Business Horizons (2013) **56**, 387—397

Available online at www.sciencedirect.com

SciVerse ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY
www.elsevier.com/locate/bushor

From avatars to mavatars: The role of marketing avatars and embodied representations in consumer profiling

Brian E. Mennecke [a,*], **Anicia Peters** [b]

[a] *College of Business, Iowa State University, 3313 Gerdin Building, Ames, IA 50011, U.S.A.*
[b] *Human Computer Interaction, Iowa State University, 1620 Howe Hall, Ames, IA 50011, U.S.A.*

KEYWORDS
Avatars;
Biometrics;
Facial recognition;
Marketing;
Privacy;
Digital signage;
Mavatars

Abstract Recent trends in advertising and social media (e.g., facial/body recognition technologies) will change how people need to think about their digital representations and privacy, as well as how managers can use these technologies to interact with customers. The term *avatar* is usually associated with a video game character or a pictorial representation on a social network, and among other components of the definition of the concept is the notion that users control the avatar's appearance and actions. Facial recognition and video analytic technologies being applied in public digital signage displays and on social networks like Facebook capture and create an embodied biometric database that is essentially an avatar-like profile that will be used for marketing products and supporting consumer applications. In this article we discuss the nature of these new marketing avatars, which we call *mavatars*, and offer a framework for understanding where and how these embodied profiles are and will be used. We also discuss and speculate how these representations and the applications they spawn will evolve; where they will be used; and the ramifications of these embodied representations for consumers, managers, and society at large.

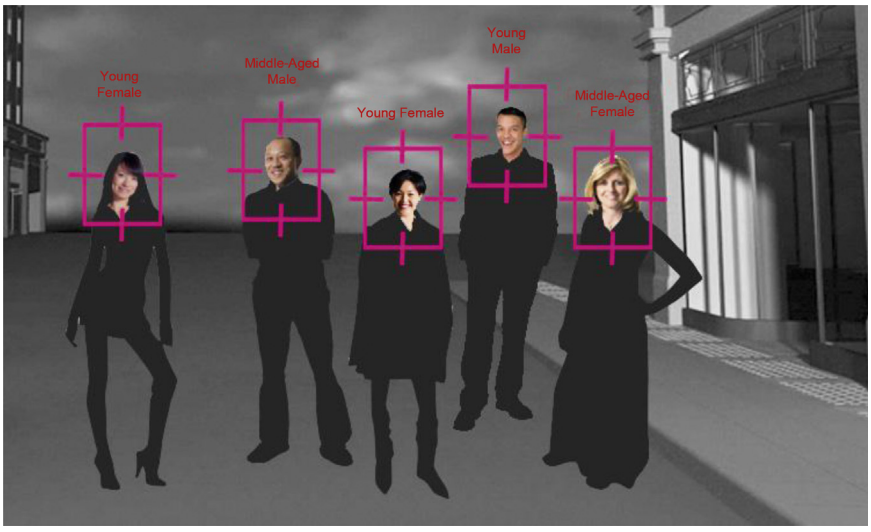
1. Your face, captured in a public space, will soon be commonplace

Recent trends in advertising and social media, including facial recognition technologies, will change the way we need to think about our digital representations and how vendors manage their relationships with customers. For example, new technologies such as multimedia digital signs are becoming common and relying increasingly on automated observer monitoring systems capable of identifying whether viewers are present, determining whether they are watching, and—most importantly—capturing viewers' physical characteristics/demographics. Systems such as those offered by Intel (2012)

* Corresponding author
E-mail addresses: mennecke@iastate.edu (B.E. Mennecke), anpeters@iastate.edu (A. Peters)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2013.02.002

Figure 1. Stylistic example of user information captured by digital signage systems



currently monitor viewership and identify general characteristics about the person being observed (i.e., the *target*) such as race, age, and sex. They can also monitor the degree of attentiveness and for how long the target watches the display (see Figure 1). Intel is quick to point out that these systems are designed to be anonymous; however, to provide useful information, they must capture data that can be used to build a profile of the target. Of course, customer profiling is not new, but what is unique about these systems is the fact that the profile now includes a multidimensional digital representation of the user's physical appearance and biometrics, as well as the viewer's behaviors in the context of their interactions with the display.

While the vendors of these audience response systems promise anonymity, social network sites like Facebook are taking this concept one step further. For example, in 2010 Facebook introduced a feature it calls 'Tag Suggest,' which scans images uploaded by users and employs facial recognition software to match these images with existing Facebook users (Mitchell, 2012). Because the users of Facebook are not anonymous and they have an existing profile that includes photos of themselves in various contexts, the image scanning software can be used to build a robust profile that includes not only demographics and other attributes, but also images of the user and the contexts in which the user engages in work, social, or leisure activities. As with digital signage, to make such a system work, Facebook builds a profile of each user that includes a biometric representation of the user's facial and, presumably, other bodily features.

We view this biometric representation and the contextual data that go with it to be something akin to an avatar because it represents those identifiable embodied and facial characteristics (i.e., biometric indicators) that would be of use for identification and that enable facial recognition applications. Unlike the avatar we might design for ourselves, the identity associated with a marketing avatar represents our identity—including not only the biometric characteristics of the target's face and body, but also a behavioral profile—from the perspective of the vendor or outsider. Additionally, and importantly, this is something that the person being viewed (i.e., the target) will have little control over. While a marketing avatar will be treated and used by vendors much like other customer profiles, the fact that these representations will use immutable biometric and behavioral characteristics will raise numerous concerns for managers and software developers related to privacy and the associated effects on public relations and litigation.

In this light, the purpose of this article is to examine issues raised by marketing avatars—which we refer to as *mavatars*—as they pertain to both marketers and consumers. On the marketing side, the challenge is for vendors to leverage applications derived from mavatars in a way that enables rich data collection, management, and use, while simultaneously balancing this with the privacy of targets (Christiansen, 2011). Of course, firms are increasingly being pressed to seek out and use these richer forms of customer data as the retail and online markets evolve to more customer-centric and highly customized modes of marketing (Johnson & Kim, 2009). The value offered by mavatars is that they will allow vendors to readily identify customers in the context of their activities and leverage this to provision more accurate marketing messages, better customer need

fulfillment, and superior customer service. Marketers often do not understand the needs of customers and how to correctly design their marketing campaigns ('Digital Ad Overload,' 2012). As a result, customers frequently turn a blind eye to ads presented online and in public spaces when they are perceived to be irrelevant. This is because consumers are not only overwhelmed by advertising, but also better informed and more selective in their attention to stimuli; capturing their attention will require personalized, location-specific, timely, and contextually-relevant messages ('Marketers Lack Confidence,' 2012). As a result, the use of mavatars will eventually be commonplace in retail and similar contexts where detailed information about customers in location-specific contexts is needed. On the consumer side, the concern relates to how mavatars will affect privacy and security and the issues this raises relevant to managing identity both online and in public spaces where vendors may be engaging in stealth marketing (Roy & Chattopadhyay, 2010). To address this topic, we first discuss the relevant technologies that are likely to enable the collection and use of mavatars. Then, we present a framework for classifying where and how mavatars and the applications built to use these data will be applied. We conclude by discussing and speculating about the implications of mavatars for marketers and consumers, as well as the future of these applications.

2. The evolving role of digital signage and customer profiling

2.1. Multimedia digital signage

Digital signage is popular, in part, because it is versatile and the dynamic content captures the attention of observers (Peters & Mennecke, 2011). Displays can render static images, video, sound, and graphics and include feeds from Internet sites, broadcast media, or even feedback images of the observer through embedded cameras (Lorrette, 2011). An important advantage of digital signage is that content can be remotely manipulated and displays can be connected with applications and hardware, such as video surveillance, near-field communications (e.g., RFID), Point-of-Sales (POS), and other interactive systems (Pondent, 2012). Recent trends in digital signage include multi-touch, gesture recognition, auto stereoscopic 3D displays, and wireless interfaces that allow targets to interact with the displayed content.

As this review suggests, signage has evolved into an interactive medium that can be leveraged by marketers to increase the likelihood that customers will pay attention to the contents of the display. As with our interactions with web pages, however, today's digital signage can be used to do much more than simply display content; many interactive screens are 'looking back' to monitor behaviors and observe the characteristics of the customer.

2.2. Audience metric signage systems

The desire and capability to monitor customers' reactions to digital advertising is not new. Banner advertising has been around almost as long as the web, and one of the chief benefits of this form of advertising is that it can be used to monitor behavior in response to ad content. For example, click-through rates, page views, and similar metrics drive web advertising and represent an important source of revenue for vendors. In retail and public spaces, the challenge facing retailers is that customers remain anonymous unless they can be incented to identify themselves. As a result, an emerging trend in retailing is to find ways to unobtrusively identify customers. One approach is to use Wi-Fi, which often involves giving customers free access in exchange for the right to identify and track them (Butler, 2012). The challenge is that this requires that customers possess smartphones, they have Wi-Fi enabled, and they are willing to opt in.

An important and unique feature of capturing audience metrics from digital signage is that these systems unobtrusively capture information about customers in context and, when run anonymously, data can be captured without requiring opt-ins. These systems provide vendors with the ability to track viewership by scanning the environs surrounding the display to identify and monitor the presence of viewers, their demographic characteristics, and their attentiveness. For example, these systems monitor responses to advertising portrayed on displays, adjust content to suit the context, and collect data that can be used to assess viewership and tie this to behavior. As the viewer is observed, the system captures biometric indicators that allow it to identify attentiveness, behaviors, emotive responses, and physical characteristics such as race, gender, and age. This biometric data is used to create the biometric representation of the target in the vendor's database that can be used to track an individual user, and it can be aggregated with other viewer data to calibrate and improve system performance.

Given the capability of digital signage and the potential benefits of accurately targeting ads to observers (Burke, 2009), we expect that this technology will continue to proliferate and become commonplace. Furthermore, while anonymity is

currently associated with these systems, it is likely that opt-in features—which allow users to participate in check-ins or rewards programs—will quickly become a standard component of these technologies. For example, in partnership with Face.com, Coca-Cola recently demonstrated an application called *FaceLook*: an interactive digital signage kiosk that allows users to post images and comments to their Facebook page simply by gazing at the kiosk (Hall, 2012). This application identifies the user and updates his or her Facebook page with a photo and information about the venue where it was taken. While FaceLook is designed as a peer-to-peer (P2P) application and was not positioned to deliver advertisements, it could easily evolve to include such capabilities.

2.3. Embodied representations on Facebook

As demonstrated by the FaceLook application, social networks will likely be integral for associating images with profiles. Not only do social network purveyors possess vast user data, but these profiles will increasingly be updated and tied together using automated tools and mavatars databases. One such application is Facebook's aforementioned tool, Tag Suggest, which is designed to provide users with tagging suggestions for newly uploaded photos (Mitchell, 2012). This is done by scanning faces in photos and matching biometrics to data stored in the company's 'photo summary information' database, which is a repository of biometric data garnered from photos tagged by Facebook users. To populate this database, Facebook uses facial recognition algorithms to scan an image for biometric indicators, search its photo summary database, associate the new biometric data with a user's profile, and update its database with the new biometric data. This representation of the user's biometrics, along with the user profile, represents the heart of the mavatars concept because it ties together the user's identity with his or her biometric representation, thus forming a digital identity that extends beyond mere biometrics.

The biometric characteristics become part of and integrated with user profiles, neither of which are seen or managed by the user, but are rather generated and maintained by Facebook. Hidden user profiles such as these are not new in that behavioral metrics regarding users' actions, preferences, and other online behaviors are routinely captured and employed to track and predict user behaviors (Angwin, 2011). What is unique about tag suggestions is that Facebook maintains an avatar-like digital representation of the user's physical form that functions as a biometric representation of, at least in part, the user's Facebook identity in relation to the company's interactions with the user—and it includes the user's behavioral profile and characteristics. Further, the profile is not controlled by the user in any substantive manner and the user has opted in via the terms of service, which grants Facebook permission to build and use this profile. The digital signage and Facebook applications are each examples of existing technologies that are enabled through mavatars. In the next section we present a framework that can be used to categorize these, as well as other existing and future, applications.

3. From avatars to mavatars: The nature and scope of marketing avatar applications

The term *avatar* as applied to a user's embodied representation in an online setting was popularized by Neal Stephenson (1992) in his book *Snow Crash*. Subsequently, 'avatar' came to be associated with embodied virtual characters in immersive virtual environments (e.g., video games). In these and similar settings, the avatar is generally a representation that includes a virtual body that can move and interact with the objects and spaces in the 3D world. The term avatar has also been applied to visual representations (e.g., pictures of users) in other online venues such as Internet forums and social networks. In these environments, the user is able to choose the avatar that represents him. For example, when a user opens a new account in Second Life, he or she can select an avatar and customize its appearance.

Of course, social networks like Facebook include numerous images of users, and such representations have also been called avatars. This is because an avatar describes an online representation of a user and these images, individually and collectively, represent the user's online identity. As illustrated by a user's intent in projecting his or her identity using images on Facebook, the important feature of an avatar is not merely how and what the avatar looks like; it is also that the user has some degree of control over the avatar and its appearance (e.g., a user can select which images to upload or delete). As with any sign, avatars are used to make statements, and have a symbolism that is generally purposeful and incorporates the user's profile and representation online. In other words, the avatar is utilized by the user to project his or her persona.

In contrast, the mavatars concept has at its core a biometric representation that retains features of an

avatar because it is an embodied representation. Importantly, though, mavatars are created, managed, and used by entities other than the target. Biometrics have been employed for decades and databases of biometric data are not new; however, we use the term 'mavatars' to describe the application of using the biometric data for marketing and similar user applications and functions. As such, the term *mavatars* is specifically used to describe the biometric representation that is used for the particular function of representing the embodied persona, which includes not only the biometric data about the target but also the behavioral and contextual profile that defines the user's identity from the vendor's, marketer's, or system's perspective. As such, mavatars are more than merely biometric data; it is the 'package' that comes with building a biometric profile associated with the user's personal profile of preferences, behaviors, and history. Because a biometric representation of a customer, client, or user is robust and extensible, a number of applications for mavatars have been and will continue to be developed. As with many types of data about customers and users, the way that mavatars are created and managed will depend on the domain of the applications for which they will be used.

3.1. Use and choice: A framework of applications

We suggest two broad application domains demarcated in a manner similar to the way business-to-consumer (B2C) and consumer-to-consumer (C2C) ecommerce is differentiated; that is, will mavatars be used by groups or organizations for functions such as marketing or monitoring (B2C) or will mavatars be used to build individual peer-to-peer (P2P) applications? Put another way, we might ask whether the functionality associated with leveraging mavatars is put in the hands of organizations or, rather, a set of end users who will utilize the application to identify and interact with other individuals? In the case of marketing to consumers as an example of an organizational application, a vendor could focus on using mavatars in a manner similar to the way existing consumer profiles are used; that is, to accurately identify consumers' behaviors and identities and use these data to more accurately and effectively provision services to customers as they, for example, peruse digital signage in public spaces. Alternatively, when mavatars are used for P2P applications, the focus will be on enabling an end-user technology and service that takes advantage of facial biometric identification. For instance, consider a peer-to-peer application that would allow the user, via his or her cell phone and a downloaded app, to take a picture of someone at a high school reunion and help that user remember the classmate's name (Steel & Angwin, 2011).

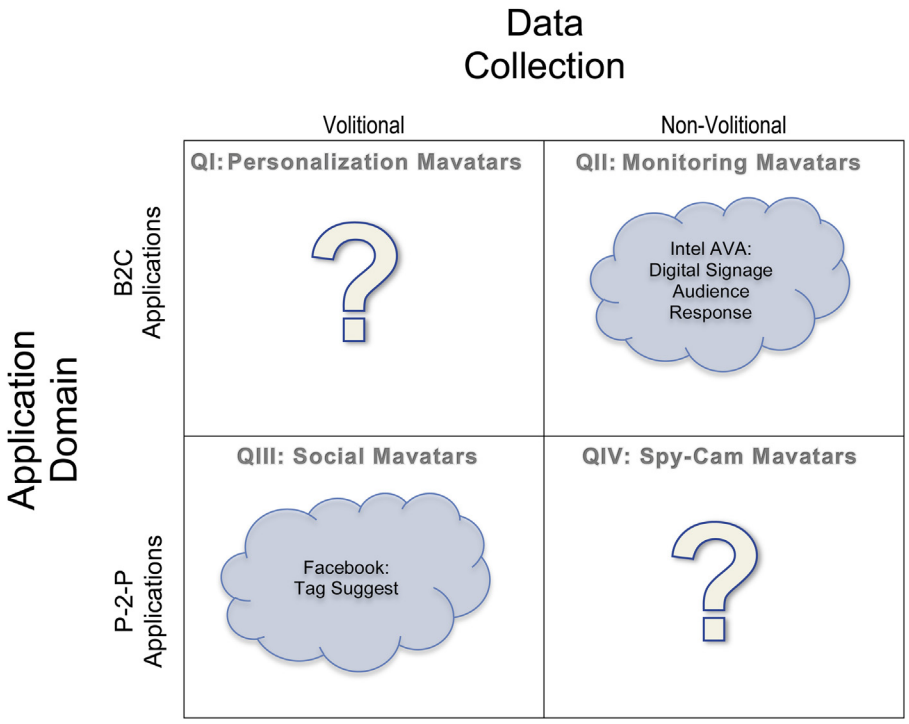
We also suggest that mavatars' use will be influenced by how data are collected. The important factor differentiating data collection procedures relates to whether the target being scanned assents to the data being collected and shared; that is, whether the target has volition to opt in or opt out. For example, Facebook collects user biometrics and does so with impunity because users opt in to facial recognition when they accept the terms of service (TOS). For current digital signage systems, the story is different. Specifically, facial recognition and audience response systems used with digital signs are designed to operate so that targets being observed maintain anonymity.

The review thus far suggests that two of the primary factors of import in classifying use of mavatars are the application domain (B2C versus P2P) and how the data are collected (volitional versus non-volitional). This suggests the framework shown in Figure 2. We discuss the implications of this framework next.

3.2. Implications of use and choice: Future mavatars applications

The two factors in our framework are represented on the two axes, and the two applications that have been highlighted thus far are shown in their respective quadrants. These particular applications are presented as exemplars; clearly, others exist, such as law enforcement applications or use by government agencies for homeland security. We label Quadrant II applications *Monitoring Mavatars* because, as with Intel's Anonymous Video Analytics (AVA) audience response system, these tools will monitor and oversee targets without their consent. Quadrant III portrays volitional peer-to-peer applications *Social Mavatars*, which will follow the general functionality typified by Facebook's Tag Suggest. It is notable that our framework contains two vacant quadrants. This begs the question: What types of applications will occupy these cells? The empty cells in Figure 2 represent applications that have yet to be exploited in a commercial or widely used manner. This framework is important for developers, vendors, policy makers, and the public because it provides a way to understand where development opportunities exist and the nature of the applications that will likely fill these empty niches. We highlight several example applications and the factors that define the characteristics of these applications in Figure 3, and discuss details about how we expect a few of these applications to be designed and used.

Figure 2. Mavatar framework

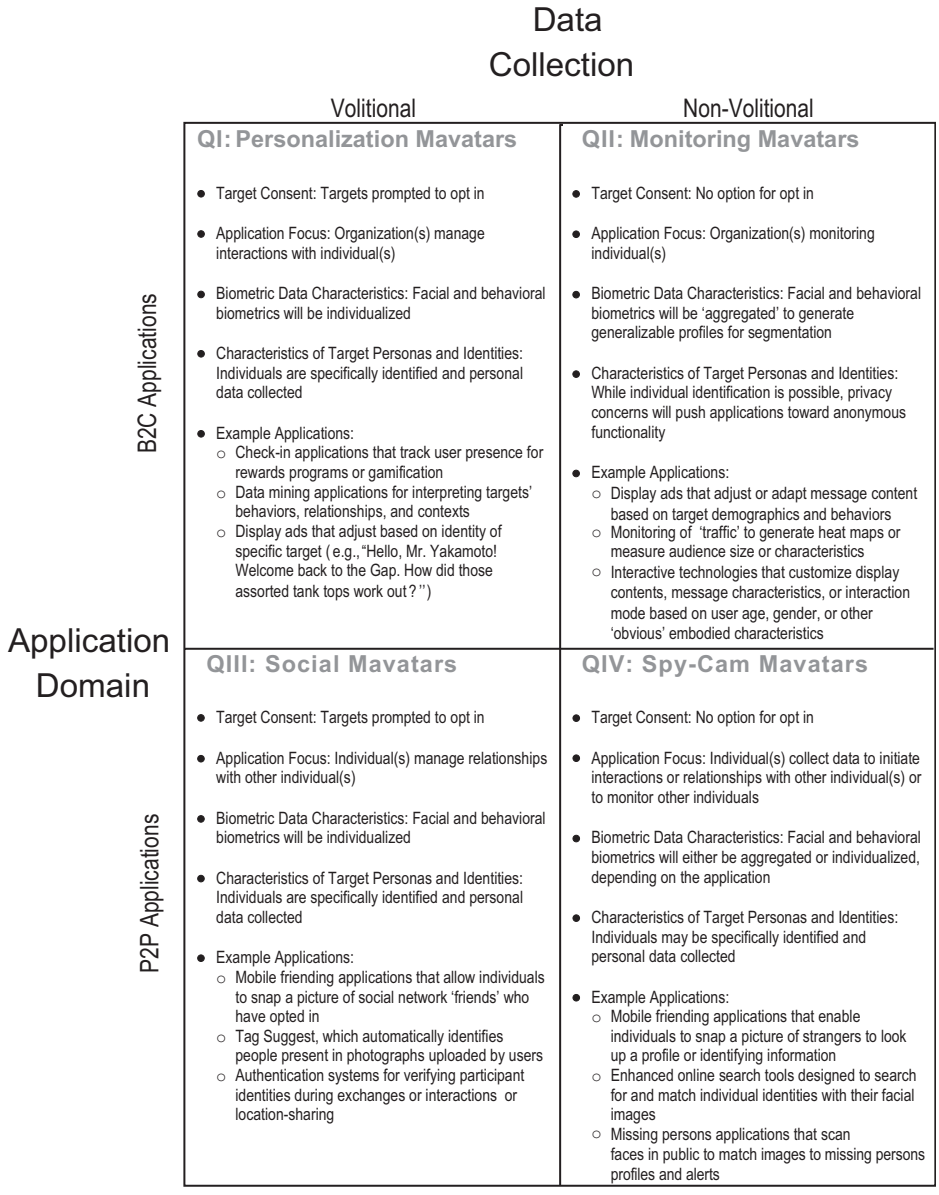


We refer to applications that will occupy Quadrant I as *Personalization Mavatars*. This represents a domain that, in other contexts, has been exploited by opt-in applications that combine customer profiles with marketing or similar objectives. For example, Amazon uses a customer's prior selections and purchases to make suggestions to returning customers and to customize solicitations. Nevertheless, applications such as those used by Amazon do not currently incorporate mavatars to manage customer engagement. We expect that there are two contexts where mavatars will be used to enhance or expand on the functionality of applications in Quadrant I: (1) in online applications involving image capture/scanning and contextual interpretation, and (2) in public spaces involving interactive digital signage or kiosks.

For online applications it is likely that Facebook and other social networking vendors are already using, even if at the experimental stage, contextual information in images to examine social relations and the preferences of their users. Because users opt in to the use of facial recognition, Facebook would be able to apply mavatars for a variety of marketing and user services that would result in the types of B2C applications we envision in this domain. For example, people make a variety of inferences based on external appearance, such as whether someone wears or doesn't wear brand-name clothes, is located in a particular venue such as a bar or a church, or is alone or in a group. Consider the following scenario: A target is in a picture with a dog on a leash; the target is wearing an "I love Budweiser" t-shirt and is holding hands with a young woman. It would presumably be possible to infer information about the target that he did not post directly to his profile: he owns a dog; he takes the dog on walks; he likes Budweiser, perhaps even all kinds of beer; and he is in a relationship. It is likely that vendors will increasingly use image scans for automated interpretation of some of these more subtle cultural symbols and for behavioral markers (Maji, Bourdev, & Malik, 2011). The value offered to vendors is that the content of images will often include a more realistic 'picture' of a user than he or she might be willing to explicitly divulge in his or her profile. As such, mavatars—as a representation of the user in the context of his or her lived experience—are much more than merely bionic representations or flat images. We therefore expect that such information will routinely be part of what is mined from the content of images posted to social networks such as Facebook, and that this rich information will be a necessity for enhancing customer engagement.

Concerning signage used for interactions with customers or the public, we expect that digital signage will eventually evolve past the types of anonymous systems represented in Quadrant II (i.e., *Monitoring Mavatars*). Specifically, it is likely that mavatars will eventually be used with digital signage to link customers with their unique profiles, but privacy concerns have thus far precluded applications in this

Figure 3. Characteristics and examples of present and expected future mavatars applications



domain from being exploited in a widespread manner. Nevertheless, the technology to enable this functionality is not fundamentally different from anonymous systems. In fact, the FaceLook application is an interactive kiosk that provides users with a peer-to-peer application (i.e., updating a user profile with a location-based image), but it could also be extended to deliver advertisements and coupons from a vendor and to garner data about behaviors that could be fed back into mavatar profiles (Hall, 2012). We expect that with the right incentives, customers will opt in to such systems, thereby enabling vendors to collect a richer set of data with which to customize their client interactions.

Quadrant IV represents *Spy-Cam Mavatars* and includes applications where targets are not offered the opportunity to opt in and the tools support P2P functions. The requisite functionality of such an application would be that it uses mavatars to identify the target and build a P2P application around this identified profile. While Face.com and other facial recognition vendors have APIs that support recognition applications for 'any photos,' no widely-distributed consumer applications yet include this functionality. It is noteworthy that Facebook purchased Face.com, with indications that Facebook is interested in mobile facial recognition applications (Reisinger, 2012). Though no commercial products are common in this space, a picture of this type of application is represented in currently available iris and facial-scanning technologies that have been developed for law enforcement applications

(Shanker, 2012). BI^2 Technologies markets the Mobile Offender Recognition and Information System, or MORIS, which is implemented on a mobile phone and is used to capture an image of the face and iris of the target. This image is then matched against a law enforcement database containing facial and iris biometrics information to verify the identities of suspects or missing persons (Denman, Bialkowski, Fookes, & Sridharan, 2011). While the law enforcement application would be a Quadrant II application if it were in the commercial space, it demonstrates the feasibility of this technology and its potential for widespread use.

Barring regulatory restrictions, we expect similar P2P technologies will soon appear for use by the general public. One possible application would entail an identification system via which the user could take a picture and use facial recognition software to match it against images in a mavatars database. Of course, the difficulty would lie in building these mavatars without access to existing profiles. To enable such an application, the mavatar profiles would need to be constructed by an entity with the resources to do so by scanning images of faces gleaned from the Internet and combining this with user information. It is noteworthy that Google recently created an application that could be used with an Android phone to scan faces and identify them using Google's database (Newman, 2011), and that the company purchased PittPatt, a facial recognition software firm (Rao, 2012). It is also possible that Facebook is considering such an application, given that the company recently acquired Face.com and its tools for facial detection and recognition. In the end, however, it is also possible that a proprietary mavatars database may not be needed, given that researchers have developed and tested iPhone-based applications for P2P identification that only need publically-available imagery from social networks (Allen, 2008; Angwin, 2011). Clearly, Spy-Cam Mavatars are feasible; what presumably keep these types of applications from being released by commercial entities are privacy concerns.

4. Privacy in the age of mavatars

As our discussion suggests, the use of tools for creating, managing, and employing mavatars will not be without controversy. Privacy is at the core of concerns about facial recognition applications in general and ultimately lies at the heart of concerns that will likely arise with greater proliferation of the use of mavatars. Researchers examining privacy have identified three privacy rights: (1) the right to be left alone, (2) the right to control one's information or limit access, and (3) the right to protect one's individuality (Norberg, Horne, & Horne, 2009). Privacy concerns related to corporate use of marketing databases are not new. Indeed, Langenderfer and Miyazaki (2009, p. 384) point out:

> As databases play an increasingly important role in our lives, there is a danger that we will lose the ability to define ourselves, having surrendered the definition of ourselves to the data gathering entities, often unregulated and beyond our control.

Mavatars exacerbate the problem because both B2C (e.g., marketing) and P2P applications will take advantage of immutable biometric characteristics in combination with the 'definition' of ourselves that we divulge in our profiles or through our behaviors. An important implication of this is that each vendor collecting and managing mavatars will be able to develop customer profiles that are more consistent; in fact, these profiles will likely be more consistent across vendors even when collected and managed by different organizations. This is due, in part, to the fact that while the behavioral and other descriptive components of a mavatars profile will vary across vendors because users may divulge different information or behave differently in various contexts, the biometric representation of each user will largely be the same for each vendor collecting data because an individual's biometric features will be the same regardless of the venue in which or the mode by which the data were collected. The result is that mavatars held by different vendors and organizations will generally be quite similar.

As is the case with current opt-in applications, most consumers do not fully appreciate how their profiles are built, aggregated, and used, and the associated risks to identity and privacy (Langenderfer & Miyazaki, 2009). Nevertheless, vendors and corporate users have thus far been reluctant to embrace applications that have the potential to be perceived by consumers as too invasive. For example, Intel (2012) freely recognizes apprehension regarding public perceptions of privacy invasion and protection surrounding Anonymous Video Analytics, the company's audience response system. This concern for privacy is directly related to the design of these systems; that is, they are designed to monitor targeted viewers in public spaces and, most importantly, they do not currently enable the person being observed to opt out. As demonstrated by a recent controversial monitoring program involving Wi-Fi tracking at a pair of malls, even anonymous tracking systems must be managed carefully by vendors and retailers (Censky, 2012). As this example illustrates, there is a great deal of

interest in collecting these types of data, so the challenge for vendors will be to balance this interest with privacy rights.

While such marketing-oriented tracking systems seem ominous, these systems generally focus on groups of people and, in the case of current uses, emphasize anonymity. Because Quadrant IV applications focus on the identification of individuals, they would seem to represent a profound threat to privacy. For example, the aforementioned MORIS facial recognition technology has attracted considerable attention from civil liberties groups because it is thought to threaten privacy, having been demonstrated to be effective for individualized surveillance related to tracking Afghani insurgents (Shanker, 2012). While corporate and government use of such systems is of concern, we also suggest that Quadrant IV applications create serious threats to privacy because of the potential for abuse and misuse. When we are in public places or post content online, we should recognize that we are sacrificing some level of privacy; however, the security and privacy implications associated with Spy-Cam Mavatars are profound. Obviously, the potential for identity theft, stalking, and privacy invasion will increase as applications based on mavatars become more accessible and integrated into mobile technology.

Our review suggests the public will be most concerned with the type of applications associated with Quadrants II and IV, primarily because opting out is not an option here. It is in this domain that industry self-governance and regulatory controls are most justified. For example, while a facial recognition application designed for end users might be constructed without an opt-in feature, it is possible that an application could be designed so that it cannot be used unless the target opts in (i.e., it is designed as a Quadrant III rather than a Quadrant IV application). While rogue applications operating in Quadrant IV will likely be developed, we are hopeful that responsible software developers and organizations would avoid involvement with this type of application and proffer opt-in alternatives.

Consumer databases have been with us for some time now and the scholarship addressing privacy suggests that the most reasonable solution would be to ''adopt more of an 'opt-in' culture'' (Norberg et al., 2009, p. 511). We suggest that while this cultural solution might work with consumer databases compiled from website behavior and purchase histories, the advent of mavatars changes the playing field such that a more robust way of viewing privacy protection is needed. For example, even with 'standard' consumer profiles, many vendors use opt-out policies, which puts the onus on the consumer (Morozov, 2011). As mavatars become an increasingly important part of interactions with vendors and others, it will be critical that individuals have the opportunity to manipulate their online profiles. This would bring mavatars closer to avatars; that is, a representation of one's identity controlled by the person being represented by the mavatars data. This is because these data are more akin to health data than to other types of behavioral and economic data. Mavatars are highly individualized, immutable; as a result, one could not 'escape' one's mavatars profile if it is largely the same, regardless of who uses it or the context in which it is used.

HIPAA Privacy Rules not only require patients to opt in, but also require that patients have a say in how their data are managed and used. Offering greater control and flexibility to the public in analogous ways to HIPAA would, we think, be a good thing and should be an important right for the public and consumers. For example, the proposed Commercial Privacy Bill of Rights Act (2011) is designed to offer some of the safeguards that would help people manage mavatars, such as the right to inspect databases and purge records.

We believe it is important for individuals to have input regarding how mavatars are created and used so that they can correct erroneous representations or, ultimately, purge their profiles (i.e., to opt out). While many people may indeed choose to opt out, we expect that more will either ignore their profiles or actually refine the profile's accuracy. An analog is Google's Ad Preferences, which collects and defines user profiles based on search behavior and divulges this profile to advertisers. Google offers users access to their Google-generated profile and also enables them to purge or correct it (Google, 2010). Many users do, in fact, enhance and refine these profiles presumably because this means they will receive fewer irrelevant ads. Ultimately, other vendors will need to manage profiles in a similar way because regulators will likely tighten privacy laws as technologies and applications continue to impinge on privacy. For example, the European Union (EU) is currently proposing stricter privacy laws under which companies will be required to obtain consent, disclose to customers what information they store about them, and ensure that customers can correct or purge that information (Sengupta, 2012). Laws and regulations in the United States are not nearly as strict as those in the European Union (Maass, 2012); however, it is likely that many multinational firms operating in the U.S. will follow the stricter EU laws because of compliance, consistency, and to maintain goodwill with the public. As a result, it is important for application developers, IT managers, and marketers to focus system designs, usage policies, and

industry self-regulation on making access to and control of personal mavatars a standard part of their development and use (FCC, 2012).

5. Implications for marketing and business

As physical entities, we live in and through our bodies and, as social creatures, our physical form and appearance carries with it important information that we can use to communicate with others (Berger, 1998). These embodied codes are important in all social interactions, including those where exchanges and commercial transactions take place. Up until a few hundred years ago, a visual inspection of patrons and a handshake represented a fundamental part of doing business; however, this changed when Richard Sears popularized catalog retailing and mass marketing. Sears succeeded because he knew his customer, the rural farmer, having himself grown up on a farm. His intimate knowledge carried his business forward, but as this business model proliferated, the intimate knowledge of the customer waned. Since that time, marketers have endeavored to recapture an intimate understanding of customers, first with segmentation, later with relationship and customer management, and most recently with detailed customer profiling and tracking. Yet, while behavioral, demographic, and historical information is important, what remained out of reach was the ability to understand the customer in the context of his or her daily activities and recapture the information that once was available only through face-to-face encounters. Facial recognition technologies are spurring opportunities to create and manage what we term *mavatars*, which offer organizations the chance to reconnect with customers using an age-old technique: recognizing who they are based on their appearance.

In the end, it is likely that we will see—in one form or another—the types of identification systems we have described proliferate. This proliferation will occur due to the fact that mavatars offer the potential to create new options for marketing and for managing social relationships. As services such as FourSquare demonstrate, consumers often opt in when they determine that the value they are offered by a product or service outweighs the risks they face by agreeing to divulge personal information.

Consequently, it is likely that consumers will accept mutually beneficial applications and marketing services in several of the application categories we have delineated. The challenge for retailers and developers is to find the point where benefits accrue to relevant stakeholders. For example, customers frequently are bombarded with irrelevant text, email, and display images, which are often ignored or dismissed (i.e., they develop display blindness). Marketers can take advantage of mavatars to offer highly customized and relevant advertising, public information, and promotional materials; this action has the potential to reduce 'noise' encountered by consumers in venues where they are otherwise bombarded by irrelevant information. A mutually beneficial application would exist when consumers are presented with personalized information and advertising that is relevant, contextual, and useful. While we have painted a picture that highlights the potential risks to privacy associated with the applications in Quadrants II and IV, we expect that beneficial applications will also be available in these domains (e.g., child recovery applications associated with Amber Alerts). As a result, responsible use by managers, proactive industry, and thoughtful government regulation will be important as applications proliferate. We hope that the framework offered in this article will be useful to managers and others in identifying these mutually beneficial applications.

References

Allen, D. (2008, August 5). *'Minority report' style gesture-based interfaces*. Retrieved June 10, 2012, from http://www.pcworld.com/article/157231/minority_report_style_gesturebased_interfaces.html

Angwin, J. (2011, August 1). *Face-ID tools pose new risk*. Retrieved November 18, 2011, from http://online.wsj.com/article/SB10001424053111903341404576480371062384798.html

Berger, A. A. (1998). *Signs in contemporary culture: An introduction to semiotics*. Salem, WI: Sheffield Publishing Company.

Burke, R. R. (2009). Behavioral effects of digital signage. *Journal of Advertising Research, 49*(2), 180—185.

Butler, C. (2012, June 22). *Will consumers opt-in for the 'store of the future?'* Retrieved June 24, 2012, from www.retailcustomerexperience.com/blog/8289/Will-consumers-opt-in-for-the-store-of-the-future

Censky, A. (2012, November 28). *Malls stop tracking shoppers' cell phones*. Retrieved June 25, 2012, from money.cnn.com/2011/11/28/news/economy/malls_track_shoppers_cell_phones/index.htm

Christiansen, L. (2011). Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven? *Business Horizons, 54*(6), 509—514.

Commercial Privacy Bill of Rights Act. (2011). *112th Congress, 1st Session, BAG11284*.

Denman, S., Bialkowski, A., Fookes, C., & Sridharan, S. (2011). Determining operational measures from multi-camera surveillance systems using soft biometrics. Published in *Proceedings of the 8th IEEE International Conference on Advanced Video and Signal Based Surveillance* (pp. 462—467), Klagenfurt, Austria.

Digital ad overload proves a major turn-off for consumers. (2012, February 27). Retrieved June 29, 2012, from www.

marketingcharts.com/direct/digital-ad-overload-proves-a-major-turn-off-for-consumers-21263/

FCC. (2012). *Location-Based services: An overview of opportunities and other considerations*. Retrieved June 26, 2012, from www.fcc.gov/document/location-based-services-report

Google. (2010). *Ads preferences: Internet-based advertising: How it works*. Retrieved June 6, 2012, from www.google.com/ads/preferences/html/about.html

Hall, C. (2012, August 28). *Coca-Cola facial recognition kiosk uploads straight to Facebook*. Retrieved May 30, 2012, from http://www.digitalsignagetoday.com/article/183849/Coca-Cola-facial-recognition-kiosk-uploads-straight-to-Facebook-Video

Intel. (2012). *Digital signage*. Retrieved June 24, 2012, from http://www.intel.com/content/www/us/en/intelligent-systems/digital-signage/digital-signage-that-displays-messages-and-measures-effectiveness.html?wapkw=digital+signage

Johnson, H. H., & Kim, S. M. (2009). When strategy pales: Lessons from the department store industry. *Business Horizons, 52*(1), 583—593.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *The Journal of Consumer Affairs, 43*(3), 380—388.

Lorrette, K. (2011). *Digital signage as a marketing communications tool*. Retrieved August 26, 2011, from www.ehow.com/about_6537336_digital-signage-marketing-communications-tool.htm

Maass, P. (2012). *Your FTC privacy watchdogs: Low-Tech, defensive, toothless*. Retrieved June 6, 2012, from www.wired.com/threatlevel/2012/06/ftc-fail/all/

Maji, S., Bourdev, L., & Malik, J. (2011). Action recognition from a distributed representation of pose and appearance. *Computer Vision and Pattern Recognition,* 3177—3184.

Marketers lack confidence in complex digital marketing abilities. (2012, May 9). Retrieved June 29, 2012, from www.marketingcharts.com/direct/marketers-lack-confidence-in-complex-digital-marketing-capabilities-22053/

Mitchell, J. (2012, June 30). *Making photo tagging easier.* Retrieved May 18, 2012, from www.facebook.com/blog.php?post=467145887130

Morozov, E. (2011, December 19). *Saving face: How Google, Facebook, and other tech companies hide behind "opt-in" policies*. Retrieved June 29, 2012, from http://www.slate.com/articles/technology/future_tense/2011/12/google_s_and_facebook_s_facial_recognition_opt_in_policies_are_a_smokescreen_.html

Newman, J. (2011, April 1). *Google won't release awesome facial recognition app*. Retrieved September 1, 2011, from www.pcworld.com/article/224007/google_wont_release_awesome_facial_ recognition_app.html

Norberg, P., Horne, D. A., & Horne, D. R. (2009). Standing in the footprint: Including the self in the privacy debate and policy development. *The Journal of Consumer Affairs, 43*(3), 495—515.

Peters, A., & Mennecke, B. E. (2011). The role of dynamic digital menu boards in consumer decision making. Published in *Proceedings of CHI EA'11* (pp. 1693—1698), Vancouver BC, Canada.

Pondent, C. S. (2012). *Implications for retail adoption of digital signage systems*. Retrieved May 26, 2012, from www.ehow.com/info_7781325_implications-adoption-digital-signage-systems.html

Rao, L. (2012, July 22). *Google acquires facial recognition software company PittPatt*. Retrieved June 1, 2012, from techcrunch.com/google-acquires-facial-recognition-software-company-pittpatt/

Reisinger, D. (2012). *Facebook acquires Face.com for undisclosed sum*. Retrieved June 20, 2012, from news.cnet.com/8301-1023_3-57455287-93/facebook-acquires-face.com-for-undisclosed-sum/

Roy, A., & Chattopadhyay, S. P. (2010). Stealth marketing as a strategy. *Business Horizons, 53*(1), 69—79.

Sengupta, S. (2012, January 23). *Europe weighs tough law on online privacy.* Retrieved June 6, 2012, from www.nytimes.com/2012/01/24/technology/europe-weighs-a-tough-law-on-online-privacy-and-user-data.html

Shanker, T. (2012, July 13). *To track militants, U.S. has system that never forgets a face*. Retrieved May 12, 2012, from http://www.nytimes.com/2011/07/14/world/asia/14identity.html?pagewanted=all&_r=0

Steel, E., & Angwin, J. (2011, August 16). *Device raises fear of facial profiling*. Retrieved September 1, 2011, from online.wsj.com/article/SB10001424052702303678704576440253307985070.html

Stephenson, N. (1992). *Snow crash*. New York: Bantam Books.