2008). If an authentic score falls below the threshold, the system’s decision will be a false reject (i.e., the correct user is rejected by the system), while if an impostor score exceeds the threshold, the system's decision will be a false accept (i.e., the incorrect user is accepted by the system).

Generally, biometric system performance is evaluated using several rates (i.e., Failure to Enroll, False Match Rate). Of these, two rates are most commonly used: (1) the False Reject Rate (FRR), indicating the percentage of authentic scores situated below the threshold, and (2) the False Acceptance Rate (FAR), indicating the percentage of impostor scores exceeding the threshold (Schouten & Jacobs, 2009). It is important to recognize that changing the threshold would not reduce both errors simultaneously (Jain & Ross, 2008). Various biometric modalities differ in terms of FAR and FRR rates. For example, for iris recognition systems, at null FAR, the FRR was between 0.5% and 1.5% (Krichen, Dorizzi, Sun, Garcia-Salicetti, & Tan, 2009). Fingerprint and iris-based systems have very low FRR (0.1% and 0.99% respectively), while voice and face-based systems have higher FRR (5-10% and 10% respectively) (Jain & Ross, 2008). Also, iris, fingerprint, and face-based systems have low FAR (around 1%), and voice-based systems have FAR of approximately 5%. However, as Jain and Ross (2008) and others pointed out, the FAR and FRR, as well as other accuracy indicators, depend on test conditions (i.e., type of sensor, number of users, number of readings per user).

OPPORTUNITIES FOR BIOMETRIC SYSTEMS IN TRAVEL

In spite of a few recent notable initiatives, generally, the deployment of biometric systems has been slow. However, as today's organizations strive to offer increased levels of convenience to their customers and employees while reducing risk and fraud (Prabhakar & Bjorn, 2008), biometric systems seem to be appropriate for achieving this goal. Specifically, the opportunities offered by biometric systems in travel can materialize in superior identity management, increased convenience, and better human resource management. Such opportunities can be achieved through specific biometric applications, such as identity management and immigration systems, registered traveler programs, biometric passports, hotel access systems, and payment/retail systems in hotels/restaurants/resorts.

Superior identity management: immigration and entry systems

In the wake of the terrorist acts of September 11, 2001 in New York and London bombings in 2005, many national and international security agencies called for an effort to increase security (Woodward, 2008). More specifically, agencies wanted to have better accountability of travelers who travel, especially by air and across borders. As a result, many travel procedures have been added or changed (i.e., TSA screenings, restrictions on carry-on fluids), which despite improving security, caused delays and frustration among travelers. To optimize the flow of travelers in sensitive areas (i.e., airports, ports of entry), several identity management and security systems have been deployed, many of them based on biometrics (Schouten & Jacobs, 2009).

In the U.S., for example, one of the most comprehensive identity management systems is the Department of Homeland Security's *United States Visitor and Immigrant Status Indicator Technology* program (US-VISIT), whose goal is to accurately keep track of travelers in- and outside of the U.S. (Woodward, 2008). The system acquires fingerprints from each visa applicants and checks if the applicant already has a visa under a different identity. Also, the visitors to the U.S. are requested fingerprints and facial images, which are then compared against a database of unwanted individuals to prevent their entry into the U.S. (U.S. General Accounting Office, 2004). In parallel, the U.S. Customs and Border Protection currently operates a system called *Global Entry*, which allows trusted enrolled travelers the possibility of expediting their immigration procedures at the U.S. ports of entry by using kiosks for authentication (Customs and Border Protection, 2010).

Superior identity management: personal travel documents (biometric passports)

An indispensable element of modern travel is the personal travel document (i.e., passport, national id card). Given that a common vulnerability of the older generation travel documents is the "look alike" type of fraud (Ministry of the Interior and Kingdom Relations, 2005), governmental agencies have yet to completely secure individual travel documents, of which the most important is the passport. To this end, the biometric (electronic) passport is viewed as a major development in the effort to increase security and eliminate identity fraud in international travel. A biometric passport incorporates certain biometric(s) of the owner, (i.e., fingerprint, face images), along with biographic identification information (i.e., name, date and place of birth, nationality). Given the addition of the biometric to the biographic data, the biometric passport should, in theory, eliminate identity fraud. In a biometric passport, the biometric information is integrated into a contactless chip, which makes the passport machine readable and blocks the release of information without the authorization of the owner (Schouten and Jacobs, 2009). Such a feature makes the biometric passport a convenient, yet secure application of biometric technology in travel.

The history of the biometric passport is rather short. The first biometric passport was adopted by Malaysia in 1998. Since then, early adopters of the electronic passport included countries like the Dominican Republic, Pakistan, Belgium, and Thailand. The European Union introduced the biometric passport on August 28, 2006 (Schouten and Jacobs, 2009). More recently, a variety of countries began issuing biometric passports, and, as of 2009, there were more than 65 countries using biometric passports, including countries such as Nigeria, Qatar, China, and the U.S. One could speculate that in a few years, the majority of countries will use electronic passports, as the national travel and identity management systems become even more integrated as a result of globalization.

Convenient air traveler processing: registered traveler programs

Given their accuracy and ease of use (Bolle, et al., 2004), biometric technologies can be at the heart of applications designed to provide air travelers convenience services in airports. For example, in mid 2000's, there have been initiatives to allow certain travelers, called registered travelers, to expedite their security checks upon authentication by biometric identity management systems (McGinity, 2005). Called the Registered Traveler program in the U.S., it included most major airports (i.e., Washington DC, Los Angeles, Chicago) (Craver, 2008). In exchange for an annual fee of $128, any registered traveler has faster access to the mandatory security check through a dedicated lane. The participants could also claim usage benefits from partnering businesses (i.e., hotels, airlines, credit card companies). Outside of the U.S., countries such as Germany, France, Great Britain, Hong Kong, United Kingdom, Canada, and Israel developed similar programs as early as 2004. Complementary similar biometric-based systems were tried by airlines or airport authorities (i.e., gate authentication without enrollment using electronic passport chips in Manchester, on-the-move passenger iris-based identification in Amsterdam).

Convenient access and payment

As illustrated by retailers such as Piggly Wiggly, Thriftway, and Kroger (International Biometric Group, 2005), the voluntary use of biometric payment systems by consumers results in increased transaction speed, accuracy, security, and positive attitudes (Woodward, 2008). There are several examples in which biometric systems are used for access management in industries adjacent to travel, such as the hotel industry (i.e., Nine Zero hotel in Boston, the Rio All-Suites Hotel and Casino in Las Vegas) (Kim, 2009; Kirby, 2008). Also, at that particular Rio property in Las Vegas, guests can use a biometric system to cash checks and perform other related financial transactions (Miller, 2005).

Further opportunities to use of biometric systems in hotels are discussed by Murphy and Rottet (2009), Kim (2009), and Jackson (2009). For example, Murphy and Rottet (2009) found that Swiss hotel guests exhibit different preferences for various biometric modalities (i.e., fingerprint, face recognition) based on the types of processes (i.e., access, payment) for which they are used in the lodging context. Kim (2009) found that convenience, physical security, data security, and personal concerns were important discriminating variables of two groups of consumers with opposite views (i.e., adopters vs. non-adopters) of fingerprint-based door-locks. Jackson (2009) predicted that a variety of biometric applications could be deployed soon in the lodging industry.

Accurate time and attendance management

Given the human-intensive character of the travel and its adjacent industries, managing human resources appropriately has always been a challenge. Hospitality organizations, for example, employ a large number of lower-skilled workers, sometimes being paid at the minimum wage or seasonally, working at irregular hours and with high turnover (Gaines, 2009). Thus, a critical aspect of human resource management is time and attendance management. More specifically, problems such as fraudulent attendance, theft, or even cash register fraud occur relatively often. Although recent technology applications (i.e., Point-of-Sale (POS) systems), manage to prevent many of the staff members' fraudulent actions, there are still numerous instances of problems, as staff members usually discover and take advantages of systems' vulnerabilities. In this context, biometric systems, which by nature have a low vulnerability to fraud, can provide the accuracy and the staff accountability necessary to remedy the problems.

Today, the opportunities to conduct more accurate and secure operations are vast due to biometric systems, especially when integrated with POS systems. Such hybrid systems can integrate staff members' biometric data within the basic POS functions (i.e., time and attendance management, transaction authorization) to increase accuracy of staff actions and prevent fraud, consequently achieving important cost savings ("M2SYS Technology", 2010). For example, restaurants firms such as RCNY Restaurants LLC (a New York area Arby's franchisee) and Tar Heel Capital (the largest Wendy's franchisee), hotels (i.e., The Venetian Macao Resort Hotel), and clubs such as the La Jolla Beach & Tennis Club (Gaines, 2009), deployed biometric-based time and attendance systems and reported immediate cost savings by reducing the instances of employees fraudulently clocking each-other out and managers' overriding the cash register ("Wendy's Franchisee", 2009).

CHALLENGES FOR BIOMETRIC SYSTEMS IN TRAVEL

Although biometric applications are extremely promising in travel, their large-scale deployment by organizations and adoption by travelers is hindered by a number of challenges. Most importantly, the generally unknown nature of functionality of biometrics to the traveling public creates, and in some cases, amplifies these challenges. The challenges need to be addressed before large-scale deployment of biometrics in travel, to guarantee adoption and its associated benefits. Such challenges include privacy, fear of harm resulting from using the system, and general user anxiety.

Privacy

Defined as the "right to be left alone", privacy has very important connotations in the contemporary interconnected society (Woodward, 2008), as it represents a critical component of electronic commerce (Gurau & Ranchhod, 2009). Privacy is generally viewed as a selective disclosure of personal information founded on the equilibrium between one's private life and his/her accepted social identity (Margulis, 2003). Biometrics and privacy have an intertwined history, which serves as a basis for their continuous evolvement. As biometric applications are continuously developed, privacy concerns arise as a critical topic for government agencies, scholars, and, most importantly, for the public (Ratha, Connell, & Bolle, 2001). In general, in travel, as in mainstream e-commerce, two major privacy issues stand out as the most critical: (1) the "intimate" nature of biometric information and issues related to its ownership; and (2) users' inability to control the collection (i.e., gait, images), storage, and use of biometric information without consent (Gurau & Ranchhod, 2009; Kim, 2009). Such challenges are exacerbated by the fact that biometrics are unique to each individual and cannot be changed if they become compromised (Bolle, et al., 2004).

The intimate character of biometric information is viewed as one of the most important concerns of consumers (Murphy & Rottet, 2009). While some consumers view certain biometric modalities as popular (i.e., fingerprint) due to their historic utilization, others view them as very intrusive (i.e., retinal recognition) (Bolle, et al., 2004). Other consumers are concerned that, by using biometric systems, they leave behind a trail of information that is very personal in nature (Jain, Bolle, & Pankanti, 1999), which can reveal sensitive information about themselves (i.e., retinal images can reveal facts about certain medical conditions). Another important drawback of biometrics is irrevocability. Biometrics leave a trace of information that is very personal in nature, which, unlike passwords or tokens, cannot be revoked (Newton, 2009). In addition, the ownership of biometric information is also an important concern. There have been concerns about storing too much personal information (Lumsden & Beldona, 2006) and about the security of that information, since biometric information is always linked with the individual user (Prabhakar, Pankanti, & Jain, 2003). However, as the technology matures, and as there is no evidence of mishandled or leaked biometric information, it appears that natural concerns about data ownership are unjustified.

A second major challenge for biometric systems is the users' inability to control the collection, storage, and usage of biometric information. This presents important questions for travelers: "Do travelers need to provide consent before biometric information, especially behavioral, is collected?" and "Can the biometric information be sold to a third party for marketing purposes?" In fact, biometrics do not make exception from the current trend according to which a variety of personal information is now recorded (i.e., academic transcripts, passports, real estate deeds) and flows among trusted institutions (i.e., national security agencies, local law enforcement) (Bolle, et al., 2004). Under these circumstances, the organizations handling the biometric systems must establish and maintain trust with their users. In the end, for biometric systems to be perceived as appropriate by their users, three conditions must be satisfied: (1) the biometric information must be used only for the purpose for which it was originally collected, (2) the biometric information must be preferably stored in a device owner by the user (i.e., a smart card, biometric passport), and (3) the personnel involved in controlling biometric information must be educated on the rights of the biometric system users (Zorkadis & Donos, 2004).

Fear of physical harm and general user anxiety

Another concern about biometric technology is the fear of suffering physical harm as a result of using the system. As some biometric modalities require that users interact with or touch the reading sensor (i.e., fingerprinting), it is natural that some consumers become concerned about the hygiene of the sensor (Kim, 2009). Others have expressed concerns about getting in the close proximity of the sensor while using iris recognition modalities (Kim, 2009). However, to date, there are no known cases of harm caused by using biometric systems.

In addition to the fear of harm, some users may feel generally apprehensive toward the use of information and communication technology (Kim & Forsythe, 2008), developing feelings of anxiety toward technology. Intuitively, biometric technology makes no exception. For some individuals, biometric anxiety may develop from information privacy concerns, while for others, it may develop based on certain beliefs, such as the belief that fingerprinting is used for criminals, or that using biometric systems may alter one's dignity (Kim, 2009). Consequently, an individual may display strong negative emotional responses to biometric systems based on his/her beliefs about dignity (Woodward, Orlands, & Higgins, 2003). Generally, as the use of biometrics beyond the traditional identity management applications is still in infancy, and insufficient information about the functionality and risks of biometric systems is available, some users may still maintain a certain general level of anxiety toward biometric systems, which may influence their attitudes towards such systems and their adoption behaviors.

INTEGRATION WITH EXISTING SYSTEMS IN TRAVEL

Intra-organizational integration

Despite the challenges, biometric systems can be integrated with existing information systems to streamline operations and facilitate a faster, more accurate, and secure access of people to information, areas, and transactions. Integration can be performed at multiple levels, from the platform to the component level (Wangler & Paheerathan, 2000). First, at platform level, biometric systems can be integrated with an organization's other hardware and application environments. For example, in hotels, biometrics can be integrated into the current POS systems to allow staff and guests more convenient, secure, and faster access to restricted areas without the hassle of using a card, or other current technologies. At destinations, biometric systems can allow travelers to visit various facilities (i.e., recreational, educational) that a destination may offer. Second, biometric systems can also be integrated with the existing systems at the data integration level. The implications for both organizations and consumers are critical. For example, organizations can keep track of the traveler behavior (i.e., preferences, loyalty) and generate databases that can feed accurate data into managerial decision systems.

Perhaps the most important dimension of integration is component integration of biometric systems into transaction management. A first advantage of such integration is travelers' easier access to transaction capabilities, in an environment that is highly secure and convenient. Second, and more importantly, by having access to data from biometric system transactions, management can draw a more accurate picture of the *personal* preferences of travelers. For example, in a group travel context, managers would be able to ascertain with accuracy which specific traveler of a traveling party engaged in certain transactions. Such information has two important managerial implications: (1) it leaves a stream of undeniable behavioral evidence, which can allow managers to elucidate issues in case of complaints, unsatisfactory service, or fraud; and (2) it provides a multitude of information necessary in the enhancement of the marketing management function, which, in the end, could result in a better marketing strategy (i.e., segmentation, targeting, and even positioning), with an impact on traveler satisfaction and loyalty.

Inter-organizational integration

The inter-organizational integration of biometric systems in travel can be pursued in three directions. A first direction is value chain integration. As a single organization's likely inability to provide the highest value to its customers by acting alone forces most organizations to join their efforts into integrated value chain structures (Xu, He, & Qiu, 2005). Thus, value chain inter-organizational integration via biometric systems can be a solution for the optimization of all processes and interactions within an organization's value chain. Optimization can be realized by creating a seamless digital workflow to achieve higher productivity and ensuring the consistency of information flowing among organizations within the supply chain (Chenhui, Huilong, & Xudong, 2008). Under these circumstances, organizations will achieve more accurate electronic data interchanges (EDI's), which are at the core of optimizing whole value chain structures and their associated managerial processes.

One can decompose the general contemporary travel experience into a multitude of sub-component experiences (i.e., information search, booking, transportation, foodservice, lodging, entertainment). Thus, a second critical integration direction is collaborative inter-firm integration, which may take place among various organizations fulfilling the same goal: adding value to the overall travel experience. For example, firms operating within the same destination (i.e., restaurants, hotels, various vendors) can join their efforts and provide a unified biometric platform to the whole destination, which could provide travelers with convenient and secure transaction and access capabilities. In spite of the difficulties arising from the compatibility of such systems, such integrative efforts may allow multiple organizations to converge toward offering their common consumer a higher-value proposition.

The third direction is horizontal inter-organizational integration, in which a travel organization can integrate their own biometric databases with those of other organizations, complementary in performing travel-related functions. For example, an airline can integrate its own biometric database with those of the national government in order to stop unwanted individuals from boarding aircraft or cross borders. Such integration will eventually create an interconnected system of databases, in which travelers can be uniquely recognized, which could further diminish the potential for identity fraud in travel and increase overall security. However, the drawback of all integration approaches is the legality of biometric information sharing. That is, given the intimate and irrevocable character of biometric information (Newton, 2009), the full legal requirements for biometric information exchange are unknown, especially if the organizations performing the integration operate across borders from each other.

CONCLUDING REMARKS

Despite its novelty, the biometric systems as an area of academic reflection can already be characterized as a mixture of ideas, perspectives, and paradigms, all aimed at elucidating the manner in which this technology adds value to firms and industries. Although a few notable theoretical and practical contributions have been recently offered by several hospitality scholars (i.e., Morosan, 2010), a systematic research effort investigating the role of biometric systems in the travel industry has not been developed yet. Thus, this research makes an important first step within this particular scholarly effort by examining the most critical opportunities and challenges, and by providing ideas for seamless integration of biometric systems with existing IT systems in travel organizations. While a plethora of subtopics remain to be examined, there are at least three critical issues that must be addressed with priority. First, there is a need to examine the extent to which biometric systems call for a change in the current business processes. Entire components of business processes, (i.e., authentication for entering transactions), could change as a result of using biometric systems. While these changes may not be fundamental, they still represent substantial departures from the traditional, pre-biometric business processes, and need to be thoroughly examined. Secondly, it is imperative to understand the manner in which biometric systems add value to the participants in the travel industry. Finally, the extent to which biometric systems change consumer behavior requires scrutiny. Providing increased security and convenience, biometric systems can induce a feeling of comfort in consumers, which may help them overcome the natural anxieties generated by the novelty of these systems, and facilitate adoption. In the end, more research is necessary in order to elucidate all aspects of this challenging, yet fascinating technology.

REFERENCES

Bolle, R. M., Connell, J. H., Pakanti, S., Ratha, N. K., & Senior, A.W. (2004). *Guide to Biometrics.* Springer-Verlag, New York, NY.

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. *Tourism Management*, *29*(4), 609-623.

Chenhui, Z., Huilong, D., & Xudong, L. (2008). An Integration Approach of Healthcare Information System, *International Conference on BioMedical Engineering and Informatics (BMEI 2008), 1*, 606-609.

Chollet, G., Dorizzi, B., & Petrovska-Delacrétaz, D. (2009). Introduction – About the need of an evaluation framework in biometrics, in Petrovska-Delacrétaz, D., Chollet, G., and Dorizzi, B. (Eds.) *Guide to Biometric Reference Systems and Performance Evaluation*, Springer-Verlag, London, pp. 1-10.

Craver, M. L. (2008). *Registered Traveler Program Finally Hitting Its Stride*, KipplingerForecasts.com. Retrieved May 7, 2009 from www.kiplingerforecasts.com.

Customs and Border Protection (2010). *Global Entry Program*, Retrieved July 12, 2010 from: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/.

Gaines, E. (2009). Biometrics provide undeniable time & attendance for Beachside Resorts, *Hospitality Technology*, Retrieved June 21, 2010 from http://www.htmagazine.com/ME2/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=97CC523C47CD44E29B85DB9A0D67C2EA.

Gurau, C., & Ranchhod, A. (2009). Consumer privacy issues in mobile commerce: A comparative study of British, French, and Romanian consumers, *Journal of Consumer Marketing*, *26*(7), 496-507.

Inskeep, T., & Claypole, T. F. (2007). Unintended consequences of biometrics, in Coats, W. S., Bagdasarian, A., Helou, T. J., and Lam, T. (Eds.) *The Practitioner's Guide to Biometrics*, American Bar Association (ABA) Publishing, Chicago, Il., pp. 174-217.

International Biometric Group (2005). *Point of sale: retailers try their hand at finger-scanning payment systems*. Retrieved May 7, 2009 from www.biometricgroup.com/in_the_news/06_20_05.html.

Jackson, L. A. (2009). Biometric technology: The future of identity assurance and authentication in the lodging industry. *International Journal of Contemporary Hospitality Management, 21*(7), 574-582.

Jain, A. K. (2007). Biometric recognition. *Nature, 449,* 38-40.

Jain, A. K., & Ross, A. A. (2008). Introduction to Biometrics, in Jain, A. K., Flynn, P., and Ross, A. A. (Eds.) *Handbook of Biometrics*, Springer-Verlag, New York, NY, pp. 1-22.

Jain, A. K., Bolle, R. M., & Pankanti, S. (1999). Introduction to biometrics, in Jain, A. K., Bolle, R. M., and Pankanti, S. (Eds.) *Biometrics: Personal identification in networked society*, Kluwer Academic Publishers, Boston, MA, pp. 1-41.

Kim, J. (2009). *A comprehensive structural model of factors influencing customers' intention to use biometrics in the hospitality industry,* Doctoral Dissertation, University of Nevada, Las Vegas. Retrieved March 10, 2010 from Proquest Dissertations & Theses, AAT 3383980.

Kim, J., & Forsythe, S. (2008). Sensory Enabling Technology Acceptance Model (SE-TAM): A multiple-group structural model comparison, *Psychology & Marketing, 25*(9), 901-922.

Kirby, A. (2008). Buying into Biometrics: Slowly but surely the industry begins to embrace the technology. *Hotels Magazine,* Retrieved on March 10, 2010 from http://www.hotelsmag.com/article/361318Buying_Into_Biometrics.php?q=biometrics.

Krichen, E., Dorizzi, B., Sun, Z., Garcia-Salicetti, S., & Tan, T. (2009). Iris recognition, in Petrovska-Delacrétaz, D., Chollet, G. and Dorizzi, B. (Eds.) *Guide to Biometric Reference Systems and Performance Evaluation*, Springer-Verlag, London, pp. 25-49.

Lumsden, S. A. M., & Beldona, S. (2006). *Biometrics technology applications in the lodging industry*. Proceedings of the 2006 HITA Conference, Minneapolis, MN.

"M2SYS Technology, TimeForge to Develop Biometric Time and Attendance Software" (2010). Retrieved June 21, 2010 from http://www.htmagazine.com.

Maio, D., Maltoni, D., Capelli, R., Wayman, J., & Jain, A. (2002). FVC2000: Fingerprint verification competition, *IEEE Trans. On Pattern Analysis and Machine Intelligence, 24*(3), 402-412.

Margulis, T. S. (2003). Privacy as a social issue and behavioral concept, J*ournal of Social Issues, 52*(2), 243-61.

McGinity, M. (2005). Let your fingers do the talking, *Communications of the ACM, 48*(1), 21-23.

Miller, V. (2005). *Casinos Leery of Biometrics, New Pay Systems*. Las Vegas Business Press. Retrieved August 26, 2009 from http://www.lvbusinesspress.com/articles/2005/12/27/news/news02.txt.

Ministry of the Interior and Kingdom Relations (2005). *Evaluation Report Biometrics Trial; 2b or not 2b,* Netherlands Ministry of the Interior and Kingdom Relations, Retrieved July 12, 2010 from http://dematerialisedid.com/PDFs/88_630_file.pdf.

Morosan, C. (2010). Theoretical and Empirical Considerations of Guests' Perceptions of Biometric Systems in Hotels: Extending the Technology Acceptance Model. *Journal of Hospitality & Tourism Research,* DOI: 10.1177/1096348010380601.

Murphy, H. C., & Rottet, D. (2009). An exploration of the key hotel processes implicated in biometric adoption. *International Journal of Contemporary Hospitality Management, 21*(2), 201-212.

Newton, E. M. (2009). *Biometrics and surveillance: Identification, de-identification, and strategies for protection of personal data,* Thesis, Carnegie Mellon University, Carnegie Institute of Technology, Pittsburgh. Retrieved March 10, 2010 from Proquest Dissertations & Theses, UMI Number: 3362266.

Prabhakar, S., & Bjorn, V. (2008). Biometrics in the commercial sector, in Jain, A. K., Flynn, P., and Ross, A. A. (Eds.) *Handbook of Biometrics*, Springer-Verlag, New York, NY, pp. 479-207.

Prabhakar, S., Pakanti, S., & Jain, A. K. (2003). Biometric recognition: security and privacy concerns, *Security & Privacy, IEEE, 1*(2), 33-42.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614-634.

Sarkar, S., & Liu, Z. (2008). Gait recognition, in Jain, A. K., Flynn, P., and Ross, A. A. (Eds.) *Handbook of Biometrics*, Springer-Verlag, New York, NY, pp. 109-130.

Schouten, B., & Jacobs, B. (2009). Biometrics and their use in passports. *Image and Vision Computing, 27*(3), 305-312.

U.S. General Accounting Office (2004). *First Phase of Visitor and Immigration Status Program operating, but improvements needed* (Government Accountability Office, Washington, DC), report GAO-04-586.

Wangler, B., & Paheerathan, S. J. (2000). Horizontal and Vertical Integration of Organizational IT Systems, in *Information Systems Engineering: State of the Art and Research Themes*, Springer.

"Wendy's Franchisee Leverages Biometrics to Reduce Fraud at the POS" (2009). Retrieved June 21, 2010 from www.htmagazine.com

Woodward, J. D. (2008). The law and the use of biometrics, in Jain, A. K., Flynn, P., and Ross, A. A. (Eds.) *Handbook of Biometrics*, Springer-Verlag, New York, NY, pp. 357-379.

Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics*. McGraw-Hill, New York.

Xu, Q., He, F., & Qiu, R. G. (2005). Heterogeneous information integration for supply chain systems, *IEEE International Conference on Systems, Man and Cybernetics, 1*, 97-102.

Zorkadis, V., & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security, 12*(1), 125-137.