International Journal of Information Management 36 (2016) 735–747

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system

Darrell Carpenter[a], Michele Maasberg[a], Chelsea Hicks[a], Xiaogang Chen[b,*]

[a] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, 1 UTSA Circle, San Antonio, TX 78249, United States
[b] School of Business Administration at Southwestern University of Finance and Economics, No. 555 LiuTai Ave, Wenjiang District, Chengdu 610074, China

ARTICLE INFO

Article history:
Received 12 October 2015
Received in revised form 25 February 2016
Accepted 27 February 2016
Available online 14 May 2016

Keywords:
Crisis response systems
Biometrics
Privacy
Case study
Ethnicity
Human-computer interaction

ABSTRACT

Biometric technology is rapidly gaining popularity as an access control mechanism in the workplace. In some instances, systems relying on biometric technology for access control have not been well received by employees. One potential reason for resistance may be perceived privacy issues associated with organizational collection and use of biometric data. This research draws on previous organizational information handling and procedural fairness literature to frame and examine these underlying privacy issues. Perceived accountability, perceived vulnerability, and distrust were distilled from the previous literature as the primary dimensions of employee privacy concerns related to biometric technology. This study assesses the effects of these privacy concerns, how they vary based on the cultural influences of Anglos and Hispanics.

Fire ground accountability is a critical management objective in the firefighting domain. In multi-unit or multi-agency crisis response scenarios, the on-scene incident commander tracks and accounts for each first responder. This research designed and deployed a new fire ground accountability system that tracked firefighters through finger pattern-based biometric logins to their assigned positions on the firefighting apparatus. An instrument measuring level of privacy concern on three underlying dimensions and demographic data was developed, validated and administered in a quasi-experimental field study. A pre-test–post-test survey methodology was employed to detect potential differences in privacy concerns as familiarity with the system increased. The study shows that Anglo and Hispanic subjects frame privacy issues differently associated with use of biometric technology in a fire ground accountability system. Finally, the study showed that some privacy concerns such as distrust and perceived vulnerability can be alleviated through system use with changes in post-use privacy concerns moderated by ethnic affiliation.

1. Introduction

The use of biometric technology has grown substantially in recent years. In many instances, this technology has been well-received. One study reported that only eight percent of users who were required to have a biometric embedded in their driver's license thought the technology invaded their privacy (Jain, Bolle, & Pankanti, 2002). Despite the success of biometrics in some contexts, anecdotal evidence from privacy organizations (Abernathy & Tien, 2006; EFF, 2006; O'Donoghue, 2001) suggests that use of biometrics in the workplace results in significant employee privacy concerns. Additionally, case law shows that the deployment of biometrics in the workplace may lead to a number of undesirable outcomes, including enticing employees to unionize (York & Carty, 2006) or seek renegotiation of existing labor contracts (Kelly & Herbert, 2004).

Employee privacy concerns may be rooted in the uncertainty of how biometric data may be used. For instance, it is well-known that carriers of certain genetic disorders including Down's syndrome can be detected from fingerprint patterns (Faundez-Zanuy, 2005; Zhai & Qui, 2010). Additionally, some forms of skin cancer can be detected through vascular scans (Hay, 2003). Using biometric data for such functions could allow systematic discrimination of people who carry certain genetic markers or diseases.

An employee's trust in the organization to act ethically is also at issue. While organizations may claim they will only use biometric technology for system access, there is little legal protection for employees if the organization decides to expand its usage of collected biometric data (Levinson, 2009). While the stated

* Corresponding author.
E-mail addresses: Darrell.Carpenter@utsa.edu (D. Carpenter), Michele.Maasberg@utsa.edu (M. Maasberg), Chelsea.Hicks@utsa.edu (C. Hicks), Chenxg@swufe.edu.cn (X. Chen).

http://dx.doi.org/10.1016/j.ijinfomgt.2016.02.013
0268-4012/

purpose of a biometric authentication system may be securing the organization's information technology resources, unscrupulous organizations could surreptitiously use biometric data for purposes unrelated to this espoused objective. Examples of potential surreptitious use include criminal history inquiries (Cole, 2004) and immigration status checks (Bump, 2008; Zureik, 2004).

The specific privacy concerns associated with biometric technology in the workplace have not been fully explored and defined. This research identifies three core dimensions of biometric privacy concern and assesses their impact on acceptance and use of a crisis response system. Improved knowledge of employee privacy concerns will help organizations address those concerns and mitigate negative impacts on the acceptance of systems incorporating biometric technology. This research further examines the influence of Anglo and Hispanic ethnic cultural differences on privacy concerns within the context of a biometrically-enabled fire ground accountability system.

2. Literature review

2.1. Dimensions of information privacy concern in the employment context

The introduction of new technologies that are construed to impact privacy may lessen employee acceptance of new systems. Jones, Anton, and Earp (2007) found that there was substantial uncertainty surrounding the privacy impact of digital authentication technologies. They further found that a third of respondents were concerned with the privacy implications of fingerprint scans and that the level of concern was highly context dependent. A review of the extant literature on employee privacy reveals three primary themes that provide insight on the issue of workplace privacy: 1) the scope of monitoring, 2) whether the system is procedurally just or fair, and 3) whether the users trust the organization to use monitoring data only for its intended purpose. These themes describe the organizational practices that generate concern and are reframed below in an employee-centric context.

2.2. Employee accountability perceptions

Perceived accountability is the degree to which employees believe they will be held more accountable for their actions when they log in with a biometric sample than when they log into a system via other means. Employees expect to provide limited personal information and accept some level of job performance monitoring in exchange for appropriate compensation. The collection of routine personal information and performance-related monitoring is usually viewed as being relevant to the employers' business objectives. Previous studies have found that employees believe it is acceptable for management to monitor employees (Grant & Higgins, 1991; Oz, Glass, & Behling, 1999). However, other studies have argued that employers need to look beyond their legal rights and consider the adverse effects on employee morale when considering monitoring efforts, especially when monitoring personal conduct during break periods or activities outside the work environment (Friedman & Reed, 2007; Tolchinsky et al., 1981). When organizational monitoring activities are not directly related to performance, employees tend to perceive the monitoring as an invasion of privacy (Alder, 2001; Alder & Ambrose, 2005; Alge, 2001; Ambrose, Alder, & Noel, 1998).

While employees often perceive a right to privacy in email communications, employers may also assert a right to monitor these systems. In early email system deployments, the privacy rights of employees with regard to employer-owned email systems were often unclear (Cappel, 1995; Oz et al., 1999). More recently, legal rulings have clearly favored the right of the employer to monitor email if they have reasonable business concerns for doing so (Friedman & Reed, 2007). However, Sipior and Ward (1995) assert that employees are likely to perceive email monitoring as invasive. In terms of monitoring scope, the email example supports the notion that employees will not accept broad monitoring activities even when legitimate business purposes are evident (Cappel, 1995).

Although employees may perceive different types of electronic monitoring as invasive, the impact of this invasiveness is sparsely documented through empirical evidence. Research has found that employees modify their behavior when they are being monitored (Stanton & Weiss, 2000). For example, more skilled employees were found to produce more work when they perceived they were being monitored while low skill employees were found to produce less work when being monitored (Aiello & Kolb, 1995; Urbaczewski & Jessup, 2002). Both more skilled and less skilled employees reported higher stress when being monitored, and lower job satisfaction (Aiello & Kolb, 1995; Urbaczewski & Jessup, 2002). Overall, the literature on electronic monitoring supports the notion that employees are concerned about systematic monitoring in the workplace and desire to retain some level of anonymity (Grant & Higgins, 1991; Oz et al., 1999). We posit that electronic monitoring leads to perceptions of increased accountability for an employee's actions. This perception, which may result in adverse outcomes for the employee, creates privacy concerns in the employment context.

2.3. Employee vulnerability perceptions

Perceived vulnerability is the degree to which employees believes their stored biometric sample is susceptible to both external threats and internal unauthorized access. Stone, Gueutal, Gardner, and McClure (1983) suggest that individuals are concerned with collection, storage, use and release practices of organizations. Specific areas of concern include understanding what is being collected, the capability to impact that collection, the opportunity to consent to collection, and the physical or psychological intrusiveness of the information collection procedures (Stone & Stone, 1990). Empirical evidence supports this contention through findings that perceptions of privacy invasions were correlated with consequences after disclosure and level of control over information (Fusilier & Hoyer, 1980; Stone et al., 1983; Tolchinsky et al., 1981). Culnan (1993) noted similar dimensions of acquisition, use and transfer of information as privacy concerns in direct marketing campaigns. There were different nuances to the concerns when considering internal customers, external customers or prospective customers. Brandimarte, Acquisti, and Loewenstein (2010) found that users with greater control over publication were more willing to disclose private information, even when they knew they could not control subsequent access to the published data.

In an empirical study, Smith, Milberg, and Burke (1996) found that collection, unauthorized use, errors, and improper access were significant concerns regarding organizational privacy practices. They also identified reduced judgment (reliance on automated decision-making algorithms) and combining of data (integrating data collected for different purposes) as secondary concerns related to organizational practices. Smith et al. (1996) also found significant correlations between privacy concerns and personality factors including trust/distrust, paranoia, and social criticism. Stewart and Segars (2002) validated the Smith et al. (1996) model using confirmatory factor analysis. They suggested procedural fairness (Culnan & Armstrong, 1999), environmental control (Hoffman, Novak, & Peralta, 1999), and control over secondary use of information (Hoffman et al., 1999) as additional factors potentially impacting concern for organizational privacy practices.