Service industries, such as health care and banking, process large amounts of sensitive customer data in their daily transactions. The information obtained from this data frequently supports the competitive strategies of organizations while concurrently causing uncertainty and concern from the customer. Furthermore and given the service orientation of these data, poor data quality can result in extensive social and economic impacts. As a result, data practices and the employees who process the data must be managed in a cautious and thorough manner to thwart any privacy violations. This article explores employees’ privacy orientation in their respective sector, health care or banking, through a parsimonious 15-item instrument. Our results indicate that health care professionals are largely concerned about errors in patient information whereas banking professionals are concerned about improper access of customer information—thereby suggesting differences in perceived privacy practices among these 2 service sectors. Several explanations are offered for the concerns that surfaced from the 2 groups. Therefore, our results build on a data quality hierarchical framework consisting of accuracy, appropriate amount of data, accessibility, and access security. Our results hold public policy, legal, and security implications to the managerial staff at both health care and banking organizations. To date, there has been little research that gives substantial insight into the privacy practices of service industry workers, such as banking and health care employees. In this article, we discuss the implications of these findings and suggest directions for future research.

1. INTRODUCTION

Information privacy is an important area that warrants consideration during any decision making process in today’s organizations [1–4]. Privacy is also an organiza-
tional issue, indicating that management needs a clearer understanding of service workers’ privacy orientation. Prior research [5] suggests that customer orientation is an individual-level construct that is central to a service organization’s ability to be market oriented. We posit that a “privacy orientation” is, likewise, an individual-level concept that impacts an organization’s capability to be privacy oriented. The notion of privacy orientation is especially challenging for today’s organizations that have the infrastructure and business need to collect data as well as those that realize the value of electronic data management and storage. Such organizations include those that utilize data about consumers to facilitate marketing, customer relationship management (CRM), and supply chain activities.

Although privacy orientation offers one approach to describing privacy practices among service professionals, a data quality framework offers a salient manner to better conceptualize our findings. Wang and Strong [6] determined that data quality (DQ) is a multidimensional construct that consists of privacy elements that provide a theoretical basis for our research. That is, both frameworks consist of accuracy, relevancy, and accessibility dimensions that stand to impact how professionals do work and the knowledge practices adhered to in their daily activities.

Health care and financial data can be used to personalize and enrich the service experience of users while enabling organizations to promote business intelligence under conditions of industry competition and legislative requirements [7, 8]; gathering such data can also be seen as potentially abusive when considering the sensitivity of health care or banking (non)disclosure. This is particularly the case of recent legislation that lends itself to trends beyond data accuracy and protection to improved data quality for critical knowledge and modes of work practices [6, 9]. To date, privacy protection laws in the United States include coverage for health care data (the Health Information Portability and Accountability Act; HIPAA), information obtained from and/or about children (the Children’s Online Privacy Protection Act; COPPA) and financial data (the Gramm–Leach–Bliley Act; GLBA) [10–14]. This implies that the U.S. legal environment has deemed health care and financial sectors as being in need of guidance with regard to consumer privacy protection; therefore, we seek to explore the privacy orientation of health and banking service professionals—as their daily activities are met with a high degree of interaction with personal consumer information in an on-the-job context.

2. THEORETICAL BACKGROUND

Brown et al. [5] defined customer orientation as an employee’s tendency or predisposition to meet customer needs in an on-the-job context. They suggested that customer orientation is central to a service sector organization’s ability to be market oriented. Furthermore, they proposed that customer/market orientation is multidimensional consisting of needs and enjoyment facets. The needs dimension represented service workers’ ability to satisfy customer needs while enjoyment describes the pleasure workers experience via customer interactions.

Health care and banking organizations in the United States are becoming similarly more customer focused in their efforts to attract, maintain, and delight con-
sumers under highly intensive competitive market conditions and increasing legislative requirements. These organizations engage in highly sensitive transactions with consumers and must walk a fine line of gathering necessary information while protecting customer privacy and the quality of personal data. Information use is a staple of today’s business, but the gain from information use and the (mis)management of that data must be balanced with the user’s perceived cost of loss of privacy. This is particularly critical in the health care and banking industries in which the widespread use of networked systems and the Internet facilitate the collection and storage of consumer data. In addition, information integrity, which is defined as the dependability and trustworthiness of information, requires that health care and banking datasets lend themselves to the highest degrees of accuracy, consistency, and reliability—thus, moving toward elevated levels of data quality to facilitate knowledge and the work of service professionals [9]. Hence, the information integrity of these data can be both a resource and bottleneck to attain effective service delivery [15]. Understanding and protecting personal privacy in information systems is even more critical in these industries where violating customer privacy in the event of misuse, whether accidentally or intentionally, can have detrimental effects [16, 17]. Moreover, such actions can result in customer dissatisfaction, patronage shifts, personal litigation, and switching service providers in highly competitive environments that are becoming more perceptive to consumers right to choice [18].

Beyond information integrity models [15], data quality models offer theoretical frameworks to conceptualize our work. In particular, the Wang and Strong [6] hierarchical framework of data quality encapsulates the dimensions of accuracy, accessibility, completeness, appropriate amount of data, and access security, just to name a few. Figure 1 illustrates that data quality falls into four categories: intrinsic, conceptual, representational, and accessibility. Each category is defined by its underlying dimensions and led to the refinement of DQ in four categories ([6], p. 18):

1. The extent to which data values are in conformance with actual or true values.
2. The extent to which data are applicable to the task of the data user.
3. The extent to which data are presented in an intelligible and clear manner.
4. The extent to which data are available or obtainable.

Specific to our research, this data quality framework offers that intrinsic data quality assesses accuracy while contextual data quality captures appropriateness of the amount of data along with completeness. The notions of accessibility and access security are linked to improper access and unauthorized secondary use as posited in the IS privacy literature [4]. This implies that organizations should be attentive to the privacy perceptions of service professionals who have daily interactions with consumer data both in the context of protecting data quality while implementing privacy protection policies.

The health care industry spent an estimated $10 billion to $15 billion on information technology (IT) in 1996 [19]. The evolving trend toward electronic medical records, integrated and community networks, and managed care has resulted in increased information sharing among providers, pharmacies, and insurers. Similarly, banks have collectively invested millions of dollars in data warehouses that aggregate customer data from various departmental databases [20]. Unfortunately, this heightened information sharing often conflicts with consumers’ desires to be shielded from unauthorized secondary use of their medical and banking records. Although many consumers believe we should have a legal right to privacy, consumers cannot rely on existing legislation for protection [21] nor can they reply on the privacy practices of professionals who play a significant role in the overall quality of data collected, accessed, or used to define service delivery.

Previous studies [3, 10, 11, 22] have added to the knowledge of privacy, customer preferences, and physical security mechanisms, such as biometrics and digital cash. Although each of these studies hint at the need to balance public policy and privacy protection, one void in these works is the lack of understanding of how health care and banking employees who have access to consumer records view privacy practices relative to safeguarding these data. This is a significant exclusion because such employees are likely to be most aware about the incidence of consumer privacy invasions, while at the same time, these employees may not realize the impact of such invasions. Recognizing these employee views will benefit managers as they are the organizational members who have oversight responsibility for information liability [12]. Such perceptions will provide the field with a basis for analyzing industry privacy practices. Managers must engage in conscious and deliberate decision-making when addressing the operation, control, and management of information systems [23]. Managers also need to consider potential information problems and take a proactive stance to reduce such risks before an undesirable situation occurs [5, 18, 24].

In this article, we discuss the privacy orientation of these employees who have regular access to personal information and draw on Wang and Strong [6] to make inferences regarding data quality. Gaining such an understanding of the internal concerns will assist both the field and practice in developing better methods and policies for privacy protection while allowing consumers to understand the people who control their information. Some researchers [4] have realized the need for validated instruments for measuring individuals’ concerns about organizational practices and therefore, developed tools to identify and measure the principal dimensions of privacy concerns. We have applied these validated tools to explore how health care and banking professionals in the United States assess the practices of their organizations.
Applying the customer orientation definition of Brown et al. [5], our study uses the privacy orientation of health care and banking professionals to evaluate organizational practices. In particular, we seek to determine:

1. What are the concerns of privacy practices among medical and banking professionals who have access to personal data, and
2. Whether there are differences between the concerns of medical and banking professionals’ privacy practices.

Our focus on electronic access to personal information in two data-intensive industries, health care and banking, suggests the appropriateness of the IS literature in reviewing tools for exploring industry privacy practices.

3. INDUSTRY PRIVACY ISSUES AND IS FRAMEWORKS

Numerous articles [11, 20, 25] have recently begun to highlight the increasing interest in personal privacy and the related concerns of consumers. Similarly, public opinion polls routinely suggest escalating public concern regarding privacy of personal banking and health care information [26, 27]. Despite these and other alarms of concern from consumer advocacy groups and congressional members, the supply and demand of consumer information continues to escalate. Such growth has spawned from a number of players who use consumer data for a myriad of reasons. In health care, these groups include: research centers, pharmaceutical companies, managed care organizations, third-party payors, and physicians. Relevant groups in the banking setting include affiliates, mortgage lending organizations, and credit reporting bureaus.

Several media outlets have devoted “special issues” to advise consumers on how to protect personal, banking and medical information; however, once consumers disclose personal information, they immediately lose control of these data. When consumers provide their social security numbers, occupations, addresses, telephone numbers, income levels, loan amounts, medical conditions, and medical backgrounds, these details often lead to unwanted inclusion in commercial databases. These occurrences follow technological changes that emerged in the 1980s, and as a result the importance of information privacy has surfaced and new laws addressing information use have begun to emerge [10–14]. These are discussed below and include GLB, HIPAA, and Model State Emergency Health Powers Act of 2001 [10].

3.1 Banking Industry

The Gramm–Leach–Bliley Banking Modernization Act of 1999 allows banks, insurance companies, securities firms, mutual funds, and brokerage firms to freely share customers’ personal banking information with affiliated groups. Although data distribution and transmission may not occur among nonaffiliates, this type of information sharing remains contradictory with traditional privacy principles that call for information collection for secondary uses of consumer data.

To this end, the Banking Industry Technology Secretariat (BITS), a division of the Bankers Roundtable, organized a study of consumers’ attitudes concerning security, privacy, and trust in 1998 (http://www.bitsinfo.org/Consumers498.pdf). Although
the goal was to understand the factors affecting the adoption and growth of electronic commerce, the study has implications to the industry as a whole. The BITS study suggests that consumers are concerned about four categories of privacy: unsolicited advertisements, accidental release of personal information, misrouting of funds, and errors. Other banking organizations, including American Bankers Association (ABA), America’s Community Bankers, Consumer Banker Association, Independent Bankers Association of America, and The Bankers Roundtable, are also involved in similar studies that explore consumer attitudes about privacy.

The banking industry is signaling a commitment to customer privacy by addressing these concerns through a set of industry principles [28]. In 1997, The Bankers Roundtable, BITS, the American Bankers Association, Consumer Banker Association, America’s Community Bankers, and the Independent Bankers Association of America agreed jointly to a set of Privacy Principles creating an industry-wide and unified commitment to the same set of guiding ideology (which are throughout the findings of Roboff & Charles [28]) that include the following [28]:

- Recognize a customer’s expectation of privacy.
- Use, collect, and retain customer information only if the institution believes the customer will benefit.
- Maintain accurate information.
- Limit employee access to information.
- Protect information via established security procedures.
- Restrict the disclosure of account information.
- Maintain customer privacy in business relationships with third parties.
- Make an institution’s privacy principles of policies known to the customer.

Following approval of the Privacy Principles, guidelines for implementing those principles were created.

To date, however, we are unable to uncover studies that explore banking (or health care) professionals’ awareness or attitudes regarding these privacy issues. Therefore, this discloses a need to explore the privacy orientation of these service workers in the on-the-job context or actual practices currently in place. Our study seeks to remedy this deficiency.

3.2 Health Care Industry

Privacy concerns have also risen from IT-enabled applications that support marketing and data mining of patient information. For instance, nearly 750 insurance companies can access the Medical Information Bureau (MIB; www.mib.com) database, the largest repository of medical information in the United States and Canada. MIB collects information on patients’ preexisting conditions, insurance applications, and pharmacy subscriptions as well as notes from hospital and physician records. In some situations, employment decisions are inappropriately based on this information, and more common, marketers are using medical information to target potential customers. Many consumers, however, are outraged and find the unauthorized, premeditated use of their information to be an invasion of personal privacy. Recent legislation concerning health care privacy is the HIPAA. These regulations
took effect in 2003 and are the first national standard to protect individual’s personal health information, including medical records [25]. Although this regulatory framework is being set forth, it is uncertain how effective it will be at protecting patient privacy because data protection ultimately depends on the organizations and individual employees who handle personal information.

In addition to HIPAA, the Model State Emergency Health Powers Act of 2001 has sought to enable states to update their legal, technical, and public policy infrastructures to minimize the impacts of bioterrorism [10]. Drafted by the Center for Law and the Public’s Health and the Centers for Disease Control and Prevention, the Health Powers Act posits that state governments, in cases of imminent biological threat, are in need of provisions for quarantine, seizure of property, mandatory treatment, and vaccination. Although the Georgetown Health Privacy Project opposes the act and has concerns regarding the privacy of health data under its provisions, medical data would be an “open system” for governmental officials to share manually and via electronic applications. The looming issue that remains is the balance between the public good and privacy advocates.

Moreover, the issue of health care privacy, as it pertains to organizational practices, holds profound implications—as service delivery impacts human life, legality, and social policy [29]. Although debates continue to question what should be done to protect individual privacy, advocates such as the Online Privacy Alliance support standards that would foster a voluntary system. These standards would appear in organizational privacy policies, which are often implemented to discourage harmful acts involving personal information. Yet, organizational policies [19, 29] and objectives often appear conflicting. Employees are frequently unclear of their roles in guarding patient information and privacy, while at the same time following orders of supervisors and providing appropriate medical treatment. With regard to human life, erroneous (or incomplete) patient data can result in deficient physician, nurse, or other medical practitioner performance whereas the legal ramifications stand to erode organizational and physician resources.

The American Medical Association advocates stricter patient privacy controls and is guided by the principal that patients’ right to privacy supersedes all other institutional and individual needs for medical information [30]. To help prevent unauthorized secondary use and other actions (e.g., the lone hacker with individual objectives) that threaten patient privacy, the following concepts have been prescribed for consideration by health care organizations [31]:

- **Privacy**: A person’s right and desire to control the disclosure of their personal health information.
- **Confidentiality**: The controlled release of personal health information to an authorized information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.
- **Security**: Policies, procedures, and safeguards used to help control access to the contents of information systems (particularly clinical databases) while maintaining the integrity and availability of the data.

Most health care systems do not accommodate an adequate protection of privacy and confidentiality; therefore, a set of security requirements for health care infor-
information infrastructure has been set forth to address the relationship among privacy rights, confidentiality measures, and system security measures [32]. These requirements include: accountability, data integrity, availability, and auditability. The need for such requirements also implies the need for greater privacy awareness from those that control the customer data.

Although many health care organizations subscribe to Rindfleisch’s [31] recommendations with intentions to maintain privacy and confidentiality, there remains a plethora of privacy concerns. The literature reveals many studies that are concerned with physically providing better security for patient privacy [33, 34]. Few studies address protection that is required beyond physical security measures. For example, many health care employees have authorized access to patient data and can sacrifice patient privacy and confidentiality without breaking system security. Health care chief information officers (CIOs) agree that the most important threats to patient privacy and confidentiality include: (a) accidental disclosures, (b) insider curiosity, (c) insider subordination, and (d) unauthorized access [19]. Although accidental disclosure refers to authorized medical personnel making an innocent mistake that results in unintentional disclosure, insider curiosity involves authorized medical personnel who abuse access privileges for personal use, such as probing for evidence about possible sexually transmitted diseases of an acquaintance. Insider subordination pertains to authorized medical personnel accessing information to release to outsiders specifically for profit or spite. Finally, the unauthorized use of clinical information by organizations is the most common problem, as patients become recipients of unsolicited marketing actions.

The literature shows that organizations, as well as the general public, have a significant degree of concern regarding privacy and how IT can enable/hinder individuals’ abilities to safeguard personal medical and banking data. Because employees of an organization are ultimately in control of sensitive consumer data, it is important to understand employee attitudes, as well as consumer attitudes, toward privacy. Thus, the information systems field is in need of research that explores individuals’ perceptions of organizational information privacy practices [4]. Smith et al. [4] previously explored privacy concerns of consumers in a heterogeneous setting. Our study is unique as it utilizes health care and banking environments to explore and “measure” privacy orientation of employees having daily exposure to consumer information by capturing their practice concerns.

Thus, we used Smith et al. [4] to anchor our measurement of privacy orientation in an on-the-job context (i.e., practices of health care and financial service workers). Further justification of Smith et al. [4] rests with the previously defined customer orientation offered by Brown et al. [5]—whereby privacy orientation can be multifaceted. The crux of Smith et al. [4] is information systems domains—thereby capturing our need to focus on data-intensive settings.

4. METHOD

4.1 Sample

Our initial activities involved interviewing 10 banking and health care executives from eight different organizations to determine their privacy orientations. Although
these interviews were semistructured and provided insight into the appropriateness of the participating organization and number of employees to target, they provided us with an idea of organizations’ willingness to participate in our study. Of the eight organizations, two emerged as appropriate for our efforts based on assistance to solicit employee participation on our behalf and an openness to provide feedback on our survey prior to its release. These interactions along with executive feedback indicated the need to reorient the original survey of Smith et al., [4] based on our on-the-job context and distinct industries; this resulted in a more content and context meaningful instrument to collect data. In addition, our banking and health care contacts did have our revised survey critiqued by their reporting managers to check for appropriateness of items, time to complete, and misspellings. Given the numerous concerns regarding privacy, we found it appropriate to work with organizations that would solicit participation on our behalf; this is a similar technique used by Brown et al. [5] in their study of customer orientation among service workers.

To test our exploratory research questions, we administered a 15-item instrument (see the Appendix) along with cover letters to 500 health care and 137 banking professionals. Employed at a large southeastern hospital, the health care participants included a random sample of claims processors, billing administrators, nurses, laboratory technicians, and physicians. Banking respondents consisted of executive officers, tellers, and loan officers working at two southeastern banking institutions. Namely, we sought those employees who have access to confidential personal data and whose daily tasks were impacted by decision-making relative to these data. In each case, the potential participants were identified from a master list of anonymous employees and were only known by two executive directors who supported our project. In exchange for participation, both the health care and banking executives were offered a synopsis of our findings relative to their organization. The demographics of all participants are provided in Table 1.

### 4.2 Instrument

Data were gathered using the survey of Smith et al. [4] and is shown in the Appendix. Within a 30-day time frame, we obtained 163 usable surveys from the health care

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Demographics of the Study’s Banking and Health Care Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Banking</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
</tr>
<tr>
<td>Women</td>
<td>102</td>
</tr>
<tr>
<td>Men</td>
<td>28</td>
</tr>
<tr>
<td>Race/ethnicity</td>
<td></td>
</tr>
<tr>
<td>Whites</td>
<td>114</td>
</tr>
<tr>
<td>Black</td>
<td>15</td>
</tr>
<tr>
<td>Hispanic</td>
<td>9</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
</tr>
<tr>
<td>Average age$^a$</td>
<td>38.5</td>
</tr>
<tr>
<td>Average years of industry experience</td>
<td>5.8</td>
</tr>
</tbody>
</table>

$^a$Given in years.
workers providing us with a 32.6% response rate. The banking professionals, however, responded with 131 out of a possible 137 for a 95.6% response rate. The significance of the banking response rate can be explained by both the size of the organization (small, statewide, and hometown firms) and top management visibility (executive has daily direct contact with operational and middle management staff). Statistical analyses were performed to assess items and constructs that impact the employees’ concerns of organizational health care and banking practices. We also analyzed the data to determine whether there are differences between the two groups.

4.3 Variables

The survey corresponds to a model that characterizes privacy along four dimensions: collection, unauthorized secondary use, improper access, and errors; each dimension is defined as [4]:

1. Collection—Concern that extensive amounts of personally identifiable data are being collected and stored in databases.
2. Unauthorized secondary use (External)—Concern that information is collected for one purpose but is disclosed to an external party who then uses the information for a secondary purpose.
3. Improper access—Concern that data about individuals are readily available to people not properly authorized to view or access this data.
4. Errors—Concern that protections against deliberate and accidental errors in personal data are inadequate.

This four dimensional privacy model was the basis for the study reported in this article.

Table 2 shows the range of responses (mean and standard deviation) by industry. Furthermore, the table gives the reader an idea of the variability (by item) of the sample. A careful examination of the results (see Table 2) indicates that banking professionals strongly support the significance of “devoting more time to preventing unauthorized access” (Item N) and “collecting too much information” (Item O). Item N has an average of 6.35 (see the Appendix for scale definitions) whereas the average response for Item O is 6.39. Other notable items with strong (greater than 5.0) mean responses and small standard deviations (less than 1.5) include “more time to verify accuracy of information in databases” (Item L), “giving information to related companies is bothersome” (Item J), and “information should never be shared unless authorized by the consumer” (Item M).

Furthermore, the banking professionals showed minimal support for the issues of “being bothered by asking for consumer information” (Item A with an average response of 2.58), “rechecking databases for accurate consumer information despite costs” (Item B with an average response of 3.87) and “think twice before recording information” (Item E with an average response of 3.52). Interestingly, our analyses for the health care data set ran counter to the above. Our health care subjects largely advocate the statement of Items K (never sell information in databases to other companies) and N (devoting more time to preventing unauthorized access).

To analyze our data, we applied exploratory factor analysis to determine the unidimensionality of each scale as a means to assess construct validity. Briggs and
Cheek [35] described factor analysis as a “way of grouping correlated variables” (p. 108) based on exploration of multiple solutions that can lead to a structure that seems conceptually meaningful (p. 108). Scales were retained if each contained a single factor and produced an eigenvalue greater than one.

In our case, we used those items listed in the Appendix to study the construct of privacy as banking and health care employees view it. Often times, a single scale must be subdivided into subfactors to make distinctions that are both conceptually meaningful and empirically useful [5, 35]. Ideally, factor loadings should be greater than .50 while items composing a scale should have a substantial reliability of .40 or greater [36].

4.4 Analysis

Table 3 shows how our items grouped by factor loadings, and the results indicate that four dimensions (unauthorized secondary use, errors, collection, and improper access) emerged from the survey instrument as shown in the Appendix.

The described results are from the sample of health care professionals. All loadings above .50 are listed in Table 3, and our results indicate the presence of four dimensions: errors, unauthorized secondary use, improper access, and collection. Scale reliabilities for these factors are .80, .70, .65, and .45, respectively. An examination of total item correlations and a varimax factor pattern led to the omission of Item O (collecting too much information about patients; see the Appendix) due to cross-loadings and poor scale reliabilities. Because Item O was omitted from our analysis, all factor loadings and interitem reliabilities now meet the statistical criteria as outlined by Churchill [37].
The above results, however, suggest that health care professionals exhibit little concern for organizational practices related to the collection of patient information. Rather, there is considerable concern regarding the inaccuracy of patients’ medical records and the degree of unsanctioned use of patient information. This interpretation is substantiated—as most of the variance explained and reported in the eigenvalues for our data is done so by errors reported at 3.22 and unauthorized secondary use at 2.07. The variance explained by collection and improper access is 1.84 and 1.42, respectively. In sum, the cumulative variance explained in Table 3 is 8.51 with 37.8% attributed to the errors dimension of privacy.

Likewise, Table 4 reports the factor loading using our banking data set. Scale reliabilities using these data were .82, .82, .70, and .60, respectively, for improper access, errors, collection, and unauthorized secondary use. The variance explained in Table 4 is 3.11, 2.37, 2.15, and 1.83 for each of the respective factors in the banking data set. These results indicate that banking employees are primarily concerned with improper access as the variance explained by this factor is 3.11. Similar to our health care respondents, the banking professionals reported significant concerns regarding privacy practices and the potential of errors in consumer data. The variance explained by the errors dimension is 2.37 for our banking data set.

Additional analyses indicate that the four privacy dimensions can be contrasted according to the clustering of the survey items. Thus, t tests were performed to determine the differences between the health care and banking subjects by survey items. Table 5 reports these values that indicate significance between the two groups along each survey item (p < .05) with the exception of Item N (“take more steps to make sure that unauthorized people cannot access”).
### Table 4
Results of Banking Data Analysis

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Item No.</th>
<th>Improper Access</th>
<th>Unauthorized Secondary Use</th>
<th>Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never sell consumer info unless authorized</td>
<td>M</td>
<td>.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Never use consumer info other than for care</td>
<td>G</td>
<td>.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No use of consumer info for any purpose</td>
<td>C</td>
<td>.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Think twice before recording consumer info</td>
<td>E</td>
<td>.71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer databases with consumer info are protected</td>
<td>I</td>
<td>.60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Double check consumer info in databases</td>
<td>B</td>
<td>.92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bothers “participant” to ask for consumer info</td>
<td>A</td>
<td>.90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Steps to ensure accuracy of consumer info</td>
<td>F</td>
<td>.69</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preventing unauthorized access</td>
<td>D</td>
<td>.84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures to correct errors in consumer info</td>
<td>H</td>
<td>.71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Steps to prevent unauthorized use in computers</td>
<td>N</td>
<td></td>
<td></td>
<td>.66</td>
</tr>
<tr>
<td>Unauthorized persons cannot access data</td>
<td>O</td>
<td></td>
<td></td>
<td>.75</td>
</tr>
<tr>
<td>Never sell consumer info in databases</td>
<td>K</td>
<td></td>
<td></td>
<td>.68</td>
</tr>
<tr>
<td>Time/effort to verify consumer info in databases</td>
<td>L</td>
<td></td>
<td></td>
<td>.65</td>
</tr>
<tr>
<td>Bothers “participant” to give consumer info to others</td>
<td>J</td>
<td></td>
<td></td>
<td>.36</td>
</tr>
</tbody>
</table>

**Note.** See the Appendix for definitions of the survey items.

### Table 5
Differences in Means Between Two Groups

| Item | t Value  | Pr > |t| |
|------|----------|------|---|
| A    | −2.31    | .02  |   |
| B    | −15.67   | <.0001 |   |
| C    | −4.63    | <.001 |   |
| D    | 2.01     | .04  |   |
| E    | 9.66     | <.001 |   |
| F    | −16.10   | <.001 |   |
| G    | 3.69     | .0003 |   |
| H    | 3.98     | <.001 |   |
| I    | −9.51    | <.001 |   |
| J    | 4.75     | <.001 |   |
| K    | −12.26   | <.001 |   |
| L    | 6.63     | <.001 |   |
| M    | −10.43   | <.001 |   |
| N    | −1.85    | .06  |   |
| O    | 19.55    | <.001 |   |

**Note.** See the Appendix for definitions of the survey items.
5. DISCUSSION

Based on our initial objectives, we determined that privacy orientation among health care and banking professionals is a multidimensional construct. Although improper access, unauthorized secondary use, errors, and collection emerged as significant constructs, there appears to be some degree of conditionality associated with how critical each subfactor is in explaining privacy. These conditions can be a function of the industry-related legal developments, criticality of the personal data needed in the decision-making process, criticality of the decision in question, and internal organizational privacy policies and procedures. Second, there seems to be significant differences among banking and health-care professionals with regard to their concerns of privacy practices. This conclusion is interesting if we consider the timing of the data collection. The survey was distributed to each sector during times of impending legislation. The banking data was collected in 2001, before GLB became effective on July 31, 2001. Similarly, the health care data was collected before HIPAA became effective on April 14, 2003. From that standpoint, both groups were aware of privacy issues and both were preparing for privacy legislation.

With regard to the multidimensional framework DQ of Wang and Strong [6], our results suggest that intrinsic data quality is a primary concern for health care and banking professionals. Errors, which is analogous to accuracy, falls within the DQ foundation. Collection is comparable to appropriate amount of data in the contextual data quality framework and scored last of the four privacy dimensions from Smith et al. [4]. This is, however, not to dilute its importance. In a broader context, our data illustrates that privacy is multidimensional, so is data quality. Although representational data quality did not emerge in our study, there appears to be support that health care and financial privacy practices also rest on at least three dimensions of data quality as defined by Wang and Strong [6].

Banking and health care are global industries; however, it may not be accurate to generalize our findings to other countries. The 1995 European Union (EU) Information Directive (Directive 95/46/EC [38]) provides a thorough legal foundation for today’s EU data protection. In particular, the EU directive has been addressing concerns related to unauthorized secondary use, improper access, collection and errors in all domains. Although the United States has recently enacted privacy legislation in health care (HIPAA) and financial (GLB) industries, the laws have only been in effect since 2001. Further research that includes EU member countries may show employees with opinions that differ from U.S. employees.

6. IMPLICATIONS AND CONCLUSIONS

Banking and health care organizations collect a substantial amount of banking and medical information during the daily activities of “doing” business. As one manager stated to us, “We have to collect these data even if they do not pertain to the case at hand. While we have the patient’s attention, our employees feel like and are directed to get the data”. Although both groups perceive unauthorized secondary use as a major deterrent in their industries, the proliferation of data mining and data warehousing technologies further facilitates these apparently widespread business
practices. Thus, the DQ framework would suggest that security and accessibility are primary concerns of these industries’ service professionals.

In addition, there appears to be tradeoffs among collection, unauthorized secondary use, improper access, and errors—thereby, impacting the privacy of those using services in these industries. Health care professionals, however, could have a sense of urgency to collect as much patient information as possible—thereby reducing the perceived need of having too little knowledge during care delivery while providing evidence that questioned the need for Item O in the medical data set. This perception has been observed in cases of emergency care, such as cardiac arrest, stroke, childbirth, and in social-laden episodes of illness (e.g., AIDS, HIV) [29]. Furthermore, errors (e.g., intrinsic data quality) in health care patient information can result in alarming outcomes including medical complications and even death.

Moreover, the banking subjects pointed to the concern of improper access in the banking industry. Given the acceleration of online and other electronic commerce services in the banking industry, Roboff and Charles’ [28] work substantiates this finding. Popular press, likewise, continues to document how unauthorized access of consumer banking data can and has resulted in wrongful unemployment, housing and credit outcomes, often unknown to both the “person” and granting institution.

A major contribution of this article is the identification of privacy concerns as viewed by health care and banking employees, and how privacy oriented these workers are. To create a “culture of privacy” within an organization, managers need to influence the privacy views of employees, particularly those with daily access to personal customer data. Recognizing these views will provide a basis for training employees accordingly, establishing privacy policy and audits, and implementing enforcement within information systems.

Furthermore, another contribution of our research is the substantiated awareness of opposing privacy orientation between health care and banking employees. This result is despite the fact that both industries were facing imminent privacy legislation. We anticipated a priori that both of these service sectors’ employees would share a similar view of privacy practices due to overarching, often profound, legal systems impacting data sharing, collection, access and transformation. Our results indicate there is not a privacy panacea for all organizations as a whole, but the individual sector must be considered. In addition, this suggests that employees from other service sectors (e.g., communications, hospitality, retail) need to be considered as well. Specific to banking and health care industries, the results of our study suggest the following recommendations for decision-makers—as knowledge about work processes facilitates the data quality needed to engender improved privacy practices [9]:

1. Clarity of roles and responsibilities should be determined, documented, and explained to employees upon entering the organization. This enables the establishment of knowing-how, knowing-why, and knowing-what.

2. The impact of adverse data management practices should be documented in a “lessons learned” systems—thereby enabling a knowledge base of avoidable practices for managers and decision makers to determine areas of improvement via change management and information technology infrastructure.
Health care and banking service managers should establish their privacy policy as it relates to the four subfactors (collection, unauthorized secondary use, access, and errors); specific guidelines as such as these, can offer employees details of (un)acceptable practices based on the knowledge base developed from Item 2 above.

In addition to the provided guidelines, policy changes may improve privacy practices and alleviate any employee concerns. Future research could address the effectiveness of such policy changes by administering the survey now that HIPAA and GLB are both in effect.

REFERENCES

INFORMATION PRIVACY IN THE SERVICE SECTOR


APPENDIX

Survey Instrument

A. It usually bothers me when COMPANY A asks for consumer(patient) information.
B. All the consumer (patient) information in computer databases should be double-checked for accuracy—no matter how much this costs.
C. COMPANY A should not use patient information for any purpose unless it has been authorized by the consumer(patient) who provided the information.
D. COMPANY A should devote more time and effort to preventing unauthorized access to personal information.

1Adapted from Smith et al. [5]. Copyright © Regents of the University of Minnesota. Adapted with permission.
E. When COMPANY A asks consumers(patients) for personal information, I sometimes think twice before recording it.
F. COMPANY A should take more steps to make sure that the consumer(patient) information in its files is accurate.
G. When consumer(patient) give personal information to COMPANY A for some reason, COMPANY A should never use the information for any other reason (other than care delivery).
H. COMPANY A should have better procedures to correct errors in consumer(patient) information.
I. Computer databases that contain consumer(patient) information should be protected from unauthorized access – no matter how much it costs.
J. It bothers me to give consumer(patient) information to other banking/health care companies.
K. COMPANY A should never sell the consumer(patient) information in its computer databases to other companies.
L. COMPANY A should devote more time and effort to verifying the accuracy of the consumer(patient) information in its databases.
M. COMPANY A should never share consumer(patient) information with other companies unless it has been authorized by the consumers(patients) who provided the information.
N. COMPANY A should take more steps to make sure that unauthorized people cannot access consumer(patient) information in its computers.
O. I’m concerned that COMPANY A is collecting too much information about consumers(patients).

Each item was rated on a 7-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). Some items were modified due to the context of this research.
Copyright of Journal of Organizational Computing & Electronic Commerce is the property of Lawrence Erlbaum Associates and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder’s express written permission. However, users may print, download, or email articles for individual use.