Hospitality Review

Volume 25
Issue 1 *Hospitality Review Volume 25/Issue 1*

Article 1

1-1-2007

Biometrics for Hospitality and Tourism: A New Wave of Information Technology

Bomi Kang
Coastal Carolina University, null@null.edu

Kathleen Pearl Brewer
California State University – Dominguez Hills, null@null.edu

Billy Bai
University of Nevada, Las Vegas, null@null.edu

Recommended Citation

Kang, Bomi; Brewer, Kathleen Pearl; and Bai, Billy (2007) "Biometrics for Hospitality and Tourism: A New Wave of Information Technology," *Hospitality Review*: Vol. 25: Iss. 1, Article 1.
Available at: http://digitalcommons.fiu.edu/hospitalityreview/vol25/iss1/1

Biometrics for Hospitality and Tourism: A New Wave of Information Technology

Abstract
The technologies that empower biometrics have been around for a number of years, but until recently these technologies have been viewed as exotic. In the not too distant future biometrics will be used to regulate internal processes and to improve services in the hospitality and tourism industries. This paper provides an understanding of the current use of biometrics in general and its practical value for the future in hospitality and tourism. The study presents a review of current practices of biometrics with special reference to the hospitality and tourism businesses, addresses key issues imposed by this technology, and identifies business and marketing implications for these industries.

Keywords
Bomi Kang, Tourism

Biometrics for Hospitality and Tourism: A New Wave of Information Technology

By Bomi Kang, Kathleen Pearl Brewer and Billy Bai

The technologies that empower biometrics have been around for a number of years, but until recently these technologies have been viewed as exotic. In the not too distant future biometrics will be used to regulate internal processes and to improve security in the hospitality and tourism industries. This paper provides an understanding of the current use of biometrics in general and its practical value for the future in hospitality and tourism. The study presents a review of current practices of biometrics with special reference to the hospitality and tourism businesses, addresses key issues imposed by this technology, and identifies business and marketing implications for these industries.

Introduction

Leading strategists suggest that the key to success is to differentiate a business from the competition and to stake one's territorial claim first (Floyd, 2003). Companies following this advice would build a competitive advantage and become a leader in their field. Interestingly, success for some hospitality companies has been achieved, in large part, by taking advantage of information technology (Floyd, 2003; Siguaw and Enz, 1999).

Technology is one of the most important competitive weapons for any hospitality company in today's fast changing environment. Of those advancements in technology, experts predict that biometrics will play an important role in the future (Floyd, 2003; Rinehart, 2000) due to several reasons such as reduced cost of the technology and increased consumer acceptance. The acceptance and use of biometric technology has grown quickly. Revenue from the sale of biometric technologies, (including law enforcement and large scale public sector use,) is expected to grow to $4.6 billion by 2008. (International Biometric Group, 2005).

The most notable function of biometrics in hospitality and tourism is the ability to lessen operators' concerns about security. Hospitality businesses have long suffered from security breaches including, network and systems security, theft by employees, and credit card theft and fraud (Rinehart, 2000). In addition, in the aftermath of September 11th the nation placed increased emphasis on security. Hospitality companies are increasingly feeling the pressure to manage risk, loss prevention, and fraud.

It has become imperative for hospitality and tourism companies to have secure identification and personal verification technologies for everyday business operations. Since many biometrical applications use unique parts of a person's genetic code, biometrics is considered as a more accurate personal authentification solution than current identification methods such as passwords, pin-based or card-based systems.

While the value of this technology can be found in secured verification, biometrics can facilitate the improvement of business operations and more importantly will enable companies to serve their customers in a more secure manner. Once the technology is integrated into exiting business solutions such as point of sales and time and attendance system, the processes are greatly expedited. Moreover, transaction data attached to customers can be utilized to assist further marketing efforts. By securely storing customer's demographical and behavioral data in company's database, hospitality and tourism companies can query different segments of the market and identify the most profitable markets more easily and accurately than inputting them manually. Companies can launch effective promotion campaigns and provide customized service to these markets in order to enhance customer retention.

Despite the great potential of the application of biometrics in hospitality and tourism businesses, there is scant research that has been conducted in this environment and the literature concerning the use and practical value of biometrics is limited. This study will 1) present a review of current practices of biometrics in general with special reference to the hospitality and tourism industry, 2) address critical issues relating to the use of biometrics; and, 3) identify business and marketing implications for the hospitality and tourism industries.

Biometrics: An Overview

Biometrics refers to "the automated methods of identifying or authenticating the identity of a living person based on physiological or behavioral characteristic" (Floyd, 2003; Rinehart, 2000). Examples of physiological characteristics include hand geometry, fingerprint analysis, facial recognition, voice recognition, and retinal or iris scan.

Fingerprint technology reads below the user's surface layer of (dead) skin by bouncing electromagnetic waves, similar to radio waves. These reflections are recorded to build up a picture of the fingerprint, which is matched against the person's known fingerprint recorded earlier. Hand readers simultaneously analyze more than 31,000 points and instantaneously records more than 90 separate measurements of an individual's hand-including length, width, thickness and surface area.

Facial recognition systems analyze images of human faces for the purpose of identifying them. The programs take a facial image and measure characteristics of distance between the eyes, the length of the nose, and the angle of the jaw. Voice recognition systems work similarly. It compares a pre-recorded voice message with the current user's voice inquiry.

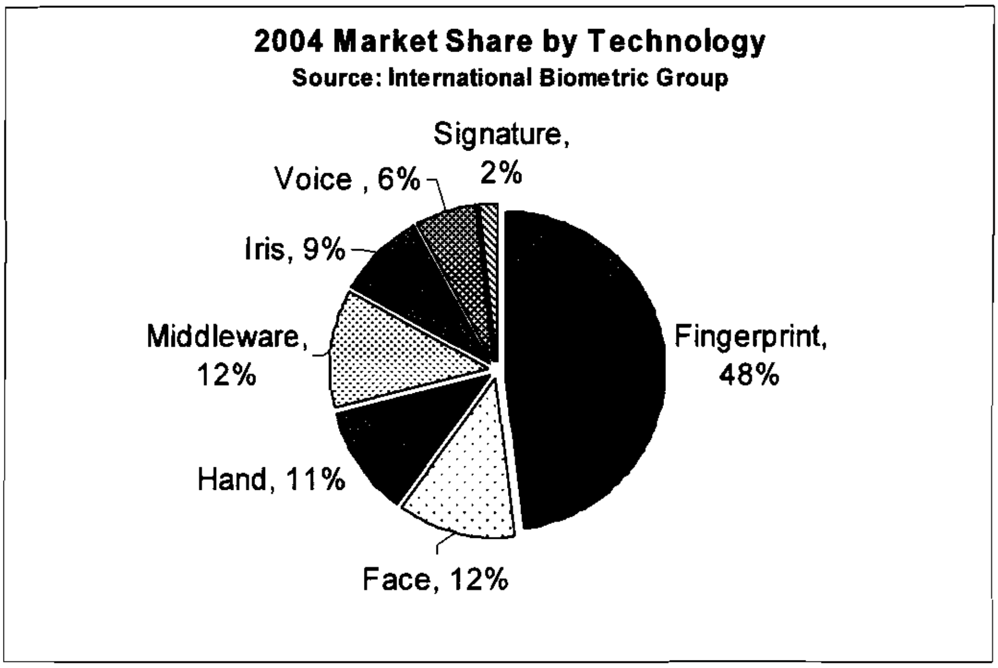
Retinal scanning and iris scanning are two separate identification methods. While retinal scanning was the first eye recognition device developed, iris identification is the biometric gaining acknowledgment due to its less intrusive nature. Iris scan involves analyzing patterns of tissue in the colored ring that surrounds the pupil and it requires no intimate contact between user and reader. Retinal scanning analysis requires the user to keep their head still and eye focused on the light when the device reads the patterns of the layer of blood vessels at the back of the eye. The two technologies using eyes are considered the most accurate physiology-based biometrics techniques.

Behavioral characteristics are more of a reflection of an individual's psychological traits. Examples of these technologies included signature comparison and keystroke dynamics. Keystroke dynamics is where the speed and pentameter of typing is recorded when typing in a password. This pattern must be matched on subsequent authentication attempts for the system to allow entry.

Identification and authentication are key defining elements of this new technology. Biometrics is typically used for two purposes: identification and verification. In these systems identification is the process of examining one individual's characteristics and selecting the individual from a group of stored images, therefore positively identifying that person from the group. Verification, on the other hand, occurs when an individual makes a claim of their identity by presenting documentation that can verify who they are. Unlike other identification or verification methods, this cutting edge technique uses an individual's unique characteristics, which cannot be forgotten, misplaced, borrowed, forged or stolen.

There are various types of biometric systems being used (Avanti, 2003). As can be seen from Figure 1, the most popular one is based on fingerprints. This biometric is increasingly being used in commerce, with roughly half of the biometric users choosing to use fingerprints (International Biometrics Group, 2005). As compared to other techniques, fingerprint recognition has the advantage of ease of implementation and low cost. In most cases, implementation requires a minimal investment of identification sensors and the corresponding software. Finally, fingerprint recognition is relatively reliable; at the same time, it is less intrusive and generally more acceptable to people than other methods. (Klein, 2003).

Figure 1. Market Share of Biometric Technology



The initial biometric application in the United States, the Automated Fingerprint Identification Systems (AFIS), was developed by and mainly served the FBI. By the 1970s, law enforcement began to use this type of biometrics for security and to identify criminals. The Department of Defense was another early user relying on this technology to maintain the integrity of their systems (Robert, 2003). In addition, federal and local governments also used it to confirm identities in forensics, such as criminal identification and prison security, historically used biometrics security applications. More recently, the United States Citizen and Immigration Services has begun to update some of its systems with biometric enhancements using hand scans or fingerprint identification at entry points into the country for immigration identification and verification (Connell and Spence, 2002). Outside of the US, biometric systems have been and continue to be used in national identification databases in the areas of social entitlements, welfare beneficiary identification, driver's licenses, immigration control, and election management (Davis, 1994). While the current use of biometrics appears strongest in the public sector, the International Biometrics Group estimates that in 2007 only one-half of the total biometrics sales will be to government and law enforcement.

As the level of security breaches and transaction fraud increases (Federal Trade Commission, 2003) and the possibility of terrorist attacks intensifies, the need for highly secure identification and personal verification technologies has become more apparent to the private sector. Many organizations have realized the need to improve on the techniques they use to keep their information and assets secure. Healthcare, social services, finance, and banking are only a few industries that have begun to deploy biometrics-based applications. Hospitals have found biometric systems to be an excellant way to respond to new government security mandates. Hospitals now use biometric applications to insure and tract correct delivery of medications to patients, to secure access to sensitive areas, and to protect electronic healthcare data (Hodgson, 2001). The banking industry with a new reliance on networked and Internet based access systems, such as those employed by on-line banking, ATMs, and other remote-access applications are taking a hard look at improvements in security that might be realized through biometrics. Automobile manufacturers and computer hardware manufacturers also have used this technology as a method to secure the access to the car and other assets (Grimes, 1998). Because of this growth in demand, companies are beginning to substantially reduce the cost of new biometric technologies (Fratto, 2003). Since biometric identification technologies are now more cost-effective, reliable and accurate, it has become more feasible in a large range of business applications where identification or authentication of a person is required.

Applications in Hospitality and Tourism

One of the earliest examples of biometric applications in hospitality and tourism would be safes and door locks. The thumbprint safe developed by ElSafe was awarded "Editor's Choice" Award for best new product at the 2001 International Hotel/Motel & Restaurant Show in New York. Biometrics-based door locks have rapidly advanced since the first installation in the Hilton Airport Hotel in Los Angeles. More advanced integration such as VIP recognition and guest room assess utilizing 3D facial recognition is currently in the works. Biometric door locks have been widely applied to existing access control systems even for homes, offices, cars, as well as safes and lockers.

One advantage of biometric technology is that it is reasonably easily to integrate with other applications. Many biometric solutions comply with open standards and therefore can be incorporated into other hospitality systems such as point-of-sales (POS), time and attendance, and casino-player tracking systems, or to secure access to storage or other restricted areas (Fratto, 2003). In addition, biometrics surveillance is widely used by casinos, using facial recognition technology to check for "bad guys" (Robert, 2003).

While there may be a multitude of biometric applications to hospitality and tourism organizations in the future, there are several applications where they could currently be applied.

Access Control Systems

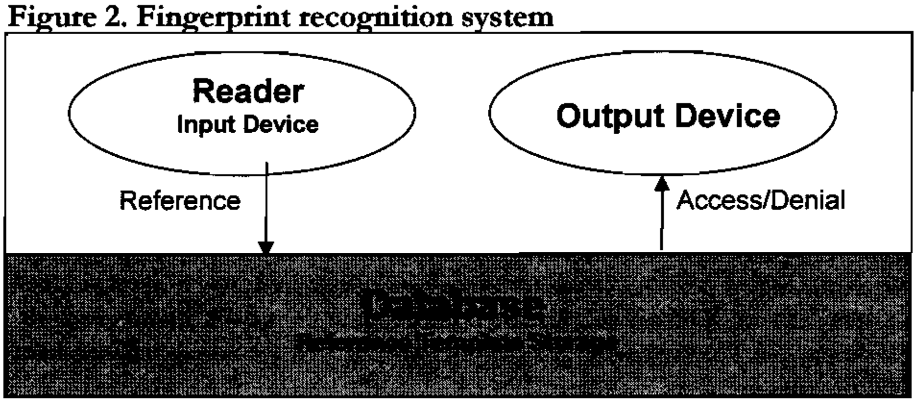
The obvious use for biometrics is to control either physical access or computer system or network access to data (logical control), through secure identification and verification. Currently access to assets or data typically involves requiring the individual to provide an identification card or input a personal identification number or PIN on a keypad. The difficulty with these systems is that they could provide positive identification of fraudulent users. These systems rely on the user to provide plastic cards and codes but they cannot determine who is actually in possession of the card or code. In addition, pins and passwords may be forgotten, and the identification cards may be forged, stolen, or lost.

In hotels and restaurants, biometric technologies enhance the control of alcohol and food storage areas as well as other areas of the property such as computer rooms. Access to those areas will be restricted by employee work shift or authority level, reducing theft with a visual event log of who entered what area at what time.

The University of Georgia has reported positive feedback using this technology. The university has changed their photo ID systems to a hand recognition system for access to foodservice facilities, campus residence halls, and recreation venues. The school reported that the new system saves time and is more accurate than their old identification method (Floyd, 2003).

Another use is to control unauthorized physical or cyber access to customer and/or employee data. Figure 2 illustrates how such a system works using a fingerprint. Once a person enrolls in the system, their fingerprint is stored in a database within the system or stored on companion devices such as a smart card

Figure 2. Fingerprint recognition system



Payment Systems

In the restaurant and shop environment, the most obvious benefit includes faster and more secure payments from the guest. No longer will cashiers need to see identification or get a signed credit card slip because the scanned image is almost fraud-proof identification (Floyd, 2003). With the touch of a finger, in seconds a restaurant could have a payment for meal, find out a guest's history, or have the address of the customer to send out future coupons. The restaurant could provide better service and the guest receives his/her order faster (Floyd, 2003; Blane, 2002; Gran, 2002).

Biometric systems can enhance the traditional point of sales systems (POS). Guests will be freed from memorizing PINs and loyalty program numbers, carrying cash, checks, and credit cards. Instead, they will register their finger images that are then linked to financial or personal information in the system. The check can then be settled and payment completed electronically, without using any of the traditional methods.

Quick service restaurants seem to see higher benefits because speed is their primary concern. Major grocery stores such as Kroger's, West Seattle Thriftway, and Wal-mart were recently testing biometric payment systems using fingerprints (Howell, 2002). And McDonald's had already joined in pilot programs that use fingerprint payment systems (Grant, 2002). Participants of the study conducted by these retail stores, stated that the processing was faster and provided convenience with more security. To use these systems, a typical checkout time takes about 20 seconds and enrollment in the program takes less than four seconds (Howell, 2002).

In another example, when a property management system is networked with the registered fingerprint of a guest, the front desk can check in the guest faster without cumbersome procedures such as asking for an I.D and a credit card. Such an online system will communicate the image of the fingerprints directly to each door so that the guest can enter their guest room without a key reducing the worry about a lock out situation. This elimination of room keys can save money tied to keycard purchases (10 cents to 15 cents per card adds up) and labor cost. At checkout, a reader scans user's index finger and the computer matches the stored print-map to the fingerprint. A loyalty discounts are automatically deducted and the account charged (Rinehart, 2000). If the individual has their data linked to banking information, an account could be debited or credit card charged at this time.

Time and Attendance Systems

Biometric applications would also allow for more secure communications through shared systems. For many years, hotels and restaurants have used I.D.-based identification method for time and attendance. Currently, certain software providers such as ADP, Stromberg and Recognition Systems have introduced new labor management systems with the added feature that uses biometrics to validate employee identification. The new system assures that the person at the time clock is only making entries for him/herself, therefore eliminating "buddy punching," (i.e., where someone clocks in or out for someone else.) The system will ensure that no one else can use access card even though the card is stolen or lost. It will reduce password entry error and the overhead costs related to producing ID cards as well.

Critical Issues

The application of the biometric technology in commerce and further hospitality and tourism is very complex because there are many issues in the process of implementing and monitoring. While biometrics has received elevated levels of support from numerous groups, it has similarly faced opposition from others. It is important to look at both positions since they provide an essential understanding of the key issues reflected in this new technology. The following section addresses several issues to resolve before the widespread adoption of biometrics is likely.

1) Cost

Technological glitches and limited integratability with other applications, has lead companies to be reluctant to invest in biometrics. Among the limitations, cost was the most important reason people were skeptical about biometric applications. As costs are reduced the price will be acceptable to the end user (O'Conner, 2002). Today a consumer can purchase a fingerprint scanner for less than $100 and this scanner is much more effective and accurate than the $1,000 scanner on the market five years ago. In addition, many computer companies are now producing computers and keyboards with built-in biometrics technology.

The cost of biometrics can also be offset in applications where several departments are using the readers. In any enterprise, the company can do door security with security on computers as well as time clock, and get three departments to share the cost of the system (Hodgson, 2001). In this way, the budget centers together on a single system which will reduce the cost for each department. The system also offsets the operating costs because a company does not have to have people full-time administering card functions. The overhead that used to come from card purchases will be diminished. The savings from recurring cost of card buying must be weighed against the additional cost of the readers when looking at systems (Hodgson, 2001).

Regardless of which form of biometrics is used, the price of implementation will drop as adoption increases, and extensive risk per reward analyses must be done in each organization to justify the use and expenditure. The choice depends on the level of security required and the budget to purchase the systems.

2) Privacy Invasion and Legislation

Biometrics is a promising technology. However, in order for it to become fully accepted, users have to be convinced to give up some of their privacy in exchange for greater security. The use of biometrics inherently poses a threat to the privacy of an individual because of its ability to track the individual from the information in a database. Therefore biometric technology is perceived as intrusive and invasive.

There has always been psychological resistance when a new system is introduced. One of the reasons that the public might be opposed to the implementation of biometric systems is that traditionally this form of identification has been used as a method to track criminals, not the common everyday person. Nevertheless certain privacy groups such as CASPIAN and Fight the Fingerprint advocate consumer's rights. Consumers are concerned that the data collected might be divulged to the law enforcement or shared with third parties without their knowledge or consent. Further, employee monitoring systems using biometrics provoke the issue of employee privacy. The protection of employees under the law has evolved and become the focus of new legislation needed as the technology moves forward in the marketplace (Buzek, 2003).

There are advocates on both sides of this issue. Both proponents and adversaries of this technology have valid arguments. As systems are adopted, experts expect to see increased legislation regarding how and when these systems can be used. If appropriately regulated, biometrics might actually assist in guaranteeing privacy rather than detracting from it. For example, biometric systems have been found to be an effective way of reducing credit card fraud and saving process time. (Howell, 2002; Buzek, 2003).

3) User Education

Because there are misunderstandings about the use of biometrics, it is important for the public to be educated concerning the use of such systems. For instance, any system implemented for authentication must be established as a "one-way" system; that is, the system can be used to verify identity, not used to find a person from the biometrics data. One such system uses extraction algorithms to convert a fingerprint image into a digital vector number, which is then stored. Therefore, the fingerprint itself is not stored and it cannot be recreated from the stored digital vector. Instead, the person is authenticated because the associated vector number of that individual recorded in this reading is within acceptable limits of the initial reading.

Strengthening e-CRM

While experts do not envision real-time customer relationship management anytime soon, the following are noted benefits and implications to the business marketing of using this biometric technology.

Customer retention

The traditional marketing mix activities are no longer able to capture the changing behavior of today's marketplace and customer relationship management (CRM) becomes fundamental (Grönroos, 1990; Grönroos, 1997). While it is important to gain new customers, what matters most is how to retain them. Developing relationships with customers is a constant challenge to businesses of all types. Through customer relationship building, companies will benefit from customer loyalty in the end (Shoemaker and Lewis, 1999). With POS integrated, the biometric technology can enhance relationships with customers in an electronic environment and more importantly, it can improve loyalty programs for repeat customers. In an early test in a quick service restaurant, a year long pilot reported that between 65 to 75 percent of the regular customers signed up to use this technology and the restaurant eliminated the paper-punched-redeeming cards for goods. Now with every customer purchase, loyalty points or rewards are saved electronically and can be redeemed at the POS (Rinehart, 2000). One other benefit to the hospitality industry is in the cleansing of information. Hotels are continually purging their records to keep accurate information on their guests (Rinehart, 2000). With the right data mining software, this biometric technology makes it easier to track and identify customers accurately with less labor cost. Customers' previous purchases can be used to predict future purchase behavior. Thus, one-to-one marketing becomes more efficient.

Customized products and services

For hospitality and tourism businesses that also rely on loyal customers, biometric systems can help streamline databases to better target and serve profitable customers. Once the customer has registered his/her fingerprints, the customer's profile associated with the fingerprints can be brought up upon check-in, enabling employees to provide several services specific to the profile of that customer. Some of these services may include room temperature control, television channel access customized to that customer's preferences, presetting wake-up times, and a custom configuration of the in-room beverage and food services that are presented on the television to that specific guest. It certainly differentiates the services for repeat customers and therefore builds loyalty.

Conclusion

The primary use of biometrics in hospitality and tourism is to regulate internal processes and security. The initial application will likely be time and attendance, workforce management and access control (Buzek, 2003). These are environments in which the employer has the ability to mandate the use as a condition of employment. It is also an area where the expense to add biometrics can be easily justified by increased security and lower worker fraud. In the long run, it is an extremely low cost method to capture and store personal preferences and identifiers. Not only does it mean a lower operating cost, but the technology has tremendous implications regarding customer relationship management and the service delivery systems provider. The hospitality industry should be proactive in the development and use of this technology.

This paper is an exploratory attempt to increase the understanding of the current use of biometrics and its practical value in the hospitality and tourism industry. Further, it is intended to initiate future discussion and research in the area of hospitality and tourism marketing in relation to the effective use of customer information via biometrics. Future research calls for more empirical investigations regarding the perceptions and expectations of the use of biometrics. Moreover, identification of actual contributions of biometric technologies to operations and management in quantifiable terms deserves special attention and consideration.

References

Avanti, The Biometric White Paper, 3 July 2003 <http://homepage.ntlworld.com/avanti>

Blane, C., "At Grocery Checkout, No Wallet Needed," *New York Times* 25 July 2002.

Buzek, G., "Biometrics for Hospitality," *Hospitality Upgrade* Summer 2003.

Connell, T. O. and B. Spence, "Securing American: Lessons Learned--Biometrics: You Can't Afford Not to Sell It," *Security Distributing & Marketing* 32(2002).

Davis, S.G., "Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine," *Information Technology & People* 7 (1994).

Federal Trade Commission Identity Theft Program, 10 July 2003 <http://www.ftc.gov/os/2003/09/synovatereport.pdf>

Floyd, J. M. "Biometrics--the Future Competitive Edge," *Foodservice Equipment & Supplies* 56 (2003).

Fratto, M., "Are Biometrics the Answer?" *Network Computing* 14(2003).

Grant, L., "Retailers Test Paying by Fingerprint ; High-tech Process Uses Biometrics," *USA TODAY* 30 July 2002.

Grimes, R., "When What You Don't Say Says as Much as What You Do," *Nation's Restaurant News*, 32 (1998).

Grönroos, C., "From Marketing Mix to Relationship Marketing - Towards a Paradigm Shift in Marketing," *Management Decision* 35 (1997).

Grönroos, C., "Relationship Approach to Marketing in Service Contexts: The Marketing and Organizational Behavior Interface," *Journal of Business Research* 20 (1990).

Hodgson, K., "Biometric Boost," *Security Distributing & Marketing* 31(2001).

Howell, D., "From Sci-fi to Sales Floor-New Technology Hits Mass," *DSN Retailing Today* 41(2002).

International Biometric Group, Biometrics Market and Industry Report 2004-2008, 20 Jan. 2005 <http://www.biometricgroup.com/reports/public/market_report.html>

Klein, K., "Trends in fingerprint recognition systems," *Security* 40 (2003).

O'Connell, T., "Biometrics: An Emerging Role for Security Dealers," *Security Distributing & Marketing* January 2002.

Rinehart, G., "Biometric Payment: The New Age of Currency," *Hospitality Upgrade* Spring 2000.

Robert, B., "Are You Ready for Biometrics?" *HRMagazine* 48 (2003).

Shoemaker, S., and Lewis, R., "Customer Loyalty: The Future of Hospitality Marketing," *International Journal of Hospitality Management* 18 (1999).

Siguaw, J. A. and Enz, C. A., "Best Practices in Information Technology," *Cornell Hotel and Restaurant Administration Quarterly* 40 (1999).

About the authors: Bomi Kang, Ph.D., is an Assistant Professor at the W. Craig Wall, Sr. College of Business Administration, Coastal Carolina University, Conway, SC. Kathleen Pearl Brewer, Ph.D. is Professor and Director of Graduate Studies, William F. Harrah College of Hotel Administration, University of Nevada, Las Vegas. Billy Bai, Ph.D., is an Assistant Professor in the Tourism & Convention Administration Department, University of Nevada, Las Vegas.