Communications of the Association for Information Systems

Volume 24 Article 15

2-2009

A Hybrid Tracking System of Human Resources: A Case Study in a Canadian University

Manon G. Guillemette
Université de Sherbrooke, Manon.Ghislaine.Guillemette@USherbrooke.ca

Isabelle Fontaine
Université de Sherbrooke

Claude Caron
Université de Sherbrooke

Communications of the Association for Information Systems

CAIS

A Hybrid Tracking System of Human Resources: A Case Study in a Canadian University

Manon G. Guillemette

Geobusiness Group, Faculty of Business, Université de Sherbrooke

Manon.Ghislaine.Guillemette@USherbrooke.ca

Isabelle Fontaine

Geobusiness Group, Faculty of Business, Université de Sherbrooke

Claude Caron

Research Chair in Geobusiness, Faculty of Business, Université de Sherbrooke

Abstract:

Radio Frequency Identification (RFID), including Real-Time Location Systems (RTLS) and Global Positioning Systems (GPS), are technologies that have evolved considerably in the past few years. They have the potential to provide a means by which organizations can follow employees in real time. However, this permanent surveillance may have unexpected impacts on employees as well as on the organization itself. We followed the systems development research process to build a hybrid RFID-GPS system that allowed for the real-time location of human resources both indoors and outdoors. We tested this system in the security service of a Canadian university and explored its impacts on the workgroup and its employees. Our findings suggest that this kind of system can work in a real-world context, and that it has distinct impacts on the individual and the organization of a type not usually observed with more traditional information systems.

Keywords: human tracking system, RTLS, GPS, RFID, prototype, individual impacts, organizational impacts, case study

Volume 24. Article 15. pp. 255-268. February 2009

I. INTRODUCTION

In the last five years, important developments have emerged in the field of Real-time Location Systems (RTLS). Organizations have been using these technologies for many purposes. These new technologies have transformed many companies—along with their working processes—in transportation, health, security, and agriculture and in both the public and private sectors. Following are a few examples that illustrate the magnitude and diversity of the phenomenon. On-board systems and GPS technology have provided major breakthroughs in transportation fleet management (vehicle tracking, speed, waiting time, etc.) [Kumar et al. 2002]. In addition, RFID technology enables parcel tracking [Ngai et al. 2007; Niederman et al. 2007; Srivastava 2005], baggage handling in the airline industry [Wyld et al. 2005], pharmaceutical product returns management and counterfeit identification [Srivastava 2005], shipment tracking and tracing [Ngai et al. 2007; Niederman et al. 2007], and control of access to restricted areas (smartcards) or border control (passports with RFID) [Lockton et al. 2005; Srivastava 2005]. In fact, positioning technologies are becoming increasingly diversified. Examples include GPS or A-GPS, passive RFID, active RFID (or RTLS), smartcards, cellular phones, on-board systems, gyroscopes, infrared-based systems, Wi-Fi, etc. Traditionally, these technologies have mostly been used to trace goods and products, but recently organizations have also begun to use them to locate users, employees and customers [Bergeron et al. 2006; Kaupins et al. 2005; Taghaboni-Dutta et al. 2006]. Technologies that track, trace, and locate are rapidly emerging [Caron et al. 2008; Clarke 2001; Hightower et al. 2001; Ngai et al. 2007].

Real-time people tracking has sparked much controversy [Clarke 2001; Taghaboni-Dutta et al. 2006]. A great deal of the research in this area has focused on the tracking of customers, either on the web or through the use of secondary data [e.g. Chellappa et al. 2005; Culnan 1993; Culnan et al. 1999]. However, few studies have examined the real-time tracking of employees in organizations, even though this practice is growing in importance in organizations today. We believe that this issue and its impacts warrant in-depth study.

Organizations want to know where their employees are and what they are doing when they are at work [Zweig et al. 2002]. If, under normal circumstances, the real-time tracking of employees at all times might seem questionable, it may be entirely relevant in other situations. We worked with a security service that wanted to track, in real time, their security guards in order to ensure their safety and the security of the organization's resources. RTLS technologies have allowed organizations to follow, in real time, the precise locations of their employees both inside buildings and outdoors, but not both at the same time. In a context where security guards patrol both indoors and outdoors, the technology should be able to follow them inside as well as outside buildings.

Despite the fact that there are now many RFID/RTLS technologies on the market (Axcess, Wavetrend, Ekahau, RF-Code, Passport Technology, etc.), it has been very difficult to arrive at the right technological combination for real-time tracking of employees both inside and outside buildings. This is because existing technologies are not effective at providing reliable indoor and outdoor tracking of mobile resources. For example, GPSs are only effective outdoors, and cellular network positioning does not provide adequate spatial accuracy for indoor tracking [Hightower et al. 2001]. Conversely, active RFID technologies (RTLS) capable of providing accurate indoor locations represent an affordable and efficient alternative solution for indoor positioning and may fill a gap left by other technologies [Caron et al. 2008]. The development of an integrated GPS/RTLS system would therefore constitute an important technological development if it can deliver the full potential of both positioning technologies [Asif 2005].

Continuously keeping an eye on employees, on the other hand, might have unpredictable impacts on the individuals and the organization. Because real-time people tracking is an emerging practice, research in this area is still underdeveloped [Clarke 2001]. Thus it is very important to expand our understanding of the characteristics of positioning technologies and how they can be used. We also need to develop a better understanding of their impacts on individuals and organizations.

The purpose of this study was to explore, in a real-world context, the impacts of an innovative human resource tracking technology on a workgroup as a whole and on the members of this workgroup. To this end, we developed a hybrid RFID/GPS system for both indoor and outdoor real-time positioning of the human resources of a security service at a Canadian university. We tested the prototype and explored the technology's impacts in an experiment involving the majority of the security guards employed by the service. The findings show that such a system can function in a real-world context, and that it has surprising impacts on the individual and the organization.

The following section provides a review of the literature on positioning technologies and their impacts. Our research methodology, called the *system development research process methodology* [Nunamaker et al. 1991], is a combined approach involving system engineering and semi-structured interviews. The methodology is presented in the third section. The fourth section presents the prototype development process, and the fifth section describes the technology's impacts and the concerns observed, which are more thoroughly discussed in the sixth section. We conclude with the theoretical and practical implications of this study.

II. LITERATURE REVIEW

RFID and other RTLS technologies are known as facilitators of real-time tracking [Asif 2005]. Electronic tracking of employees, a form of electronic work monitoring, can be considered a specific type of surveillance that presents certain challenges to the companies that use it [Tabak et al. 2005; Zweig et al. 2002]. Surveillance can take many different forms: application sharing, video surveillance cameras, hidden microphones, telephone monitoring of employee conversations, computer-based monitoring of employee keystrokes [Stanton et al. 2000; Zweig et al. 2002], and e-mail and Internet monitoring [Stanton et al. 2000]. However, the introduction of real-time location systems offers a new form of surveillance that expands the scope of surveillance to troubling proportions.

Research on the use of RTLS technologies in surveillance activities has been limited [Clarke 2001]. Some examples of research in this domain are the taxonomy of location systems proposed by Hightower and Borriello [2001]. The main objectives of their taxonomy were to help developers of location-aware applications better evaluate their options when choosing a location-sensing system and help researchers identify opportunities for new location-sensing techniques. They used the taxonomy's four main properties to evaluate the characteristics of location systems needed by particular applications. They recommended that researchers develop technologies on the principle of sensor fusion, defined as "the use of multiple technologies or location systems simultaneously to form hierarchical and overlapping levels of sensing" [Hightower et al. 2001], in order to provide aggregate properties that are not possible when location systems are used individually. Other researchers have provided in-depth discussions of the implications of the use of RTLS technologies by user organizations and governments [Ohkubo et al.] and for technology providers and policy makers [Clarke 2001] as well as other ethical challenges [Glasser et al. 2006; Lockton et al. 2005; Peslak 2005; Taghaboni-Dutta et al. 2006]. Clarke observed that ethical concerns have recently been raised about data surveillance applications in which the whereabouts of an individual can be monitored and movement can be tracked. He urged researchers to identify the impacts of what he called data surveillance technologies on individuals and societies [Clarke 2001]. Finally, Caron et al. [2008] discussed indoor positioning combined with digital mapping and spatial analysis (microgeomatics) and real-time location services. Microgeomatics is the field of real-time tracking and spatial analysis of people and equipment motions in a closed space [Caron et al. 2008]. At the heart of their discussion is a detailed review of existing indoor positioning methods and techniques.

This literature clearly shows that managers can choose from a wide range of RTLS technologies that can be adopted by their organization to track people or goods, either inside or outside buildings. Moreover, the literature establishes that no existing technology used alone is able to locate people or goods both inside and outside buildings. What the literature makes less clear, however, is the fact that organizations also face different choices related to their use of these technologies. For example, organizations can choose to use them to control people, or they can decide to take advantage of RTLS technologies to optimize decision-making processes. In either event, it is very difficult to predict how the people being tracked will react . Even if an organization chooses not to use these technologies to control its employees, employees may still be reluctant to be continuously tracked.

Traceability enabled by real-time positioning technologies can have negative effects, especially when it facilitates an invasion of privacy [Kaupins et al. 2005], thereby contributing to higher stress levels among employees. Traceability may also bring about a certain form of discrimination in the workplace, employee mistrust, and a decline in productivity [Hartman 1998]. On the other hand, positioning technologies can also be valuable for the people and organizations using them. For example, in the health care sector it might be useful to be able to locate patients with problematic diseases such as memory loss [Glasser et al. 2006; Janz et al. 2005]. Another important example of the beneficial aspects of such technologies would be in the security industry, where they could help ensure a safer work environment for the security staff and also greater public safety. In fact, studies have shown that perceptions of the impacts of tracking technologies could be highly context-specific [Culnan 1993].

This experimental and exploratory study therefore aims to provide answers to three specific research questions:

1. Is it possible to develop an efficient human resource tracking system with the ability to track employees both indoors and outdoors in a real-world context? What would the main features of this system be?
2. What are the impacts of a human resource tracking system on individuals?

3. How does a human resource tracking system impact the workgroup?

III. METHODOLOGY

Our study is based on the *system development research process methodology* proposed by Nunamaker et al. [1991]. This approach combines four research strategies: theory building, systems development, experimentation, and observation, and integrates them into a coherent research process of five structured steps. The first step of the methodology is the formulation of research questions and the identification of a strategy for answering them. The second step deals with the development of the system architecture. In this step, the functionalities of system components and the interrelationships between them are defined. The third step is to analyze and design the system. At this stage, the database/knowledge base scheme and processes needed to carry out system functions are developed. The fourth step is to build a prototype. Finally, the fifth step consists of monitoring and evaluating the system. System monitoring can be carried out through case studies, laboratory experiments or field experiments. Then the case studies or experiments can be evaluated through interviews in order to acquire relevant knowledge.

IV. DEVELOPING THE SYSTEM AND ANALYZING ITS IMPACTS

Constructing a Conceptual Framework

To clearly define our research problem, we will now present the context of our experiment. This study was conducted in the security service of a Canadian university. The service employs 12 full-time guards, four part-time guards, and 10 others working on a temporary basis. The campus covers 0.64 square kilometers and comprises approximately 50 buildings. For security purposes it is divided into three main sectors, with a guard assigned to each one. The guard is responsible for patrolling the sector and responding to all emergency calls from that sector. Around-the-clock patrols and surveillance are provided on the campus and scheduled in three eight-hour shifts and two 12-hour shifts, which overlap. In addition, a security guard is present at all times at the control station.

Before beginning a shift, each patrol guard consults the surveillance report prepared by the previous guard. Then the guard starts patrolling his or her sector. The patrol route taken is at each guard's discretion. During evening and night shifts, each patrol guard has to call in regularly (every 30 minutes) to the control station to report their position. The activity diagram shown in Figure 1 summarizes this process.

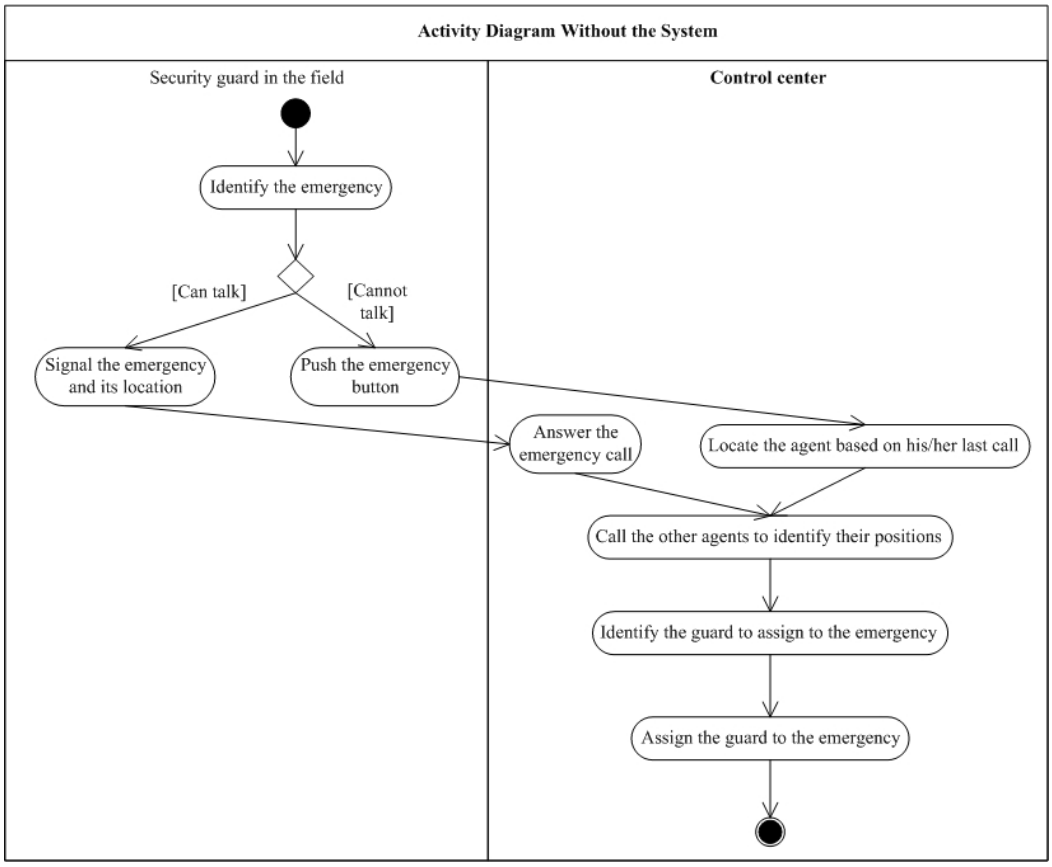

Figure 1. Activity Diagram without the Prototype

The Problem

There are several risks for security guards associated with these practices. For instance, patrol guards may find themselves in situations where they are unable to report their position; they could be unconscious, or under the control of a malevolent individual. In sum, an emergency situation could prevent them from using their radios to report their positions to the guard at the control station. If, for example, the endangered security guard were to have an emergency button to press, it would only inform the control station that a patrol guard is in distress, without indicating position. In such situations, there is no efficient means for the control station to locate the distressed guard on the campus. It might therefore be impossible to send reinforcements in time and to the correct location. The risk is that this practice greatly compromises the guards' safety, not to mention the security they provide on campus.

The Solution

One possible solution to this problem would be to implement a security guard tracking system that would enable the guard at the control station to locate each and every one of the patrol guards at any given time. Thus, in an emergency, it would be possible to send other patrol guards to the distressed guard's precise location to ensure their safety as well as campus security. This system would also help the guard at the control station coordinate interventions by identifying which patrol guard is closest to the scene of the emergency and direct that guard to respond. Figure 2 shows the activity diagram for this system. In a situation of a guard being unconscious and unable to press the button, the control station will be able to detect a potential problem with the system. Indeed, on the control station's screen, the position of the guard will remain unchanged for a relatively extended period of time indicating that something wrong probably happened. The guard at the control station will then call the patrolling guard supposedly in distress, and in case of no answer, will send rescue. Given the fact that security guards patrol both indoors and outdoors and there are currently no means for accurately tracking individuals under these conditions, the development of such a system for security services is highly relevant.

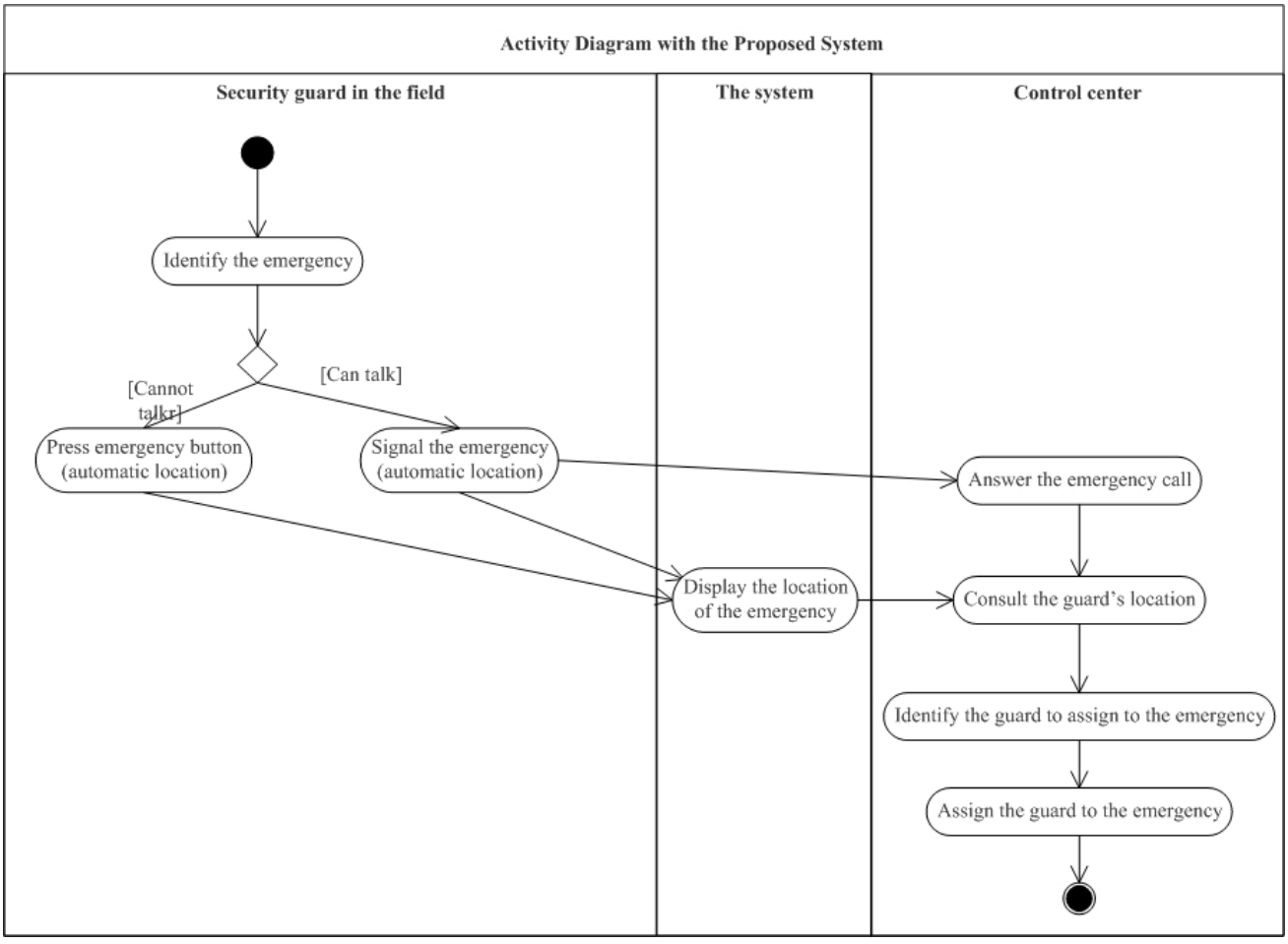

Figure 2. Activity Diagram Using the Prototype

System Architecture

A positioning system designed to solve these issues should enable real-time tracking of patrol guards within buildings and outdoors on the campus. We therefore developed a system that would meet these requirements, and

Communications of the Association for Information Systems

tested it in the context of the university campus security service described above. Finally, we evaluated the impacts of the system on both the workgroup and the security guards.

System Analysis and Design

Technology provides different ways to locate a person. For instance, a GPS uses a GPS receiver that picks up emission signals sent by a plurality of satellites and a trilateration (distance measurement) process to determine a position [Hightower et al. 2001]. Trilateration is a method for determining the intersection of three spherical surfaces given the centers and radii of the three spheres [Caron et al. 2008]. Yet one of the disadvantages of GPS systems is that they cannot provide indoor tracking [Hightower et al. 2001; Xiang et al. 2004]. However, the accuracy of GPS is quite good for locating persons (1-5 metres) [Hightower et al. 2001]. Similarly, cellular telephone networks can identify the approximate position of a mobile device by detecting which cell is being used by the device [Clarke 2001]. However, the accuracy of this technology is still insufficient (approximately 200 meters, depending largely on the size of the cell).

Moreover, there are several technologies that provide indoor tracking, such as technologies based on active (RTLS) radio-frequency identification (RFID). RFID only provides short-distance radio signal transmission to RFID readers [Caron et al. 2008]. Once picked up by a reader, these signals are relayed to a computer to be processed. RFID tags can be active or passive [Asif 2005]. Active tags have their own energy source and send the identification and position data needed for real-time tracking. Passive tags have no battery and are activated using the power generated by the magnetic field of the radio waves of the reading sensor. As a result, they are only activated when they are near a reading sensor, and this reduces their scope. Passive tags are therefore a constraint on establishing real-time tracking.

Another active RFID approach is based on the use of the radio waves of Wi-Fi technologies [Pahlavan et al. 2002; Xiang et al. 2004]. As opposed to the traditional RFID approach, the Wi-Fi approach does not require the installation of specific aerials or receivers, only needs a connection to an existing Wi-Fi network [Caron et al. 2008]. This positioning method usually consists of gathering signals and mapping their distribution. It requires the installation of at least three receptors per positioning point. When appropriately calibrated, Wi-Fi provides sufficient accuracy [Hightower et al. 2001]. The positioning model resulting from this procedure can then be applied to identifying the position of an object or person [Xiang et al. 2004].

In choosing from these technologies for our study we took into account several characteristics specific to the university campus. First of all, we had to ensure that the entire campus was covered with the chosen tracking technology. Second, we eliminated methods requiring the purchase of expensive RFID antennas due to financial constraints. Finally, we discarded solutions based on cellular identification because of their poor accuracy. This narrowed our choices down to GPS and RTLS technologies. While GPS is a very accessible technology, it can only be used for outdoor positioning. On the other hand, at the time of our study 90 percent of the buildings located on the main campus were already equipped with Wi-Fi access, but this access was limited to inside campus buildings. We therefore decided to design and develop a hybrid GPS/RTLS (or active RFID) solution for security guard tracking.

Tracking Device

For the outdoor tracking, we integrated GPS receivers into the microphones of radios that were similar to those already used by the security patrol guards. In the course of the experiment, the participating guards were given Kenwood TK-3180K2 radios equipped with Kenwood KMC-38GPS microphones. The GPS receiver in the microphone reported its position through radio waves at a given frequency. For the indoor tracking, we chose an Ekahau RTLS hardware and software solution that offers real-time people tracking anywhere there is Wi-Fi coverage. This solution was chosen from the various RTLS tracking solutions because we already had access to the necessary equipment (Ekahau beacons) and software licenses needed to develop the prototype.

Data Transmission

In order to design the system architecture, we first identified three different themes for the system design: functional architecture, technological architecture, and data architecture. We decided to carry out the modeling using the UML language. Figures 1 and 2 illustrate the activity diagram before prototype use (the before situation) and with prototype use (the experimental situation). Figure 3 shows the data transmission protocol used in our prototype.

Before our system was implemented, when a patrol guard was in distress and could not report his position, the guard at the control station could only make a rough estimate of his position according to the information he had sent to the control station during his last report. With the new system, the position was automatically available in real time.

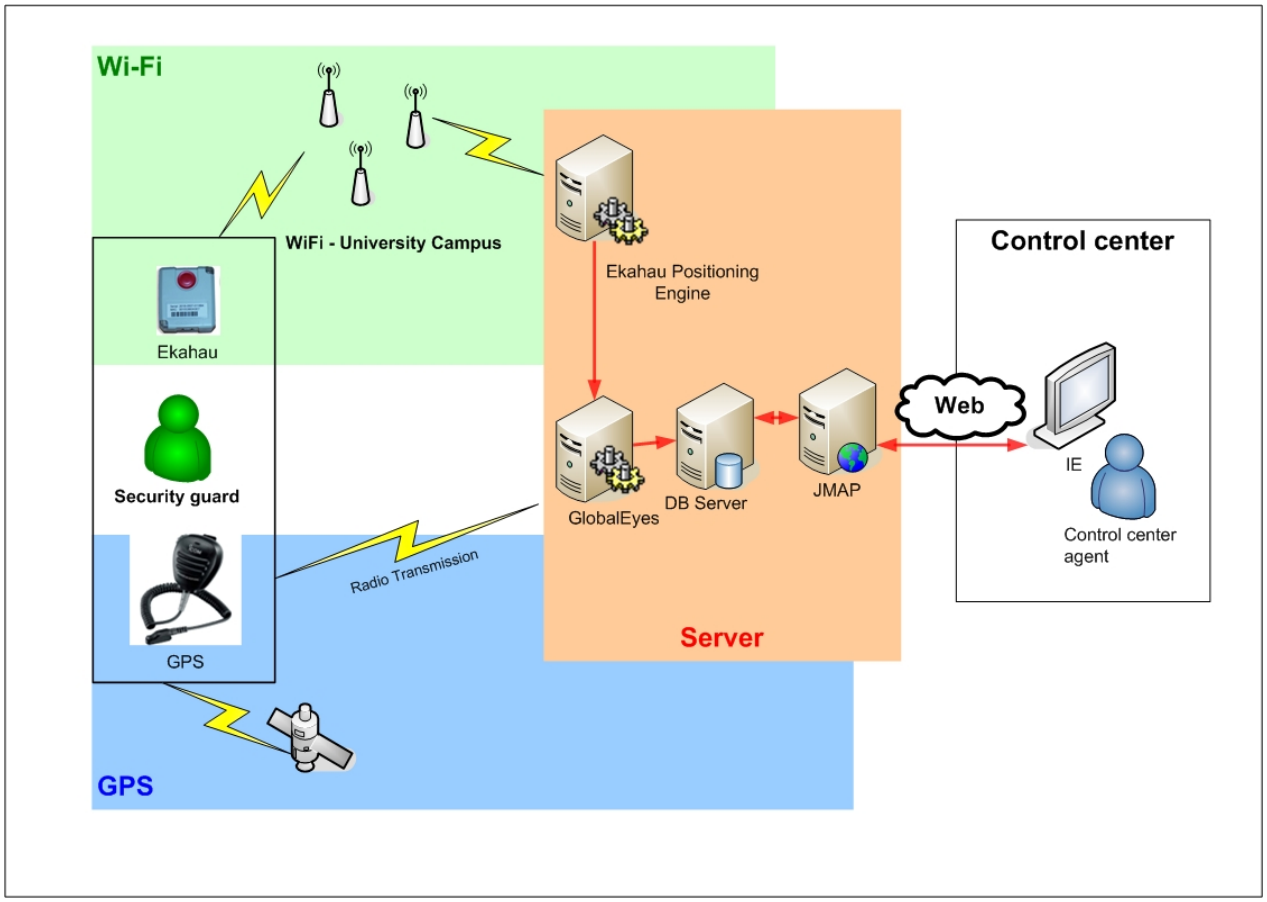

Figure 3. Architecture of the Prototype

When the patrol guard was inside a campus building, the Ekahau beacon would send the data from the received radio-wave signals to the positioning device. The positioning device would then calculate the guard's position using a calibrated spatial model. When the patrol guard was outdoors but still on the campus, the GPS receiver would calculate his position by trilaterating signals from satellites. This data would then be sent to a middleware (Global Eyes from Mercanstream Technologies) that would process the raw positioning data and transmit it back to the data server. Finally, JMap software (Kheops Technologies) would display the position of the guard in a Web browser by superimposing the positioning data on a map of the campus (outdoors) or on a map of each building (indoors) (see also Figure 4).

Building the Prototype

The prototype was built in three major stages. First of all, the entire campus was mapped. The exterior features of the campus were already available in spatial geo-referenced shapefiles. The plans of the buildings, originally in DWG format (AutoCAD), were converted into shapefiles and then geo-referenced.

Second, the positioning model was built and adapted to the Ekahau system (for the indoor tracking). This means that the movements most likely to occur inside buildings were schematically represented as "rail" shapes, then the positioning model was calibrated by physically recording radio-wave signals at various sample points (every 3 to 5 meters) on each floor of the campus buildings so as to ensure high positioning accuracy.

Third, the software interface was programmed using the JMap developer toolkit. The necessary telecommunications and positioning equipment was acquired, and, finally, rigorous functional tests were carried out on the overall system in our laboratory before it was deployed at the control station and in the hands of the security guards.

System Monitoring and Evaluation

The security guards were contacted through a letter and asked to participate in the study. Twelve guards agreed to carry the equipment during their shifts and participate in an interview afterwards. The prototype experiment was carried out from November 27 to December 11, 2006. At the start of each working shift, a member of the research team was on site to install the device and explain how the software worked to the guard at the control station. We

collected positioning data during 40 of the 42 work shifts during the experimental period. Most of the time, two or three guards carried the device during each work shift.

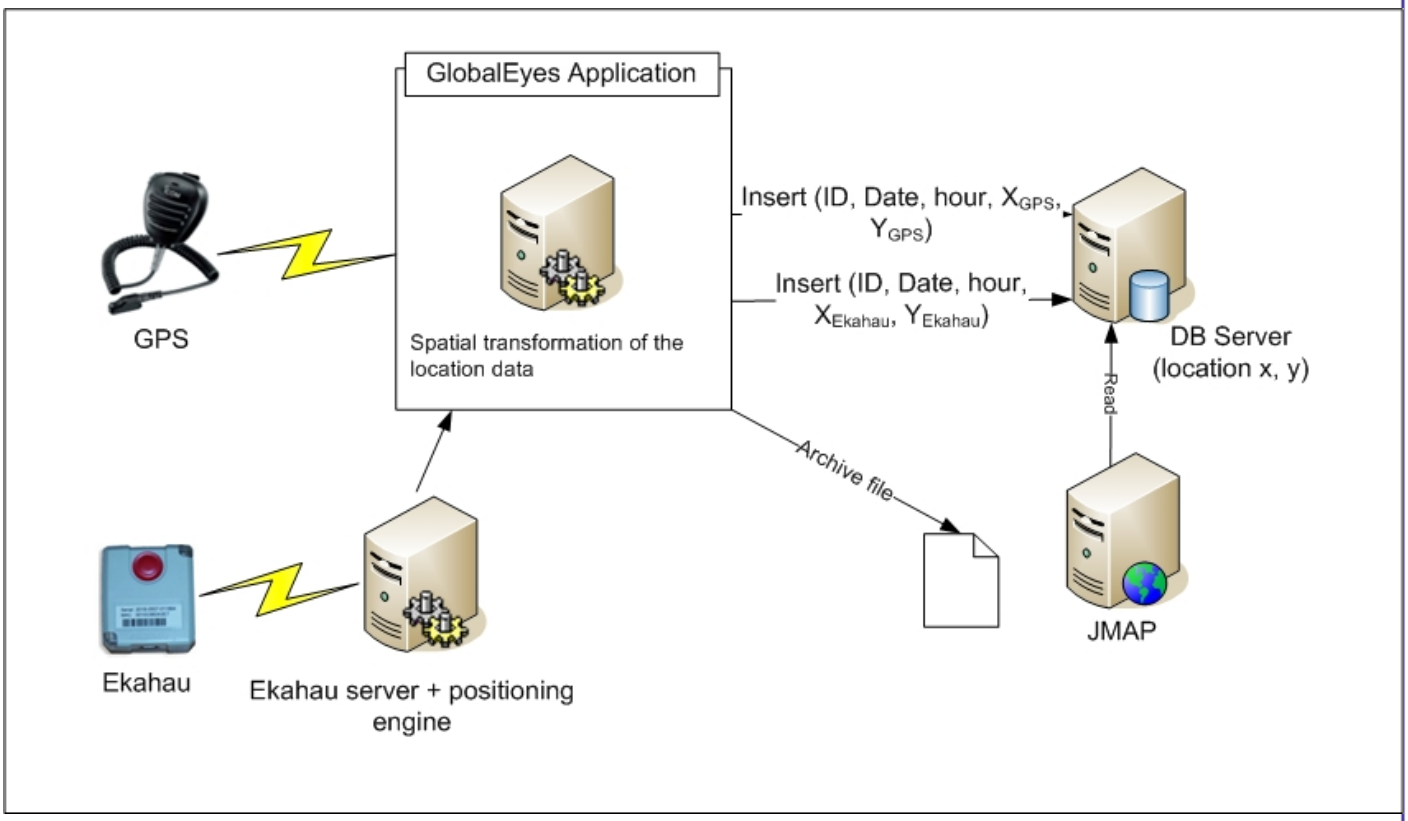

Figure 4. Data Transmission to the Server

Semi-structured interviews were conducted with the participants in the week following the completion of the experiment. Both the guards that used the system at the control station and those that carried the device on patrol were interviewed. We also conducted interviews with some of the security service directors in order to evaluate the impacts on the organization. The interviews were recorded and transcribed. The analysis was carried out through an iterative coding process. The observations made and notes taken during the experiment by members of the research team were transcribed and analyzed in a similar manner. This evaluation of the system was meant to determine how it could be improved and measure the potential impacts on individuals and the organization.

V. RESULTS

This section begins with a presentation of system characteristics. This is followed by a presentation of observed impacts on individuals, and we end with the observed impacts on the workgroup.

System Characteristics

The experiment presented here confirms that it is possible to develop a system that satisfies all of the important characteristics described above, namely real-time tracking as well as indoor and outdoor tracking. To this end, we surveyed the patrol guards for their perceptions of the different characteristics of the system.

Concerning the system software used at the control station, the guards noted the ease of use of the interface and the suitability and utility of the functionalities offered. The only suggested modification involved displaying the building number of the premises on the building plans.

As for the information characteristics, two concepts were highlighted during the interviews: information accuracy and information exactness. These elements were directly influenced by the technological choices we were forced to make — especially the refresh frequencies, which were too long (five minutes for the GPS and 15 seconds for the Ekahau tag) — and some physical limitations on the campus (the Wi-Fi network only covered 90 percent of the campus). Our data indicated that the refresh rate was not high enough to satisfy the agents. Most of them would have liked a tracking system with a refresh rate of about one minute. This system parameter depended on the number of wireless access points we were able to use, and sometimes they were insufficient. Achieving a positioning accuracy of under five meters [Ekahau 2007] would have taken three wireless access points per location.

Some of our sectors had only one available access point. In sum, the intrinsic characteristics of the system determined the refresh rate of the prototype, which was causing delays and dissatisfaction. Several of the agents saw a relationship between the characteristics of the system and this problem. For example, officers said there was room for improvement, since the refresh rate exceeded one minute and this caused data distortion.

> Your project has a lot of potential. However, the tracking could be monitored with a one-minute delay. Actually, if you follow someone and you need to know exactly where they are, for example, in an emergency situation, the system is a little bit misleading. (Guard #5)

Finally, the guards expressed satisfaction with the equipment used (radio and tags), and added that the equipment did not interfere with their work, suggesting another important characteristic of such a system — transparency. The patrol guards did suggest two modifications to the functioning of the radio in order to make it more convenient to use. They mentioned a shrill sound that occurred when the GPS receiver was out of range. Some patrol guards also found it uncomfortable to hear crackles every five minutes when the radio sent positioning data to the system and when they would release the radio transmit key. The guards stressed the importance of solving these problems before considering a permanent use of the system, again reinforcing the importance of transparency.

Individual Impacts

We tried to gain a better understanding of the system's impacts on the guards. More specifically, we asked them what their impressions were of their experience, then we asked whether or not they would be interested in continuing to use such a system, and why. We learned that organizational directives, perceptions of usefulness and privacy invasion, and procedural justice were key to understanding the guards' intention to adopt such a system.

Perception of Utility

We found that the specific characteristics of the system largely influenced the guards' perceptions of its usefulness in their work. Indeed, some of the guards mentioned that, within the context of the experiment, inaccurate information (mainly due to slow refresh rates) made them doubt the usefulness of the system.

> It doesn't take long to understand that the refresh rate is too slow to track a person 'step by step,' so it is doubtful that we could use this system in emergency calls. (Guard #9)

Others took into account the fact that the proposed system was a prototype and concluded that a real-time tracking system like the one they had tested could be very useful, both to improve communication between the patrol guards and with those at the control station and to make patrolling safer. Finally, some guards mentioned the usefulness of such a system to optimize reinforcement dispatches by identifying which patrol guard is closest to the scene of the emergency.

> When there was an emergency call, we were able to identify that he [a specific patrol guard] is the closest, and this functionality appears to be useful. (Guard #12)

Organizational Directives

The guards often mentioned the influential power of the organizational directives (conditions associated with the use of the system) on their behavior with respect to the system and their intention to keep on using it on a continuous basis. These conditions determine "who" (who has access to the data), "how" (how the collected data are being used) and "why" (what are the intentions of the other persons who have access to the data, such as supervisors).

Within the framework of our experiment, we exercised some control over this variable. More specifically, we denied data access to the supervisors and other executives of the security service in order to ensure that we would have the guards' participation. The only persons authorized to consult the security patrol guards' movements were the guards at the control station and the research team. In real life, the situation might have been different. The participating guards told us that they would have felt uncomfortable participating in the experiment if their superiors had had access to the data and had been able watch their movements all day long. Fundamentally, it is the perception, from the security guards, of the way the superiors might want to use the collected tracking data that makes the difference with respect to individual impacts.

> It would certainly have made a difference; in other words, if the boss had said: "We use the system, and have full access to everything that is going to happen." In that situation, fewer of us would have participated. I might have refused as well! What matters is: what is the purpose at the very end? (Guard #3)

Some of the guards even said that they would not carry a tracking device in the future unless their superiors were perfectly clear about how the data would be used.

Perception of Privacy Invasion

A third concept that was highlighted in the interviews was privacy invasion. When the guards were asked if they felt that their privacy had been invaded during the experiment, most of them answered that it had not. We nevertheless found some inconsistencies in their responses that suggested the opposite.

For example, the security guards first said that they did not feel that their privacy had been invaded because they did not see this question as relevant to their work, and that they had "nothing to hide."

> No, it is not really my private life, because I am working, and I am paid to do the job. (Guard #3)

But later in the interviews, some remarks revealed that they did feel an invasion. These remarks included words like spy, eye, big brother, etc. For instance, when Guard #6 was asked, at the outset of the interview, if he had felt that his privacy was invaded, his answer was no, but later he said:

> It's as if there's an eye constantly watching you, that's what's most embarrassing. (Guard #6)

Perception of Justice

The fourth concept emphasized in the interviews was justice (or fairness). Most of the guards found it fair to be tracked by a real-time positioning system. Yet others saw a close link between the perception of justice and organizational directives. As a matter of fact, these guards thought that it was perfectly fair to be tracked, as long as the system was not used to question their work. They underscored the fact that they believed the situation to be fair as long as the system was used as an additional tool to support locating guards in distress. But if the system were to be used to question the relevance of their choices or ask them to justify their movements, they would consider it profoundly unfair to be tracked in this way. They would lose confidence in their work, and they considered this unacceptable.

> Question: Did you think it was fair to track the guards' positions?
>
> Answer: Yes, but we must remain careful. We should never be asked: What were you doing there? (Guard #2)

Finally, some guards mentioned that the lack of accuracy and exactness in the positioning data (due to the slow refresh rates) made the whole tracking process unfair in their eyes. Indeed, they were anxious about the fact that someone consulting the data might reach false conclusions about their work.

> It's fair [to be tracked], but the slow refresh rate could make somebody say: Ah, the guard stayed there 10-15 minutes. But in fact that's not true. It was due to the wrong delay, so no, [it isn't fair]. (Guard #9)

Issues Facing the Workgroup

Our third research question deals with the impacts of such a tracking system on the workgroup. The results indicate that the security guards found some aspects of the system very useful. In particular, they emphasized the importance of rapidly obtaining the information needed for decision-making in emergency situations. For instance, to know the position of each patrol guard at a glance, so as to identify which guard is the closest to the response situation, appears very useful and absolutely relevant to their work. However, since no real emergency situation occurred during the experiment, our subjects did not have an opportunity to test their perceptions.

Moreover, since this particular campus is small, the guards were not convinced that the system would improve their response capabilities. However, they were convinced that in similar contexts but with larger areas to patrol and more patrol guards, this system would clearly improve response times.

> Only once is enough for it to be decisive: at some point, if you need someone quickly. [With this system], the guard at the control station is able to see if there is someone close by […]. You must make a quick decision. You turn back and look at the screen. You see that there is a guard 30 seconds away from the place you want to send a response…Yes indeed, it could be useful. (Guard #4)

Finally, one of the supervisors of the security service stressed the importance of using the resulting information to improve work processes. In his opinion, the information retrieved from the system could help optimize patrol routes. In other words, the system could create a patrol plan that would ensure coverage of the whole area while minimizing the guards' movements. This would result in cost savings, along with better security on the campus.

> It could impact the patrol routes. For example, one of my current tasks is to identify what is essential on the patrols in each sector, how much time should be spent in each building, etc.

> Visualization would provide a picture of what is currently taking place. Visualizing [the data provided by the system], I could see how, a week ago, the five guards on duty from Monday to Friday performed their evening patrol, how long they stayed in the buildings, which floors they patrolled... I could do all this from my office. But actually, I will have to go out in the field. It would sure help us a lot when we create patrol plans.

VI. DISCUSSION

In this study we employed a methodology inspired both by system engineering and semi-structured interviews. This approach allowed us to develop a hybrid RFID/GPS system that provided both indoor and outdoor real-time human resource tracking and the capacity to evaluate the related impacts on individuals and organizations. We believe that our experimental study, which followed a "theory in use" approach rather than a "theory espoused" approach (Argyris et al. 1995], was appropriate for finding relevant answers to our three research questions.

In fact, our results proved that it is technologically possible to develop an innovative real-time tracking system using RTLS technologies and GPS. Our respondents suggested a few improvements to the prototype that would make it fully operational. In particular, they suggested modifying the refresh rate and improving the accuracy and exactness of the system. Because the study was carried out in an experimental context, we had to make technological choices that influenced system characteristics. However, the respondents stressed the importance of making the necessary changes before any permanent implementation of the system in order to ensure its adoption. The guards' recommendations reinforce the importance of implementing a system with as few functional defects as possible in order to avoid user resistance and encourage use [Ngai et al. 2007].

In addition, our results brought out a key point on which all the security guards agreed: the importance of clear organizational directives. The organization's and the superiors' intentions regarding the use of this system appeared to weigh heavily in the guards' decisions on whether or not they would adopt the system. The idea that their superiors might have access to the data made several security guards very uncomfortable. Others were more open to the idea, but clearly expressed their need to know the organization's true intentions with respect to the system and, more specifically, with respect to how the data would be used. The importance given to organizational directives also arose with respect to perceptions of justice and privacy invasion. As other authors have observed in similar contexts [Culnan 1993; Culnan et al. 1999; Zweig et al. 2002], perceptions of privacy invasion and justice are essential to understanding individuals' reactions towards certain types of information systems. We will discuss each of these concepts in the following paragraphs.

Privacy protection is defined as the right of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [Westin 1967]. For individuals, one of the major characteristics of privacy protection is the right to move anonymously [Westin 1967]. Consequently, tracking a person's position is considered sensitive information with a direct impact on privacy [Hengartner et al. 2005]. We found contradictions in the interviewee's responses regarding their perceptions of privacy invasion. These contradictions can be explained by imagining a pair of scales in which there would be perceptions of privacy invasion on one side and perceptions of individual security (a benefit) on the other. Individuals will agree to be tracked as long as the perceived benefits exceed the inconveniences [Culnan et al. 1999]; therefore, using the system as a working tool to ensure the guards' safety helped several guards agree to give up some of their privacy, which they considered less important than their personal security. In contrast, the guards' perceptions of privacy invasion became very important in the context of the system used as a tool to control their work.

The perception of organizational justice refers to people's concerns regarding the systems that affect them at work [Greenberg 1990]. There are at least two types of organizational justice: distributive justice and procedural justice. Distributive justice refers to the justice of the result. It is inspired by equity theory, according to which individuals compare their personal "effort/remuneration" ratio with those of others [Greenberg 1990]. On the other hand, procedural justice refers to the perceived justice of the politics and processes tied to decision-making [Greenberg 1990]. Therefore, an individual who perceives the processes leading to a decision as fair is usually more satisfied with the decision rendered than someone who sees the same processes as unfair [Greenberg 1990]. Surveillance and tracking systems are mainly associated with procedural justice, since they figure among the tools used to evaluate work. Within the framework of our study, the security guards felt that using the system as a means to evaluate their work would have been absolutely unfair. Moreover, they were concerned about the informal judgments that their managers and colleagues might make about them on the basis of erroneous information provided by the system. For these reasons, they felt that the tracking was unfair. Conversely, using the system to support their work was considered entirely fair.

Finally, we focused on evaluating the potential impacts of such a real-time tracking system on organizations. The respondents indicated that such a system would mainly be useful as a means to rapidly provide vital information to

support decision-making in emergency situations. Respondents mentioned that the ability to immediately know security guards' positions in an emergency would help improve the service's response times. In fact, they pointed out that the broader the area to be covered and the greater the number of people to be tracked, the more useful the system would be. Finally, the supervisors mentioned their interest in using the data provided by the system to analyze patrol patterns, optimize patrol efficiency, get the most out of their human resources and improve the overall safety of the area.

Limits of the Study

The results presented herein must be evaluated within the limits of the study. We must reiterate the fact that the prototype was tested in a real, but controlled, environment and for a short period of time. No emergency situations occurred during this period, which limited the scope of our experiment, yet the guards referred to past experiences, as if to infer the potential usefulness of the system. It may also be possible that since the guards were working in an experimental context, they may have not used the system as seriously as they would have in real life. In addition, we decided not to change the guards' working practices during the experiment, which might have limited the potential benefits associated with system use. Care should therefore be taken when generalizing the results of this study to other organizational contexts. Finally, we chose not to give the supervisors access to the data, which may limit generalizations. However, this choice proved to be relevant, since it not only encouraged the guards to participate in the study, it also emphasized the influence of the organizational directives on the guards' adherence to such a system.

Managerial and Theoretical Contributions

This study has opened various research avenues, and its implications are numerous. First of all, our community would benefit from a better understanding of why some guards refused to be tracked in our experiment. Since only one nonparticipating guard shared his reasons for not participating, we were unable to provide any satisfactory explanation for this issue. However, a better understanding of the determinants of participation in tracking studies will allow researchers to improve participation levels by managing these factors. This could facilitate the development of an important body of knowledge on tracking technologies and their management.

Moreover, we noticed important contradictions in some of the participants' responses, particularly with respect to perceptions of privacy invasion. We believe that in order to better understand how tracking systems impact the perception of privacy invasion, it will be necessary to study the source of these contradictions. Some of our observations indicate that individual characteristics could be an important determinant in the perception of privacy invasion, as observed by other researchers [Smith et al. 1996]. We believe that this issue should also be explored in future research. This could help us to develop tracking systems that are more easily accepted by users.

Also, our results proved that this system could be useful in various contexts in which indoor and outdoor tracking is necessary. The system could support, for example, crisis management when actions need to be coordinated (civil crises, police responses, fires, etc.) [Caron et al. 2008]. It may also be useful in hospitals, where it could be used to track high-risk patients or health care professionals. In fact, the system we have developed could easily be adapted to other contexts. A better understanding of the adoption process for this type of system could support successful implementations and realize potential benefits for individuals and organizations.

Finally, in order to fully capitalize on the potential benefits of tracking systems, managers wishing to set up such a system in their organization should pay particular attention to employees' perceptions of how the organization will use the system and the data it generates. Such systems should clearly be presented and used as tools intended to support the work of employees and not as control tools. The planning of implementation processes should therefore incorporate intensive communication activities aimed at clarifying the organization's intentions in order to build trust and acceptance of these systems.

To conclude, within the framework of this research we have developed a unique and innovative system that combines dynamic mapping, GPS positioning and RTLS positioning. One of the most important issues resulting from the use of this type of system is whether or not improvements to collective security will compensate for the breaches of privacy that may arise. This issue appears to be particularly relevant at a time when national and international authorities are imposing security measures (such as counter-terrorism and gun control measures) while individuals are claiming their legal right to privacy. This subject clearly deserves further investigation, and we encourage further academic work in this area.

ACKNOWLEDGEMENTS

The authors wish to thank the Social Sciences and Humanities Research Council of Canada (SSHRC), the Natural Sciences and Engineering Research Council (NSERC) of Canada, and the Research Chair in GeoBusiness (Faculty

of Business, Université de Sherbrooke) for funding this research. The authors would also like to express special appreciation to Professors Martin Richter and Michel Berthiaume. Finally, our sincere appreciation to all the people who agreed to participate in this experimental study.

REFERENCES

Argyris, C., and D. Schon. (1995). *Organizational Learning II: Theory, Method and Practice* Addison-Wesley: Massachussett.

Asif, Z. (2005). "Integrating the Supply Chain With RFID: A Technical and Business Analysis," *Communications of the AIS* (15) pp 393-427.

Bergeron, F., L. Gingras, and C. Caron. (2006). "A Framework for Evaluating Strategic Location-Based Applications in Businesses," *Canadian Journal of Regional Science/Revue canadienne des sciences régionales* (XXIX:3), pp 461-474.

Caron, C., D. Chamberland-Tremblay, C. Lapierre, P. Hadaya, S. Roche, and M. Saada, M. (2008). "Indoor Positioning," in: *Encyclopedia of GIS,* S. Publications (ed.).

Chellappa, R. K., and R. G. Sin. (2005). "Personalization versus Privacy : An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), pp 181-202.

Clarke, R. (2001). "Person Location and Person Tracking. Technologies, Risks and Policy Implications," *Information Technology & People* (14:2), pp 206-231.

Culnan, M. J. (1993). ""How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp 341-363.

Culnan, M. J., and P. K. Armstrong. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp 104-115.

Ekahau. (2007). "So Small, Yet So Accurate. Real-Time People and Asset Tracking Over Wi-Fi Networks," 2007.

Glasser, D. J., K. W. Goodman, and N. G. Einspruch. "Chips, Tags and Scanners: Ethical Challenges for Radio Frequency Identification," *Ethics and Information Technology* (9), pp 101-109.

Greenberg, J. (1990). "Organizational Justice: Yesterday, Today and Tomorrow," *Journal of Management* (16:2) pp 399-432.

Hartman, L. P. (1998). "The Rights and Wrongs of Workplace Snooping," *The Journal of Business Strategy* (19:3) pp 16-19.

Hengartner, U., and P. Steenkiste. (2005). "Access Control to People Location Information," *ACM Transactions on Information and System Security* (8:4), pp 424-456.

Hightower, J., and G. Borriello. (2001). "Location Systems for Ubiquitous Computing," *IEEE Computer* (34:8) pp 57-66.

Janz, B. D., M. G. Pitts, and R. F. Otondo. (2005). "Information Systems and Health Care II: Back to the future with RFID : Lessons Learned - Some Old, Some New," *Communications of the AIS* (15), pp 132-148.

Kaupins, G., and R. Minch. (2005). "Legal and Ethical Implications of Employee Location Monitoring," Proceedings of the 38th Hawaii International Conference On System Sciences, Los Alamitos.

Kumar, S., and K. B. Moore. (2002). "The Evolution of Global Positioning System (GPS)," *Journal of Science Education and Technology* (11:1), pp 59-80.

Lockton, V., and R. S. Rosenberg. (2005). "RFID: The Next Serious Threat to Privacy," *Ethics and Information Technology* (7), pp 221-231.

Ngai, E. W. T., T. C. E. Cheng, S. Au, and K.-h. Lai. "Mobile Commerce Integrated with RFID Technology in aContainer Depot," *Decision Support Systems* (43), pp 62-76.

Niederman, F., R. G. Mathieu, R. Morley, and I.-W. Kwon. (2007). "Examining RFID Applications in Supply Chain Management," *Association for Computing Machinery. Communications of the ACM* (50:7), p 92.

Nunamaker, J. F., M. Chen, and T. D. M. Purdin. (1991). "Systems Development in Information Systems Research," *Journal of Management Information Systems* (7:3), pp 89-106.

Ohkubo, M., K. Suzuki, and S. Kinoshita. (2008). "RFID Privacy Issues and Technical Challenges," Association for Computing Machinery. *Communications of the ACM* (48:9), p 66.

Pahlavan, K., X. Li, and J.-P. Makela. (2002). "Indoor Geolocation Science and Technology," *IEEE Communication Magazine* (40), pp 112-118.

Peslak, A. R. (2005). "An Ethical Exploration of Privacy and Radio Frequency Identification," *Journal of Business Ethics* (59:4), p 327.

Smith, H. J., S. J. Milberg, and S. J. Burke. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp 167-196.

Srivastava, L. (2005). "Ubiquitous Network Societies: The Case of Radio Frequency Identification," ITU Workshop on Ubiquitous Network Societies, Geneva, Switzerland, p. 38 p.

Stanton, J. M., and E. M. Weiss. (2000). "Electronic Monitoring in Their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance," *Computers in Human Behavior* (16) 2000, pp 423-440

Tabak, F., and W. P. Smith. (2005). "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development," *Employee Responsibilities and Rights Journal* (17:3), pp 173-189.

Taghaboni-Dutta, F., and B. Velthouse. (2006). "RFID Technology Is Revolutionary: Who Should Be Involved in this Game of Tag? " *The Academy of Management Perspectives* (20:4), p 65.

Westin, A. F. (1967). *Privacy and Freedom*, (1st ed.) Atheneum, New York.

Wyld, D. C., M. A. Jones, and J. W. Totten. (2005). "Where Is My Suitcase? RFID and Airline Customer Service," *Marketing Intelligence & Planning* (23:4/5), pp 382-395.

Xiang, Z., S. Song, J. Chen, H. Wang, J.Huang, and X. Gao. (2004). "A Wireless LAN-Based Indoor Positioning Technology," *IBM Journal of Research and Development* (48:5/6), pp 617-626.

Zweig, D., and J. Webster. (2002). "Where Is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23:5), pp 605-633.

ABOUT THE AUTHORS

Manon G. Guillemette is an assistant professor of Information Systems, a researcher with the Geobusiness Group and the director of a research group on business intelligence named PRISME at Université de Sherbrooke, Canada. She received her Ph.D. in Business Administration from HEC Montréal. Her research interests include management of the IT function and the contribution made by IT to organizations. She is also interested in tracking technologies and business intelligence. Findings from her work have recently appeared in the proceedings of the *Hawaii International Conference on System Sciences*, the *International Conference on Information Systems*, the *Americas Conference on Information Systems* and the *Administrative Sciences Association of Canada*.

Isabelle Fontaine is an IT professional who works for the City of Montreal in Quebec (Canada) as an business analyst. She recently received her Master's in Business Administration with a specialization in management of information systems from the Université de Sherbrooke. She is interested in tracking technologies, business intelligence, IT security and auditing. Findings from her work have recently appeared in the proceedings of the *Hawaii International Conference on System Sciences.*

Claude Caron is a full professor of Geographic Information Systems (GIS) at the Faculty of Business at the Université de Sherbrooke, director of the GeoBusiness Research Group, and Holder of the Chair in Business Geomatics. After completing a Master's degree in Geodetic Sciences in 1991, he worked as a lecturer and scientific researcher at the *École polytechnique Fédérale de Lausanne* (EPFL —Switzerland) until 1994. He then completed a Ph.D. (Geomatics) at Laval University in January 1997, worked for DMR Consulting Group Inc. as a senior geomatics consultant until 1999, and was a professor of geomatics at Laval University until 2002. His current research interests include studying and improving business processes for implementing geomatics technologies.

Communications of the Association for Information Systems

ISSN: 1529-3181