AIS Transactions on Human-Computer Interaction

Volume 8 | Issue 2 Article 2

2016

Impact of Human Resource Information System Policies on Privacy

Kimberly M. Lukaszewski
Wright State University, kimberly.lukaszewski@wright.edu

Diana L. Stone
University of Albany, SUNY, and Virginia Tech, diannastone2015@gmail.com

Richard D. Johnson
University at Albany, rjohnson@albany.edu

Recommended Citation

Lukaszewski, K. M., Stone, D. L., & Johnson, R. D. (2016). Impact of Human Resource Information System Policies on Privacy. *AIS Transactions on Human-Computer Interaction, 8*(2), 58-73. Retrieved from https://aisel.aisnet.org/thci/vol8/iss2/2
DOI:

Transactions on Human – Computer Interaction

Research Paper

Impact of Human Resource Information System Policies on Privacy

Kimberly M. Lukaszewski
Wright State University
kimberly.lukaszewski@wright.edu

Diana L. Stone
University of Albany, SUNY, and Virginia Tech
Diannastone2015@gmail.com

Richard D. Johnson
University of Albany, SUNY
rjohnson@albany.edu

Abstract:

Organizations are increasingly using human resource information systems (HRIS) to collect and store employee data to enhance employment decision making. In this paper, using a 2 x 2 x 2 experimental design, we 1) examine the effects of three HRIS policies on employees' perceptions of invasion of privacy, 2) assess the moderating effects of amount of work experience on the relations between these HRIS policies and employees' perceptions of invasion of privacy and 3) discuss the implications of these findings for developing fair information policies. Results revealed that individuals perceived a HRIS was more of an invasion of privacy when HRIS data were used for only the benefit of the organization than when it was used to benefit employees. In addition, the results indicated that individuals perceived that a HRIS was more invasive of privacy when the data were accessed by supervisors than when they were accessed by the HR department only. Furthermore, individuals' amount of work experience moderated the relations between (a) purpose of the data collection, and (b) access to data and perceptions of invasion of privacy. Implications for theory, research, and practice are discussed.

Keywords: HRIS, Privacy, HRIS Policies, Purpose of Data, Access, Ability to Check Accuracy.

1 Introduction

Organizations are increasingly using human resource information systems (HRIS) to manage employee data. Surveys have revealed that 80 percent of large organizations now use HRIS to collect and store data about employees to enhance employment decision making (CedarCrestone, 2013). A HRIS is "a system used to acquire, store…analyze…and distribute information regarding an organization's human resources" (Kavanagh, Thite, & Johnson, 2015, p. 17). These systems offer several benefits including 1) reduced costs, 2) decreased time needed for HR processes, and 3) increased self-service capabilities (e.g., Lippert & Swiercz, 2005). As a result, a HRIS may not only increase the efficiency of the HR function but also help HR provide better services to employees.

Despite the many advantages of a HRIS, researchers have raised concerns about the extent to which they have the potential to violate employees' rights to privacy (e.g., Eddy, Stone, & Stone-Romero, 1999). For example, a recent survey found that 74 percent of respondents noted that it is important for them to control their personal information, and only 9 percent indicated that they have a lot of control over it (Pew Research Center, 2015). Researchers have warned that the increased use of computerized systems gives employers access to data that may unfairly stigmatize employees (Zafar & Stone, 2015). For instance, a HRIS may give supervisors access to data that have little job relevance (e.g., bankruptcies), and one survey indicated that a large number of organizations collect data about employees' credit history, driving records, lifestyle, and workers' compensation claims (e.g., SHRM and West Group, 2000).

Furthermore, researchers have expressed concerns that a HRIS will decrease employees' perceptions of control over information and that organizations will release data to third parties (Zafar & Stone, 2015). An organization that uses a HRIS also creates a major change in the employment environment and may increase employees' feelings of vulnerability (Lippert & Swiercz, 2005). Even modest systems may give anyone, with or without authorization, access to highly sensitive information (wages). Privacy is typically based on the expectation that sensitive information will not be shared, but surveys have indicated that 69 percent of organizations share data with third parties (Sanders, 2015). Not surprisingly, the loss of employee privacy may also have a negative effect on organizations. Research showed that invasion of privacy is negatively related to employee attitudes and to organizational citizenship behaviors (Alge, Ballinger, Tangerala, & Oakley, 2006).

These days, many employees express concern that hackers will breach their organizations' HRIS and steal their identities. For example, there have been over 500 million breached employment records since 2005 (Privacy Clearinghouse, 2013). In one incident, a U.S. Airways employee leaked a database containing bank account data for about 3000 pilots (Constantin, 2011), and, in 2010, a hard drive was stolen from AMR Corporation that included social security numbers and health records. The AMR employees experienced identity theft.

Another privacy issue is that the HRIS data may be inaccurate and negatively affect employment decisions. For instance, research has showed that 73 percent of companies make errors when checking individuals' backgrounds and that using inaccurate data results in adverse outcomes (SHRM and West Group, 2000). For instance, Hilton hotels terminated one of its executives when data in a background check incorrectly noted that he had been convicted of a misdemeanor and served six months in jail (Socorro vs. IMI Data Search, Inc., 2003). In spite of concerns about inaccurate HRIS data, 60 percent of companies do not ensure that data are correct (CedarCrestone, 2013). In addition, no federal law requires private-sector employers to provide employees access to their files, and most do not allow them to correct their records (SHRM, 2015). However, ten state laws give private-sector employees access to records, and 20 allow public-sector employees to check the accuracy of their records (SHRM, 2015). Despite these laws, sociologists argued that, unless organizations commit to the underlying values of a law, they may rarely heed them voluntarily (speed limit laws) (Etzioni, 1996). Thus, even when privacy laws exist, some employers may not comply with them, not give employees access to records, collect data that are not job relevant, and give supervisors access to the HRIS data. Therefore, we believe that organizations that voluntarily adopt HRIS policies are more likely to maintain employee privacy, but we need research to examine their effectiveness. As a result, we examine the effectiveness of three privacy policies.

Even though many organizations now use HRIS and despite growing concerns about privacy, little empirical research has examined the use of fair information policies as a means of alleviating invasions of privacy. Some notable exceptions include Bélanger and Crossler (2011), Lippert and Swiercz (2005), Lukaszewski, Stone, and Stone-Romero (2008), and Smith, Dinev, and Xu (2011). Given the paucity of research on privacy, in this paper, we 1) examine the effects of three HRIS policies on employees' perceptions of

invasion of privacy, 2) assess the moderating effects of amount of work experience on the relations between these HRIS policies and employees' perceptions of invasion of privacy and 3) discuss the implications of these findings for developing fair information policies.

When employees perceive their privacy has been invaded, they may also believe that systems are unfair (Gilliland, 1993). However, we focused primarily on privacy as perceived control over information because justice theorists argued that privacy and fairness are two separate constructs (Gilliland, 1993). Empirical research also supports the distinction between privacy and fairness (Eddy et al., 1999). Privacy and justice theories do include one common variable (correctability), but we used Stone and Stone's (1990) privacy model rather than justice models because it focuses on specific factors that influence perceptions of privacy.

1.1 Privacy Policies

According to Stone and Stone (1990), privacy refers to the degree to which individuals value controlling personal information. Their privacy model suggests that three primary factors influence individuals' privacy perceptions: 1) the degree to which individuals value controlling their personal information (e.g., people may value controlling information about their genderual orientation more than that about previous work history because the former information often leads to stigmatization), 2) the degree to which they perceive that they lack the ability to control over their information, and 3) the lack of control leads to negative outcomes (e.g., loss of job opportunities).

Taken together, individuals are likely to perceive that their privacy has been invaded when a) they value controlling information, b) they perceive that they lack control over information, and c) the lack of control leads to negative outcomes. The model also indicates that informational factors (e.g., information type), individual factors (e.g., work experience), and socio-cultural factors influence the factors noted above. To date, research has found support for many of the predicted relations in the model (Black, Stone, & Johnson, 2015), and research in management information systems (MIS) has found indirect support for two factors in it. Research has revealed that privacy concerns form because of 1) individual values regarding privacy and 2) situational cues that enable people to assess the consequences of information disclosure (Xu, Dinev, Smith, & Hart, 2008).

In spite of employees' growing concern about privacy and HRIS, 70 percent of organizations have still not established written policies for regulating employee information, and, even when they have policies, 30 percent of organizations do not communicate them to employees (Wilkie, 2015). In the US, the Privacy Act of 1974 established guidelines for federal employee records, and several states (e.g., California) have laws that protect public employee records. However, few laws affect the management of private-sector employee information. The European Data Act regulates the control of employee information in Europe, and other countries have also established privacy regulations (e.g., Hong Kong).

Although some research has examined the information factors in the privacy model (e.g., data release) (e.g., Eddy et al., 1999), little research has examined the effects of HRIS policies on employees' perceptions of invasion of privacy Thus, we assessed the effects of three HRIS policies (the purpose of the data collection, access to data, and the ability to check the data's accuracy) on perceptions of invasion of privacy (hereinafter referred to as privacy perceptions). We also examined if one individual factor (e.g., work experience) moderated the relations between the HRIS policies and privacy perceptions.

1.2 Purpose of the Data Collection

The privacy model (Stone & Stone, 1990) suggests that the purpose of the HRIS data collection may be an important determinant of privacy perceptions because, for one, the reason an organization collects data often affects HR decision making. For example, a person may not perceive their privacy has been invaded when their organization uses their HRIS data for promotion purposes and they benefit from it. However, they may believe that their privacy has been invaded when their organization uses the same data for layoff purposes, which benefits only the organization. When an organization uses data only for itself, individuals may believe they have no power to control information and its consequences. Some previous research on privacy has provided support for these arguments and suggested that privacy perceptions vary with the purpose and judged benefit of the data collection (e.g., Simmons, 1968).

We know of no research on the purpose of the HRIS data collection and privacy perceptions. Thus, we hypothesize:

Hypothesis 1: Individuals are more likely to perceive their privacy has been invaded when their organization uses it for HR planning purposes than when they use the data for employee tracking and safety purposes.

1.3 Access to Data

Stone and Stone's (1990) privacy model argues that individuals who can access data may affect employees' perceptions of invasion of privacy. The model posits that, when some targets (e.g., HR decision makers) access data, employees will be more likely to perceive that they have lost control over information and experience negative consequences than when non-decision makers have access. For instance, when supervisors have access to HRIS data, employees may fear that they will use the data for HR decisions and that such use will result in negative consequences.

However, when HR managers or staff (hereinafter HR administrators) have access to HRIS data, employees are less likely to believe they have lost control over information or experience negative outcomes than when supervisors have access to HRIS data because administrators do not typically make employment decisions but supervisors do. Assume that a supervisor has access to HRIS data that show an individual filed for bankruptcy many years ago. The supervisor may make the inference that the person lacks planning and money-management skills and deny the person a promotion to manager. However, this individual will likely perceive that this supervisor has invaded the individual's privacy because the data does not relate to the individual's job or is out of date. However, if HR administrators were the only ones who had access to the data, the employee would be less likely to experience an invasion of privacy.

Legal analysts have argued that employers should restrict access to employee files, but companies often give immediate supervisors and HR administrators access to all types of records (Findlaw, 2015). Some companies believe that supervisors have a legal right to access personnel files, but organizations are not always clear about the types of data that their supervisors can and cannot access (Findlaw, 2015). For example, it may not be clear that supervisors should not have access to disability or medical data because this data may bias decision making or reveal stigmatizing medical conditions about employees. One exception is that employment laws require that organizations keep medical data separate from employment data (ADA, 1990), but many organizations now ask employees to provide health information to offset rising healthcare costs (Hicks, 2014). Even when employees do not reveal the information, organizations can ascertain employee medical problems by the amounts of healthcare they use (Hicks, 2014).

Previous research on privacy (Stone, Gueutal, Gardner, & McClure, 1983) has provided indirect support for the relation between the target of information disclosure and privacy perceptions. Stone et al. (1983) found that individuals were more likely to perceive their privacy had been invaded when law enforcement could access their data than when employers could access it. Stone et al. (1983) state that individuals felt that data revealed to law enforcement would more likely result in negative consequences (e.g., legal action) than data released to employers.

Thus, we hypothesize:

Hypothesis 2: Individuals are more likely to perceive that their privacy has been invaded when supervisors can access HRIS data than when only HR administrators can access HRIS data.

1.4 Ability to Check Data Accuracy

The Stone and Stone (1990) privacy model argues that individuals' ability to check the accuracy of the HRIS data is an important determinant of their privacy perceptions because, when employees can do so, they can correct errors and maintain control over personal information. However, if they cannot check the accuracy of data, they may feel vulnerable and believe that they have lost control over the information and its consequences. Assume that a company must layoff some of its workers, and an employee's HRIS file shows a poor credit record. However, the employee's job does not involve responsibility for money, and the data are inaccurate because the person has never had a poor credit rating. Nevertheless, the company may infer that it cannot trust the person and discharge them. The layoff based on inaccurate data could have been avoided if the employee had the opportunity to review and correct their file.

Surveys have indicated that some HRIS data are inaccurate, especially data from background checks (Neighly & Emsellem, 2013), and only 34 percent of employers purge files of obsolete or erroneous data (Harris Interactive, 2002). Furthermore, no current U.S. federal law requires employers to provide

employees access to their records, but several states have passed legislation that gives public and some private-sector employees access (SHRM, 2015). We believe that one means of alleviating privacy concerns is to give employees the chance to review and correct their HRIS data. Thus, we hypothesize:

Hypothesis 3: Individuals are less likely to perceive their privacy has been invaded when they can check the accuracy of their data in a HRIS than when they cannot.

1.5 Individual Factors

Stone and Stone's (1990) privacy model argues that several individual variables are likely to influence privacy perceptions. One of those variables is an individual's amount of work experience. We limited our study to this variable because we had no clear basis for making predictions about other factors (e.g., education). For example, one can expect that individuals with a great deal of work experience should value controlling their HRIS data more than those with little experience because those with a lot of experience may have more potentially discrediting information (e.g., poor performance ratings) in their files than their counterparts.

One reason for this is that older individuals with more work experience may be less knowledgeable about HRIS but more likely to perceive that a HRIS will result in negative job outcomes than their counterparts with less job experience. Thus, we believe that individuals with a lot of work experience should react more positively when organizations implement privacy policies than those with little experience. Thus, we hypothesize:

Hypothesis 4: Individuals' amount of work experience moderates the relations among 1) purpose of the HRIS data collection, 2) access to the HRIS data, 3) ability to correct the HRIS data and their privacy perceptions.

2 Method

2.1 Overview

Using a 2 x 2 x 2 experimental design and data from 309 employed individuals, we examined the effects of 1) purpose of the data collection (HR planning vs. employee tracking), 2) access to data (HR access only vs. supervisory access), and 3) ability to check the accuracy of data (no ability to check accuracy vs. ability to check accuracy) on employees' privacy perceptions. We also assessed the degree that individuals' work experience moderated the relations between the policies above and privacy perceptions.

2.2 Participants

We obtained data from 309 employed individuals (145 men, 160 women, 4 missing) enrolled in part-time graduate business program at a large Southeastern university in the US. On average, they were 28.89 years old and they had 7.04 average years of work experience. They were employed in a variety of positions including manager, accountant, teacher, and engineer. Seventy-seven percent were white, 6.4 percent were Asian, 5.1 percent were African American, and 4.2 percent were Hispanic. Two hundred twenty participants indicated that they were not familiar with HRIS, and 68 were familiar with them.

2.3 Procedure

First, we asked participants to complete an informed consent agreement. Second, we randomly assigned them to an experimental condition. Third, we asked them to play the role of an employee and read a description of a firm's HRIS policies. Then, they completed a personal data sheet depicting the data collected for a HRIS. Fifth, they completed measures designed to assess 1) their privacy perceptions, and 2) their demographic background data, and 3) manipulation checks. Finally, we debriefed them on the study's purpose.

2.4 Manipulations

As we note above, we asked participants to play the role of an employee in a hypothetical organization. Each scenario[1] described a fictitious organization, and we manipulated the independent variables by varying the information presented in the scenarios. The beginning of each scenario read as follows:

> *Assume you are employed by Magnetechnics, a high technology firm that designs and manufactures magnetic imaging equipment for health care facilities. The firm has recently decided to develop and implement a Human Resources Information System (HRIS). A HRIS is computerized system used to store and retrieve information about employees.*

Following the introduction, the scenarios stated "Attached is a data sheet for you to complete as an employee". We designed the data sheet based on the information collected for PeopleSoft HRIS (a widely used HRIS).

2.5 Purpose of the Data Collection

We varied the purpose of the data collection by varying the reasons in the scenarios for why the fictitious organizations collected data on their employees. In the HR-planning purpose condition, the organizational scenario read "The firm needs to collect personal data about you to assist with human resources planning and decision-making. The organization needs to collect your personal data in order to utilize human resource skills more effectively.". In the employee tracking condition, the scenario read: "The firm needs to collect personal data about you to track your employment data, and notify others in emergencies.".

2.6 Access to Data

We manipulated the access to data variable by varying the information in the scenarios. All scenarios stated: "The data you provide on the data sheet will be entered and stored in a computerized HR system controlled by the Human Resources Manager.". Then, the scenario varied information about who had access to the data. In Human Resources Management Department only conditions, the scenario read: "Note that the Human Resources Administrator will be the only people who have access to your personal data.". The supervisor condition scenario stated: "Note that your immediate supervisor will have access to your personal data.".

2.7 Ability to Check Accuracy

We manipulated our employee participants' ability to check the accuracy of their data also by altering the information in the scenarios. The no ability to check the accuracy condition scenario stated: "When you complete the data sheet we want you to make sure that your data are accurate and complete. The reason for this is that once your data are entered into the HRIS you will not have the opportunity to correct…it unless there are unusual circumstances (e.g., marriage).". In the ability to check the accuracy conditions, the scenario read: "After your data are entered into the HRIS you will have the opportunity to see, correct or amend your data on a yearly basis. A copy of your employment record will be provided to you each year, and you will be asked to verify the accuracy of the data and make any necessary changes.".

2.8 Measures

2.8.1 Perceptions of Invasion of Privacy

We measured perceptions of invasion of privacy with a six-item summated scale using a seven-point (strongly disagree to strongly agree) Likert-type response format. A sample item included: "The collection of personal data for the HRIS was an invasion of privacy.". We scored the scale so that higher scores reflected greater perceptions of invasion of privacy. The coefficient alpha reliability estimate for this scale was .89. Previous studies on information privacy have established the construct validity of this questionnaire (Lukaszewski et al., 2008): they found that scores on the measure were positively related to other measures of privacy (Stone et al., 1983).

[1] Note that we used a total of 8 scenarios in the study, but each participant only received one scenario that corresponded to a particular experimental condition.

2.9 Analyses

We used multiple regression analysis to analyze the study's data. We chose this analysis because statisticians argue that, even though multiple regression and ANOVA are part of the same general linear model, multiple regression is appropriate when cell sizes are unequal (Cohen, Cohen, West, & Aiken, 2013). Given that our study had unequal cell sizes, we complied with Cohen et al.'s (2013) recommendation. Cohen et al. (2003) also argue that multiple regression and ANOVA produce essentially the same results (p. 3-4) but that regression is more robust than ANOVA.

3 Results

Table 1 provides the results of correlational analyses, and Table 2 provides the descriptive statistics by experimental condition. Note that our independent variables did not correlate because we used an experimental design (see Table 1).

Table 1. Correlations Among Variables

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
(1) Purpose	--								
(2) Access	.01	--							
(3) Ability to correct	.00	.00	--						
(4) Invasion of privacy	-.09	-.09	-.01	--					
(5) Gender	-.07	-.07	-.07	.10*	--				
(6) Age	.04	.08	.13*	.27*	.10*	--			
(7) Work experience	.04	.07	.14*	.30*	.10*	.89**	--		
(8) Employed	.05	.01	.03	.03	.04	.21**	.26**	--	
(9) Knowledge of HRIS	-.10*	.02	-.02	.07	.00	.22**	.21**	.16**	--

* p < .05.
** p < .01.
Used one-tailed significance test.

Table 2. Descriptive Statistics by Experimental Condition

	Criterion variable		
	Perceptions of invasion of privacy		
	M	SD	N
Purpose HR planning (benefitting only the organization)	33.99	7.84	152
HR Access only	33.28	8.19	80
Ability to correct data	33.57	7.88	37
No ability to correct data	33.02	8.52	43
Supervisory access	34.99	7.42	72
Ability to correct data	34.39	7.36	38
No ability to correct data	35.24	7.58	34
Purpose employee tracking	32.47	9.55	154
HR access only	30.76	10.42	79
Ability to correct data	30.85	10.39	41
No ability to correct data	30.66	7.21	35
Supervisory access	34.27	8.23	75
Ability to correct data	34.69	7.22	35
No ability to correct data	33.90	9.10	40

Note that higher scores indicate higher levels of perceptions of invasion of privacy.

Table 3 presents results of the regression analysis for each of our hypotheses.

Table 3. Results of Regression Analysis

	Criterion variable	
	Perceptions of invasion of privacy[1]	
Predictor variables	*B*	*T*
Purpose of data collection (P)	-.267	-3.116***
Access to data (A)	.162	1.957**
Ability to correct data (C)	-.052	-.916
Work experience (E)	.210	.741
A x E	-.285	-1.459*[2]
P x E	.338	1.993**

[1] R = .383. F (6, 271) = 6.657, p < .0001.
***p < .01, **p < .05, * < .10.
[2] Pedazur, (1997) argued that p < .10 is an acceptable criterion for testing interaction terms.

3.1 Manipulation Checks

We used three items as checks on the study's manipulations, and the overall the results reveal that participants perceived the manipulations as expected. For instance, 130 participants correctly noted the HR-planning purpose as intended and 10 did not, and 108 viewed the employee-tracking purpose accurately and 39 did not. Chi square analysis indicated that the majority of participants viewed the manipulation as anticipated ($\chi 2 = 130.29$, p =.000).

Similarly, 151 participants correctly identified the HR-only access manipulation and 6 did not, and 103 viewed the supervisor access accurately and 28 did not. Chi square analysis indicated that most of the participants viewed the manipulation as expected ($\chi 2 = 177.35$, p = .000). Finally, 126 detected the no ability to correct the files manipulation correctly and 14 did not, and 133 identified the ability to correct files manipulation accurately and 15 did not. Results indicated that majority of participants recognized the manipulations as intended ($\chi 2 = 184.2$, p = .000).

We did not eliminate participants from the analysis if they did not perceive the manipulation accurately because, for one, the majority of participants viewed the three manipulations as intended, and the main effects for purpose of the data collection and access to data were statistically significant. Even though the main effect for ability to correct the data was not statistically significant, only 15 participants out of 133 did not perceive this manipulation accurately. In addition, only 14 out of 126 did not perceive the no ability to correct data manipulation as intended. Given the relatively small number of participants who did not perceive this manipulation correctly, we do not believe that eliminating them would change the study's results.

3.2 Tests of Hypotheses

3.2.1 Hypothesis 1

Hypothesis 1 states that individuals are more likely to perceive their privacy has been invaded when their organization uses it for HR planning purposes than when they use the data for employee tracking and safety purposes. The results of the regression analysis showed support for this hypothesis (see Table 3). The R =.383 and the F were statistically significant ($F(6, 271) = 6.657$, p < .0001). The t value associated with the regression coefficient for purpose of data was also statistically significant ($\beta = -.267$, $t = -3.116$, p < .01). The findings reveal that, when an organization collects HRIS data for HR planning, the mean level of invasion of privacy was greater (M = 33.99) than when the organization collects it for employee tracking (M = 32.47). The interaction between purpose of the data collection and individuals' work experience qualified this main effect, which we discuss in Section 3.24.

3.2.2 Hypothesis 2

Hypothesis 2 states that individuals are more likely to perceive that their privacy has been invaded when supervisors can access HRIS data than when only HR administrators can access HRIS data. The results of the regression analysis showed support for this hypothesis (see Table 3). The t value for the regression

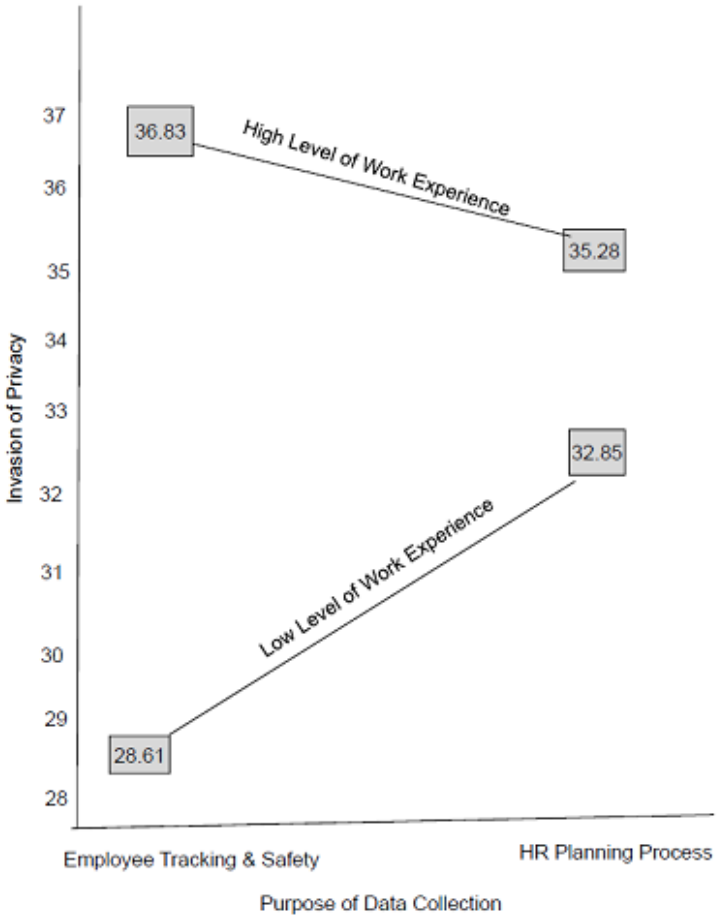
coefficient was statistically significant (β = .162, t = 1.957, p < .05). When supervisors accessed the HRIS data, the mean level of invasion of privacy was greater (M = 34.52) than when the HR department accessed it (M = 32.03); in other words, the participants viewed supervisors' accessing HRIS data as more invasive than when the HR department accessed it. The interaction between access to data and individuals' amount of work experience qualified this affect, which we discuss in Section 3.2.4.

3.2.3 Hypothesis 3

Hypothesis 3 states that individuals are less likely to perceive their privacy has been invaded when they can check the accuracy of their data in a HRIS than when they cannot. The results of the regression analysis showed no support for this hypothesis (see Table 3). The t value for the regression coefficient was not statistically significant (β = -.052, t = -.916, p > .05).

3.2.4 Hypothesis 4

Hypothesis 4 states that individuals' amount of work experience moderates the relations among 1) purpose of the HRIS data collection, 2) access to the HRIS data, 3) ability to correct the HRIS data and their privacy perceptions. Results of the regression analysis showed support for two of these interactions (see Table 3). These findings indicated that individuals' amount of work experience moderated the relation between purpose of the data collection [AL1] [KL2] and perceptions of invasion of privacy (β = .338, t = 1.993, p <.05). In addition, individuals' amount of work experience moderated the relation between access to data and perceptions of invasion of privacy (β = -.285, t = 1.459, p <.10). However, individuals' amount of work experience did not moderate the relation between the ability to check the accuracy of data and employees' perceptions of privacy. To understand these interactions, we plotted the data in Figures 1 and 2.



Low level of work experience = t(139) = 2.856 p =.0025
High level of work experience = t(136) = -1.276, p =.10

Figure 1. Interaction of Purpose and Individuals' Amount of Work Experience

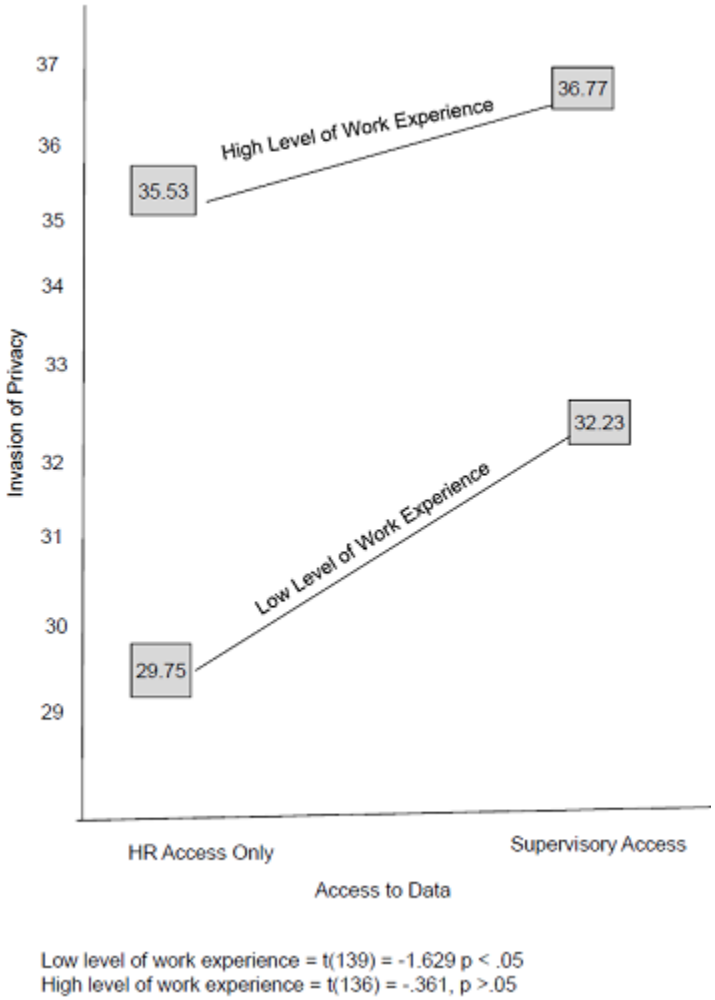


Figure 2. Interaction of Access and Individuals' Amount of Work Experience

Figure 1 shows that, when individuals had high levels of work experience, they more likely perceived that a HRIS used for employee-tracking purposes was invasive (M = 36.38) than one used for HR-planning purposes (M = 35.28). These results are opposite to those that H1 hypothesizes to be the case.

Furthermore, the results reveal that, when individuals had low levels of work experience, they more likely perceived that a HRIS used for HR planning purposes (Mean = 32.85) was invasive than one used for employee tracking (Mean = 28.61) (t[139] =2.86, p = .002). These findings indicate that the relation between purpose of data collection and privacy perceptions depend on individuals' work experience.

The two-way interaction for access and individuals' work experience reveals that, when individuals had low levels of work experience, they more likely perceived that a HRIS was invasive when supervisors had access (M = 29.75) than when HR administrators had access (M = 32.23), (t[139] = -1.629, p < .05). However, when individuals had high levels of work experience, we found no differences in reactions to who had access to the data (M (HR-only access) = 35.53, and M (Supervisory access and HR administrator access = 36.77)) (t[136] = -.361, p > .05). As a result, the relation between access to the HRIS data and invasion of privacy depends, in part, on an individual's amount of work experience.

3.3 Supplemental Analysis

Although we present no hypotheses regarding the relations between demographic variables and employees' perceptions of invasion of privacy, results of correlational analyses (see Table 1) revealed that women, older individuals, and those with higher levels of education levels were more likely to perceive invasions of privacy than their counterparts. We found no relations between knowledge of HRIS or employment status with privacy perceptions.

Also note that, when one uses experimental designs, independent variables are uncorrelated, and each beta weight is equal to the zero-order correlation between the independent and dependent variable (Cohen et al., 2013). Therefore, one can determine the amount of explained variance for each variable by squaring the beta weights. For example, purpose of data collection explained 7 percent and access to data explained 5 percent of the amount of explained variance in privacy perceptions.

4 Discussion

Overall, our results provide qualified support for three of our hypotheses. The results reveal that individuals perceived that a HRIS invaded privacy more when 1) the organization used HRIS data for HR-planning rather than employee-tracking purposes and 2) supervisors had access to the data rather than HR administrators. These findings also showed that these relations depended on individuals' amount of work experience.

The results showed that individuals' amount of work experience moderated the relations between 1) purpose of the data collection, 2) access to data, and 3) privacy perceptions. For instance, the results reveal that individuals with low levels of work experience believed that an organization that used HRIS data for HR planning invaded their privacy more compared to those with high levels of work experience. However, when individuals had high levels of work experience, they felt that an organization that used a HRIS for employee tracking invaded their privacy more than an organization that used a HRIS for HR planning. These results are opposite to our predictions, and we need future research to identify the reasons for these findings. It could be the case that those with little experience are younger and have more knowledge about how organizations use their HRIS data (e.g., to eliminate jobs) than their counterparts.

We also found support for our prediction that amount of work experience would moderate the relation between access to data and privacy perceptions. These results show that, when individuals had low levels of experience, they more likely perceived that a HRIS was invasive when supervisors had access to it than when HR administrators had access to it. However, when individuals had high levels of experience, the results show no differences in reactions to who had access to the data. Again, we need research to understand the bases for these findings. It may be that those with little experience (typically younger workers) more likely know how supervisors use HRIS data than those with considerable experience (typically older workers). Little research has focused on how individual factors are related to reactions to HRIS polices, and we need research to examine how other factors (gender, ethnicity) are related to privacy perceptions.

Surprisingly, our results do not support individuals' amount of work experience as a moderator of the relation between ability to check the accuracy of data and employees' perceptions of invasion of privacy We discuss the potential reasons for this in Section 4.2.

4.1 Implications for Theory, Research, Practice, and Society

We believe that these results have important implications for theory, future research, practice, and society as a whole. For theory, the results support several of the predicted relations in Stone and Stone's (1990) privacy model. In particular, they indicated that reactions to two privacy policies (i.e., purpose of data collection and access to data) depend on individuals' amount of work experience. These findings imply that future research needs to devote much more attention to the interaction of information and individual factors.

We also believe that future research should identify other factors and policies that may affect privacy perceptions. For example, Stone and Stone's (1990) privacy model argues that the type of information and the value regarding control over that information are key determinants of privacy perceptions. However, some types of information may be invasive regardless of the procedures used to manage it. For instance, medical data may be invasive even if employees have the opportunity to correct it because individuals often place considerable value on controlling this type of information because it can potentially stigmatize them. Thus, we believe that the ability to correct highly sensitive data may not alleviate privacy concerns, but the ability to correct job-related data may ameliorate them. Organizations should also establish policies that place limits on the types of data stored in their HRIS and conduct audits to purge files of obsolete or inaccurate data.

Second, our results reveal that who has access to data affects privacy perceptions, but we focused on access to all types of HRIS data. One policy that may decrease concerns about privacy is to give supervisors and HR administrators access to different types of HRIS data. For instance, supervisors need access to

work-history data (e.g., performance appraisals) for HR decisions, but HR administrators need access to race, gender, and disability data for government reporting. Organizations should limit access by the target's need to know the information, and systems should establish strict limits on access to confidential (medical) data.

Third, Stone and Stone's (1990) privacy model suggests that the transparency of the data collection should influence employees' privacy perceptions, and employees may not trust a HRIS if they do not understand how their organization will use their data (Lippert & Swiercz, 2005). Thus, employers might use training to enhance employees' knowledge of how they use their employees' HRIS data. This policy should increase the transparency of procedures and may alleviate concerns about privacy. However, we need research to examine its effectiveness.

Future research might also examine if individual factors (e.g., gender, ethnicity) moderate the relations between HRIS policies and privacy perceptions. For example, some research on selection (Rosenbaum, 1973) has found gender, ethnic, and socioeconomic status differences in privacy concerns about the collection of varying types of data. In particular, women were more concerned about the disclosure of personal information than men, but men were more concerned about the release of financial data than women. Thus, gender may interact with the type of HRIS data to influence privacy perceptions. As we note previously, future research should examine the interactions between individual and informational and/or procedural factors and privacy.

Although no specific laws prohibit the collection of data about age, race, or gender in the US, civil rights laws indicate that these data may serve as prima facie cases of unfair discrimination. As a result, HRIS developers should be familiar with HR and privacy laws and ensure that HRIS keep data about protected classes, medical information, and other confidential information separate from employment records.

Our results also have key implications for society as a whole. Over thirty years ago, the Privacy Protection Study Commission (1977) warned that the proliferation of databases would have a negative effect on privacy in our society. Since those warnings, we have seen numerous breaches of privacy and security in HRIS (Zafar and Stone, 2015). Thus, we believe that organizations need to proactively establish fair information-management policies and security systems that protect the privacy of all members. These policies would ensure a balance between the organization's need for information and individuals' rights to privacy in our society.

4.2 Limitations

Our study has several limitations. First, we conducted the study via a role play, which may have reduced its realism. However, because using simulated settings often reduces effect sizes, these results may have actually underestimated the extent to which HRIS policies affect privacy perceptions. Future research should replicate these findings in actual organizations before making generalizations from this data. A second limitation is that the participants in the study were well-educated individuals in the U.S. Southeast, and they may not represent all employees. Thus, we need research to examine how individuals with diverse backgrounds in other parts of the country react to HRIS policies.

Another limitation is that the study's context may have influenced the results for the ability to correct HRIS data. For example, we asked participants to complete an employment form, which we entered into a HRIS. Therefore, the ability to correct the data manipulation may have been less important in this context than if the system had stored the data for a long time. Future research should examine this policy in other contexts.

In summary, we examined the relations between three privacy policies and one individual variable and privacy perceptions. We hope that our results will help organizations establish fair information policies that alleviate employees' concerns about privacy and ensure their HRIS fairly treat employees' data.

References

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology*, *91*(2) 221-232.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1042.

Black, S. L., Stone, D. L., & Johnson, A. F. (2015). Use of social media in the hiring process and applicants' privacy. *Employee Responsibilities and Rights Journal*, *27*, 115-159.

CedarCrestone. (2013). *CedarCrestone 2012-2013 HR systems survey*. Retrieved from http://www.sierra-cedar.com/wp-content/uploads/sites/12/2014/07/CC_2012-2013_HRS_Survey_WP.pdf

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013), Applied multiple regression/correlation analysis for the behavioral sciences (3rded.). Mahwah, NJ: Lawrence Erlbaum Associates.

Constantin, L. (2011). *Thousands of US Airways pilots victims of data breach.* Retrieved from http://news.softpedia.com/news/Thousands-of-US-Airways-Pilots-Victims-of-Data-Breach-194268.shtml

Eddy, E. R, Stone, D. L., & Stone-Romero, E. F. (1999). The effects of information management policies in reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology*, *52*, 335-358.

Etzioni, O. (1996). The World-Wide Web: Quagmire or gold mine? *Communications of the ACM*, 39(11), 65-68.

FindLaw. (2013). *Who can look at employee personnel files*? Retrieved from http://files.findlaw.com/pdf/smallbusiness/smallbusiness.findlaw.com_employment-law-and-human-resources_who-can-look-at-employee-personnel-files.pdf

Gilliland, S. W. (1993). The perceived fairness of selection systems: An organizational justice perspective. *Academy of Management Review*, *18*(4), 694-734.

Harris Interactive. (2002). *Privacy and the workplace*. Retrieved from http://www.diogenesllc.com/privacyandtheworkplacesurvey.pdf

Hicks, M. (2014). Balancing wellness programs and employee privacy. Retrieved from http://idahobusinessreview.com/2014/01/09/balancing-wellness-programs-and-employee-privacy/

Kavanagh, M. J., Thite, M., & Johnson, R. D. (Eds.). (2015). *Human resource information systems: Basics, applications, and future direction* (3rd ed.). Thousand Oaks, CA: Sage.

Lippert, S. K., & Swiercz, P. M. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science*, *31*(5), 340-353.

Lukaszewski, K. M., Stone, D. L., & Stone-Romero, E. F. (2008). The effects of the ability to choose the type of human resource system on perceptions of invasion of privacy and system satisfaction. *Journal of Business & Psychology*, *23*, 73-86.

Neighly, M., & Emsellem, M. (2013). *Wanted: Accurate FBI background checks for employment. Reward: Good jobs.* Washington DC: National Employment Law Project.

Pedhazur, E. J. (1997), *Multiple regression in behavioral research: Explanation and prediction* (3rd ed.). Belmont, CA: Wadsworth.

Pew Research Center. (2015). Americans' attitudes about privacy, security, and surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Privacy Clearinghouse. (2013). *Chronology of data breaches security breaches 2005-present*. Retrieved from http://www.privacyrights.org/data-breach

Privacy Protection Study Commission. (1977). *Personal privacy in an information society*. Washington DC: U.S. Government Printing Office.

Rosenbaum, B. L. (1973). Attitudes toward invasion of privacy in the personnel selection process and job applicant demographic and personality correlates. *Journal of Applied Psychology*, *58*(3), 333-338.

Sanders, R. (2015). *6 reasons to digitize employee files*. Retrieved from http://www.archivesystems.com/resources/articles/35/6-reasons-to-digitize-employee-files#sthash.eNCw0D2n.dpuf

SHRM. (2015). *Access to personnel files: 50 State laws*. Retrieved from http://shrm.org/legalregulations

SHRM and West Group. (2000). *Workplace privacy survey*. Retrieved from www.shrm.org/surveys

Simmons, D. D. (1968). Invasion of privacy and judged benefit of personality test inquiry. *The Journal of General Psychology*, *79*(2), 177-181.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Socorro v. IMI Data Search, Inc. (2003). U.S. Dist. L.E.X.I.S. 7400.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy value, beliefs, and attitudes across several types of organization. *Journal of Applied Psychology*, *68*(3), 459-468.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection strategies. In K. M. Rowland & G. R. Ferris, (Eds.), *Research in personnel and human resources management* (pp 349-411). Greenwich, CT: JAI Press.

Wilkie, D. (2015). Paid sick leave, data privacy top emerging topics in employee handbooks. Retrieved from http://www.shrm.org/hrdisciplines/employeerelations/articles/pages/employee-handbook-topics.aspx

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the International Conference on Information Systems.*

Zafar, H., & Stone, D. L. (2015). HRIS privacy and security. In M. J. Kavanagh, M. Thite, & R. D. Johnson (Ed.), *Human resource information systems basics, applications, and future directions* (3rd ed., pp. 530-554). Thousand Oaks, CA: Sage Publications.

About the Authors

Kimberly M. Lukaszewski is an associate professor of management at Wright State University. She received her MBA in human resources information systems (HRIS), and her doctorate in organizational studies from the University at Albany, State University of New York. Her research focuses on human resource technology, human resources information systems, information privacy, e-recruitment, social media and its effect on employment decisions, and diversity issues. She has presented numerous papers on these topics at national and regional conferences, and has published articles in *Communications of the Association for Information Systems, Human Resource Management Review, International Human Resources Information Management Journal, Journal of Business and Psychology, Journal of Business Issues, Journal of Managerial Psychology,* and *Journal of Technology Research*. She has served as a Guest Editor for special issues at Transaction on Human-Computer Interaction and Journal of Managerial Psychology. She is currently on the editorial board at Journal of Managerial Psychology.

Dianna Stone received her Ph.D. from Purdue University and is a Visiting Professor at the University at Albany and an Affiliate Professor at Virginia Tech. Her research focuses on electronic human resource management, e-selection, privacy, diversity, and cross-cultural issues in organizations. Results of her research have been published in the *Journal of Applied Psychology, Personnel Psychology, the Academy of Management Review, Journal of Management, Journal of Managerial Psychology*, and *Human Resource Management Review*. She is currently the Editor of Research in *Human Resource Management* and Associate Editor of *Human Resource Management Review*. She has also edited books on Electronic Human Resource Management with Hal Gueutal, and is editing The of Handbook of the Psychology of the Internet at Work with Guido Hertel, Richard Johnson, and Jonathan Passmore. She is a Fellow of the Society for Industrial and Organizational Psychology, the American Psychological Association, and the Association of Psychological Science.

Richard D. Johnson, PhD, University of Maryland, is an Associate Professor of Management, Department Chair, and Director of the Human Resource Information Systems (HRIS) program at the University at Albany, State University of New York. His research focuses on HR Technology, the psychological impacts of computing, training and e-learning, and issues surrounding the digital divide. His research has been published in outlets such as *Information Systems Research, Journal of the Association for Information Systems, Human Resource Management Review,* and the *International Journal of Human Computer Studies.* Dr. Johnson is a Past Chair of AIS SIGHCI and is a Senior Editor at *Data Base* and an Associate Editor at *AIS Transactions on Human-Computer Interaction.* He is also an editor of the book, *Human Resource Information Systems: Basics, Applications and Future Directions.*

Transactions on Human – Computer Interaction