PLNU/Bus 625 Marketing Research Project

Privacy Vs. Safety: Acceptance of Tracking Technology

Marketing Research Report: Spring 2017

Nick Cesare, Kevin Londerholm, Kale Simpson, Max Wicklund

May 2017

Table of Contents

Figures

Preface

The objective for the research project was to gather demographic information regarding Radio Frequency Identification Technology. Working in conjunction with Telaeris inc. and Marketing Professor Dr. Harry Watkins at Point Loma Nazarene University, the MBA team assembled a viable survey and gathered responses from our test audience.

The test audience for our research survey was the Telaeris Inc. company email list, as well as responses from social media promotion via LinkedIn. Additional survey responses were gathered through the Security Industry Administration contacts.

- Intended audience

The data is intended for the RFID industry and general public to receive and interpret to uncover the opinions and concerns toward the technology capabilities of the product.

- Why audience should read the plan.

This data is valuable for ensuring that new products and users of RFID technology are aware of the capabilities and receptive audience for its implementation for the use in public and the work environment.

- How participation in this project has served the needs of your team.

Responses from or target audience have given significant data to draw valuable information to answer research questions regarding perceptions of RFID technology.

Chapter One:
Executive Summary

This report details the results of a research study by PLNU's graduate MBA students on behalf of Telaeris Inc. The study sought to evaluate how key stakeholders assess the balance between the privacy concerns and the perceived benefits of using applications of Radio Frequency Identification (RFID) technology.

The research method involved is a web-based survey, designed through Qualtrics, administered to an email list and LinkedIn network provided by Telaeris Inc. Approximately 140 responses were received and analysis was done using SPSS.

The primary limitations of the survey involve a small sample size limited to the Telaeris email list and LinkedIn network and limited draw from outside of the security industry.

Research analysis revealed that the largest concern amongst respondents is the concern of hackers being able to skim important data from RFID applications. As for the perceived benefits of RFID applications, responses were strongest towards the security, safety, and convenience RFID provides, while remaining neutral towards the perceived benefit of efficiency.

Chapter Two:
Introduction and Background

Radio Frequency Identification (RFID) is a wireless technology that is capable of actively or passively tracking products, parts and, significantly for the purposes of this study, people. RFID technology has enabled numerous applications such as employee ID's, public transit passes, passport ID's, etc. These applications potentially deliver many benefits including increased safety, efficiency, convenience, and effectiveness.

However, with the rise of RFID use in various industries to track people, concerns over privacy tracking have also emerged, with the potential of slowing the adoption of the technology for this purpose.

This study is focused on measuring the range and intensity of these concerns, assessing how the concerns are balanced in respondent's minds against the benefits of RFID technology, and assessing possible methods of allaying these concerns. The results will be useful for Telaeris, Inc. in its marketing and educational efforts, and will help our client, David Carta, further position himself as a thought leader in the industry.

.

Chapter Three:
Research Objectives, Methodology & Limitations

Research Objectives

The research objectives for this study were as followed:

- Assess stakeholder perceived benefits and concerns with respect to selected RFID people tracking applications.
- Measure respondent assessments of various methods of allaying concerns.
- Determine whether attitudes vary significantly by key demographics

Methodology

The methodology used for this project was a web-based survey sent out in a solicitation email to a set list provided by Telaeris Inc. In addition to being sent to the email list, the survey was also posted to LinkedIn to allow for participation by the followers of the Telaeris CEO (David Carta), and market research team member profiles. All data was processed and analyzed using SPSS.

The survey itself was powered by a platform called Qualtrics. This platform allowed for the housing, organization, and exportation of data to be further analyzed in SPSS. Qualtrics was used to formulate the survey, providing formatting for answers as well the ability for question "re-directs"-dictating the survey responders journey.

Our client contact for this project, was Telaeris CEO, David Carta

Limitations

The primary limitation of our research was that the timing of the dispersal of the survey with the broader SIA audience did not allow for enough time for data analysis. The reach of our survey was limited to the email lists and professional connections of both Telaeris Inc. and the PLNU Market Research team. The responses collected were quantitative in nature and greater nuance for some of our findings could be obtained by supplementing research with qualitative methods such as personal interviews or focus groups.

Chapter Four:
Demographics

This section details the demographic characteristics of our sample.

58% of the respondents work for a company providing RFID related products or services

Figure 1: Percent of Respondents who work in the Security Industry

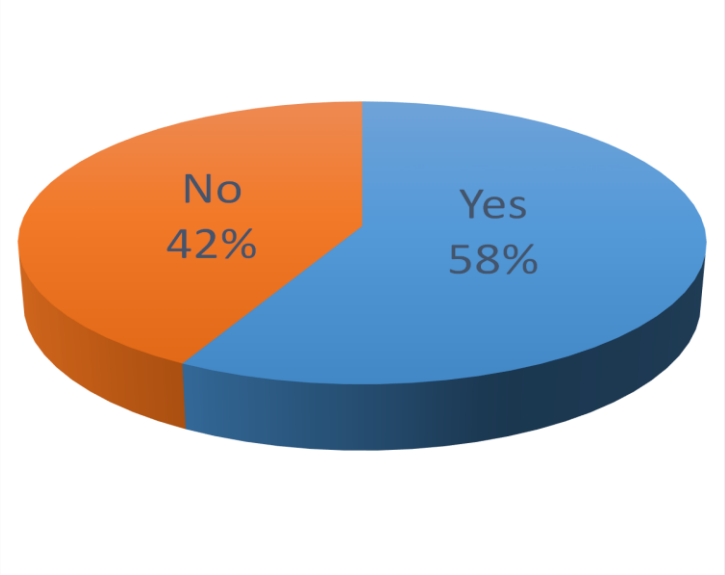


Figure 1 shows that the majority (58%) of respondents do work for a company that provides services or solutions that use RFID.

Figure 2: Industry of Respondents' Firms

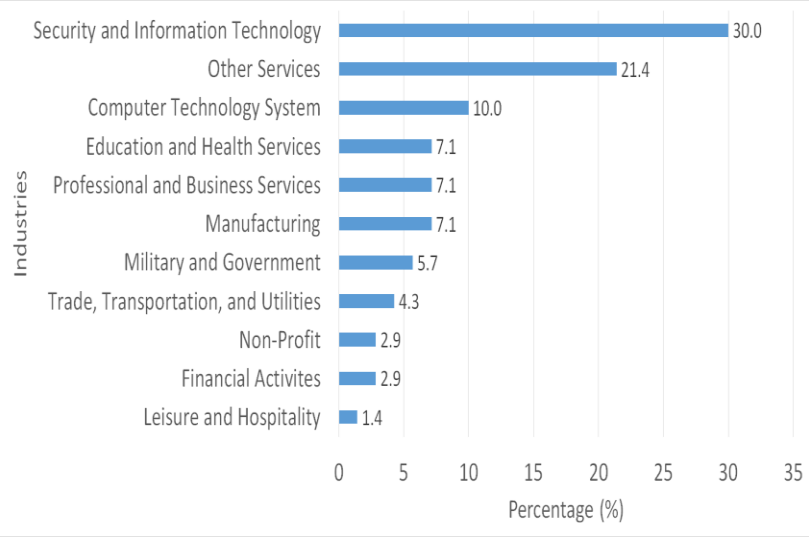


Figure 2 shows that approximately 30% of respondents work within the Security and Information Technology industry with Other Services (21.4%) and Computer Technology Systems (10.0%) rounding out the top three industries that respondents work in.

Figure 3: Size of Company or Organization

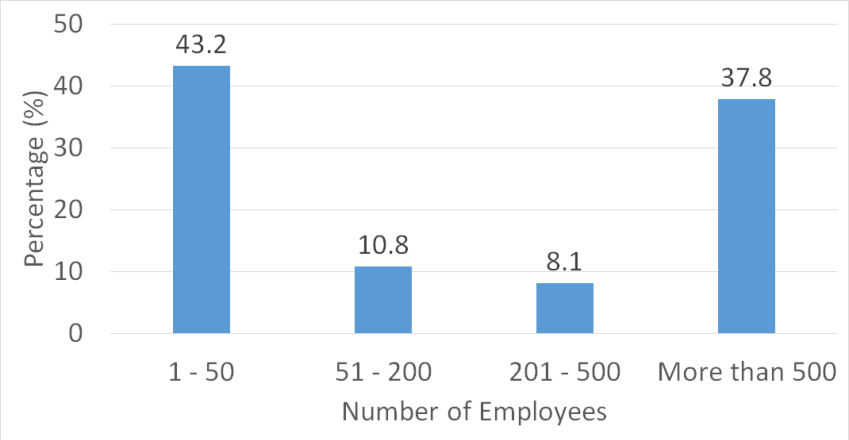
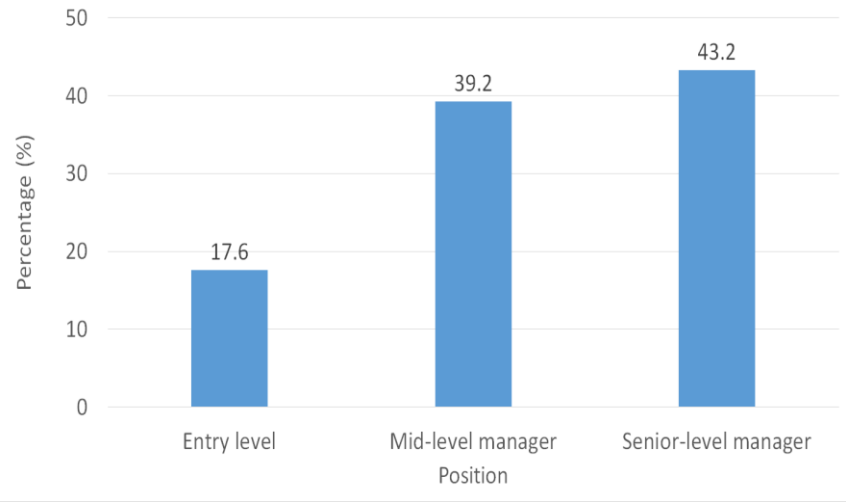


Figure 3 shows the size of the organizations that respondents work for. Over 80% of respondents work for either very small organizations (1-50 employees) or large organizations (500 + employees

Figure 4: Job Position of Respondents



Most respondents hold mid- or senior-level positions in either very small or very large organizations .

Figure 4 show that the large majority of respondents hold mid- or senior level positions within their firms, and are in the latter

portion of their working careers.

Figure 5: Age of Respondents

.

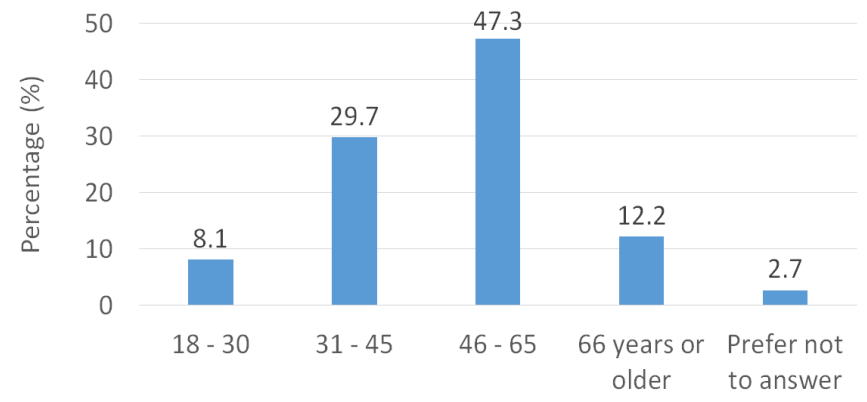


Figure 5 reveals that nearly half of respondents are within the age range of 46-65 with the bulk of respondents (77.0%) were between the ages of 31-65.

Figure 6: Level of Education of Respondents

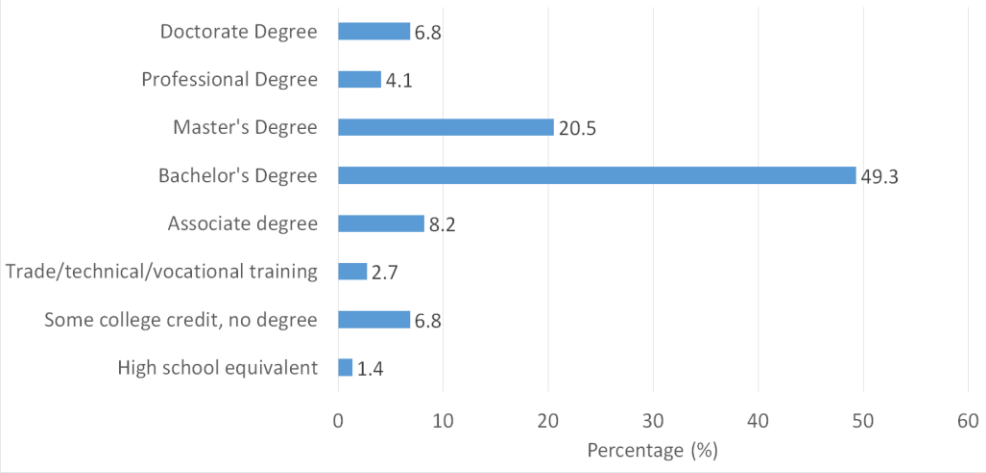


Figure 6 shows that close to half of the respondents hold at least a Bachelor's degree with and additional 31.4% holding degrees above or equivalent to a Bachelor's.

Figure 7: Ethnicity of Respondents

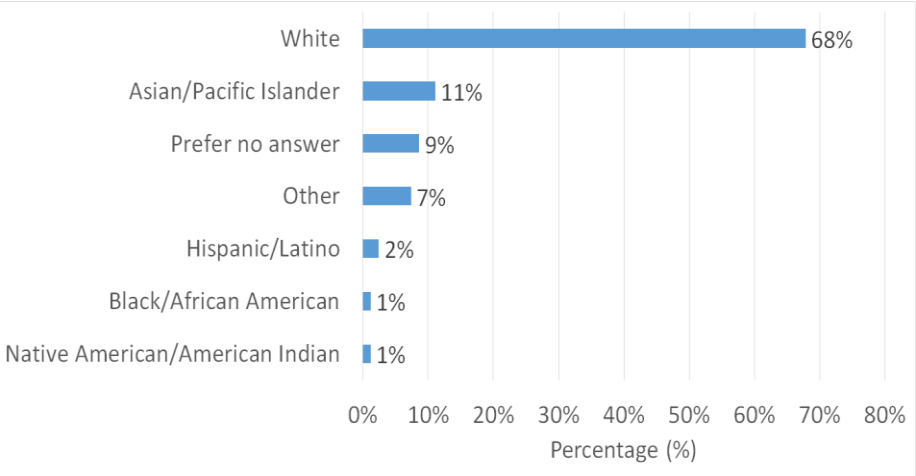


Figure 7 shows that the nearly 70% of the respondets identify themselves as Causcasian.

Figure 8: Children Under The Age of 18 at Home

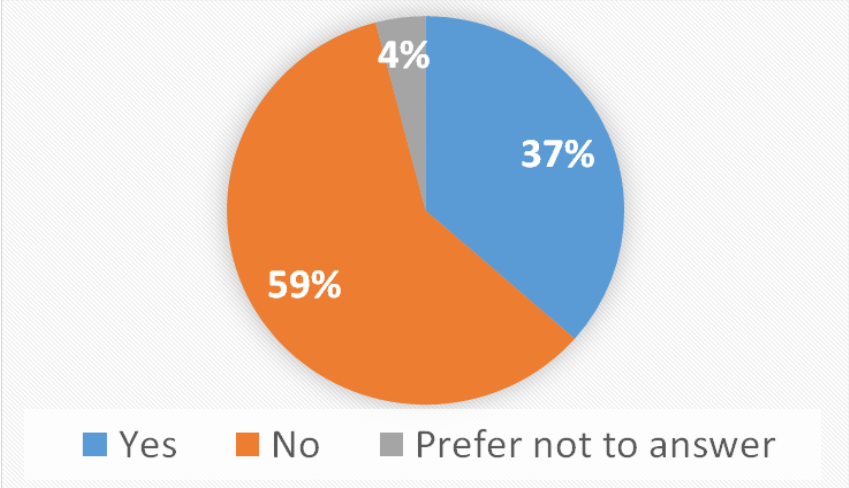
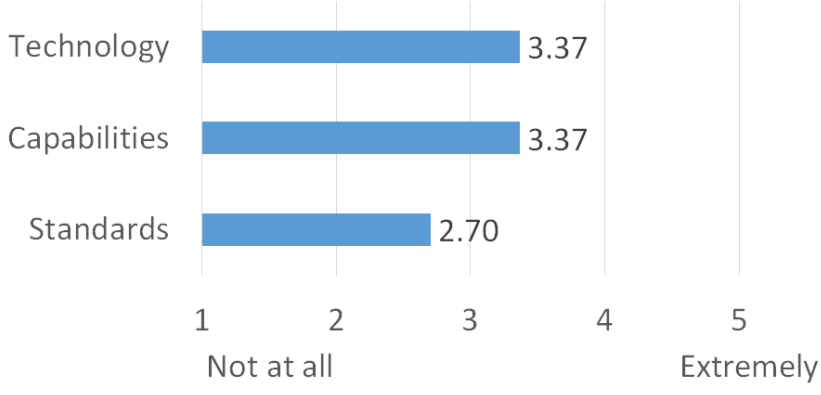


Figure 8 shows that the majority of respondents do not have children living at home (consistent with the age and career stage results).

Chapter Five
Research Findings

Knowledge of RFID:

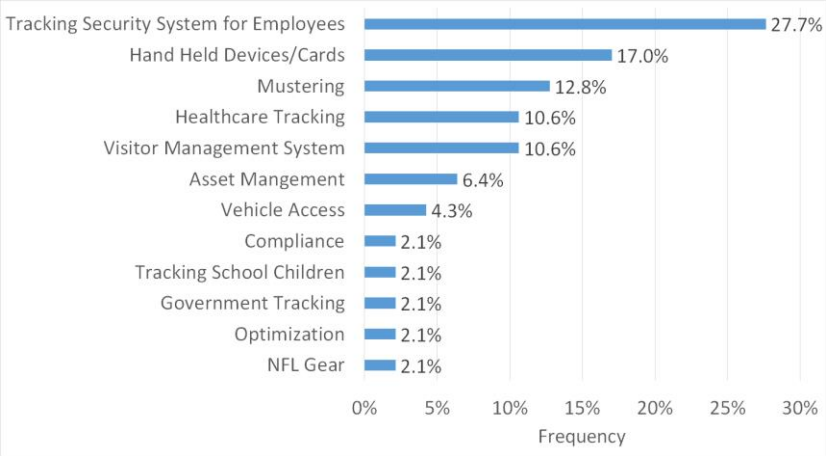
Figure 9: Average Knowledge of RFID



Respondents are least knowledgeable about RFID standards

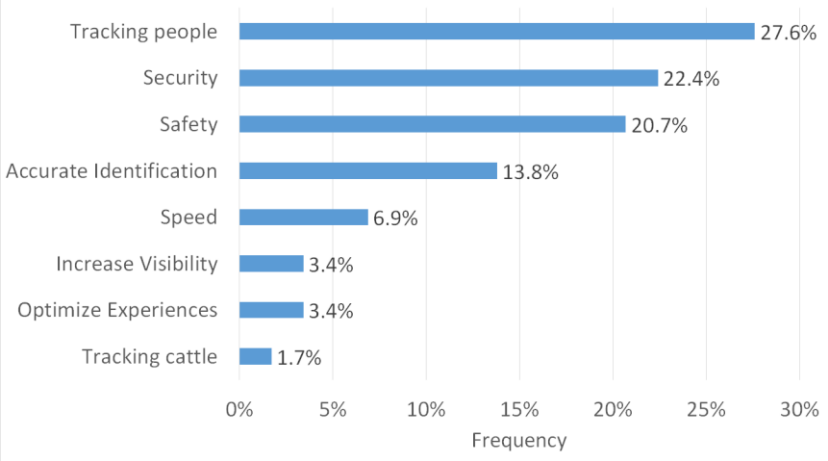
Respondents were asked to gauge their level of knowledge concerning different aspects of RFID on a scale from 1 - 5, 1 was not having any knowledge at all while 5 was having extremely high knowledge. Respondents had highest knowledge in regards to RFID technology and its capabilities with average scores of 3.37. Knowledge of RFID standards was much lower with an average of 2.70. Respondents were more knowledgeable on RFID technology and its capabilities than the standards.

Figure 10: Application of RFID (verbatims)



Respondents were asked to list any applications of RFID technology in which it is used to track people. The most common application listed, with 27.7% of responses, was a tracking security system for employees. The application with the second most awareness was RFID in handheld devices or cards with 17%. Mustering, Healthcare tracking, and visitor management rounded out the top 5 responses for the application of RFID. The sorted verbatim responses to this question appear in Appendix A.

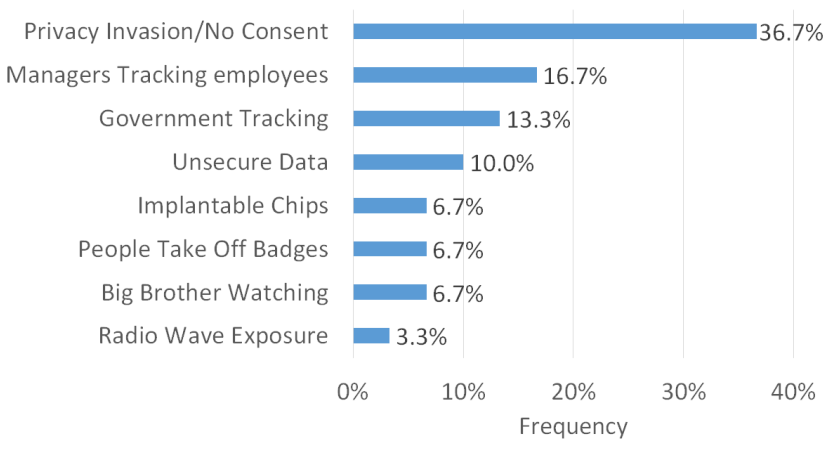
Figure 11: Benefits of RFID (verbatims)



Respondents were asked to list any benefits that the use of RFID technology provided. The most common benefits listed were the ability to track individuals and security benefits with 27.6% and 22.4% of the responses respectively. Safety, accurate

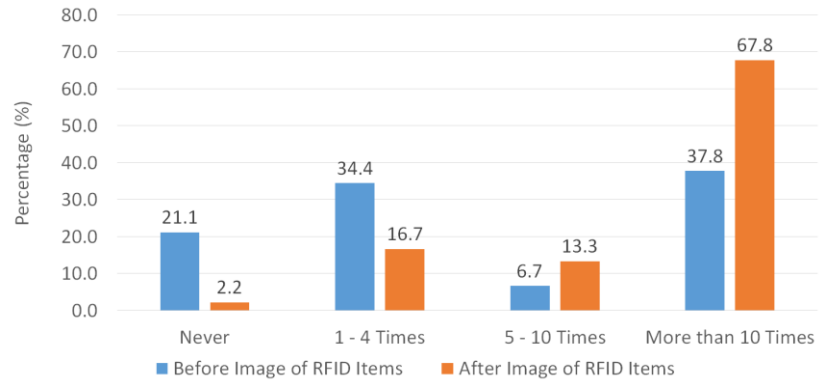
identification, and speed made up the rest of the top five benefits of using RFID technology listed by respondents. The sorted verbatim responses to this question appear in Appendix A.

Figure 12: Concerns of RFID (verbatims)



Respondents listed their concerns regarding the use of RFID technology to track people and the largest concern listed was that it invaded privacy without consent with 36.7% of responses. Respondents also showed concern for managers tracking their employees, the government tracking people, and having unsecure data with RFID. The respondents showed concern for privacy invasion and tracking of humans by employers or the government. The sorted verbatim responses to this question appear in Appendix A.

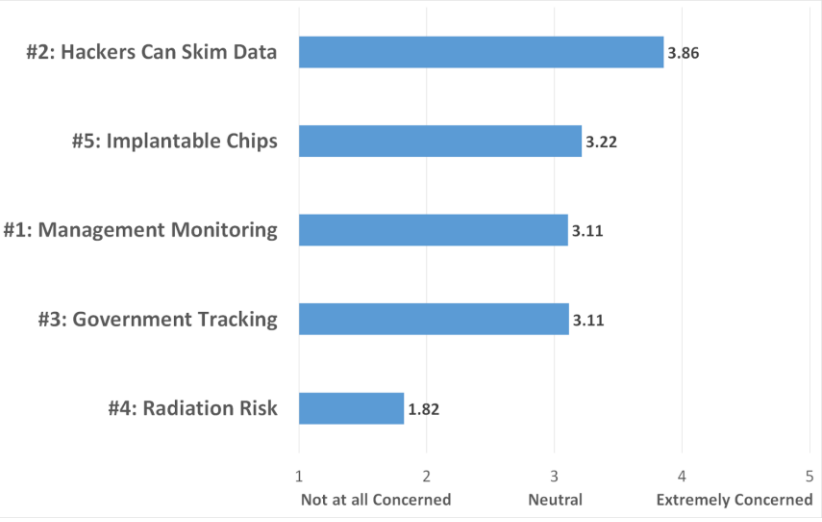
Figure 13: RFID Use in Last Month



Respondents were then asked to gauge their usage of RFID technology in the last month with ranges from never up to more than ten times. The respondents were asked this question twice with an educational piece in between the inquiries. The hypothesis being tested was that if respondents were shown an image of everyday items that have RFID technology, then the respondents would recognize that they make greater use of RFID-using devices than is commonly recognized. The above figure shows the usage rates increased greatly after being shown the image of everyday RFID-using items. The frequency for more than ten times per month before being shown the image was a mere 37.8% and after being shown the image, this jumped to 67.8% of respondents.

Importance of RFID Concerns:

Figure 14: Average Importance of RFID Concerns

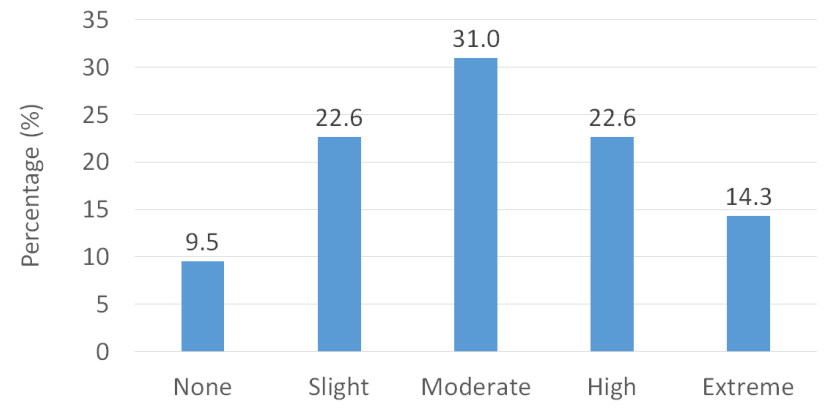


Respondents were asked to gauge the level of importance for five concerns associated with RFID on a scale of 1 - 5. The concern the respondents felt was most important was that hackers could skim individual's private data from RFID cards and tags with an average importance of 3.86. The concern with the second most importance was that implantable RFID chips could be used as universal identification for everything from security to payment with an average of 3.22. Tied for third place with an average of 3.11 was the concern that tracking people by RFID could be used by management to monitor where employees are and what they are doing and the concern that RFID is a tool that the government could use to track people. The concern with the least importance was the concern that RFID tags and readers could pose a radiation risk.

Hacking is the greatest concern, while Radiation exposure is least important.

Concern #1: Management Monitoring:

Figure 15: Concern Level for Management Monitoring



The concern level for management monitoring centered around a moderate level with 31% of respondents feeling this way. 22.6% respondents felt highly concerned about this issue and 14.3% were extremely concerned for management monitoring their employees. 9.5% of respondents felt no concern.

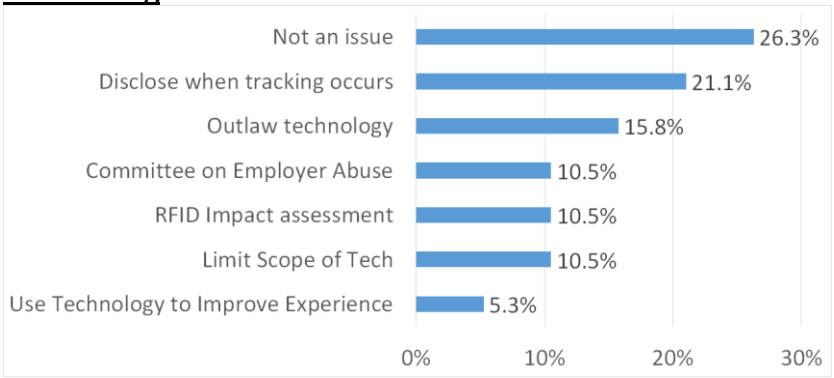
When the level of importance for this concern was tested for significant difference between demographic groups, there was no significant difference found between groups.

Figure 16: Effective Ways to Address Management Monitoring

RANK	RESPONSE	MEAN RANK
1	Educational Resources	2.29
2	Case Histories	2.37
3	Employee Opt-Out Option	2.81
4	Company Policies	3.16
5	Other	4.37

Respondents were asked to rank the effective ways to address this concerns regarding management monitoring and educational resources ranked the highest. Case histories were second, employee opt-out was third, company policies were fourth, and other options were fifth.

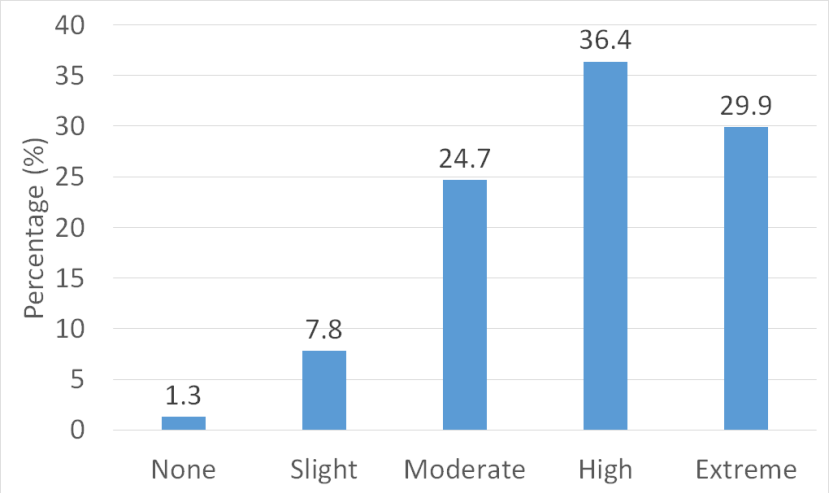
Figure 17: Other Effective Ways to Address Management Monitoring



Respondents were given the option to write other effective ways to address management monitoring and the most common way to address the issue was that it was not an issue. The option with the second highest frequency was to disclose when the tracking occurs.

Concern #2 Hackers Skimming Data:

Figure 18: Concern Level for Hackers Skimming Data



The concern level for hackers skimming data from RFID technology was highest among respondents at a high concern level at 36.4%. There was a significant difference in level of concern between demographics when broken up into industry of work, number of employees in the organization, age, and education level. Concern about hacking varied significantly by RFID engagement (industry insiders less concerned), and position in the firm (mid-level managers most concerned). Respondents from smaller firms seem less concerned about this issue than respondents from larger firms, and younger respondents (18-30) were less concerned than older respondents (46-65).

Figure 19: Effective Way to Address Hackers Skimming Data: Average Rank

RANK	RESPONSE	MEAN Rank
1	Educational Resources	1.99
2	Case Histories	2.70
3	Employee Opt-Out Option	2.70
4	Company Policies	3.09
5	Other	4.54

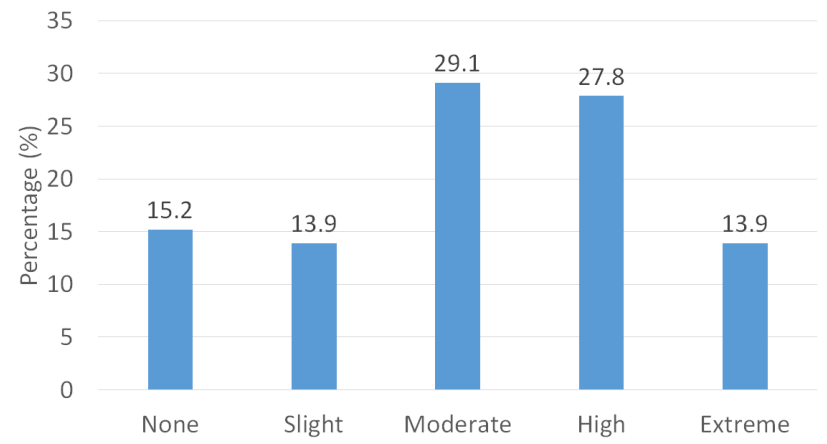
The most effective way respondents thought the issue of hackers skimming data could be addressed was through educational resources. They then ranked case histories and employee opt-out as a tie for second most effective ways. Company policies was in third place followed by other ways wrapping up the effective solutions.

Some other effective solutions that respondents thought would address this issue (from verbatim comments) are listed below:

- The industry needs to support the equivalent of CERT to fix issues
- Do not put private data on the card
- Show the data up front so they are informed & not speculating
- Provide two factor authentication required to read the tags.

Concern #3 Government Tracking:

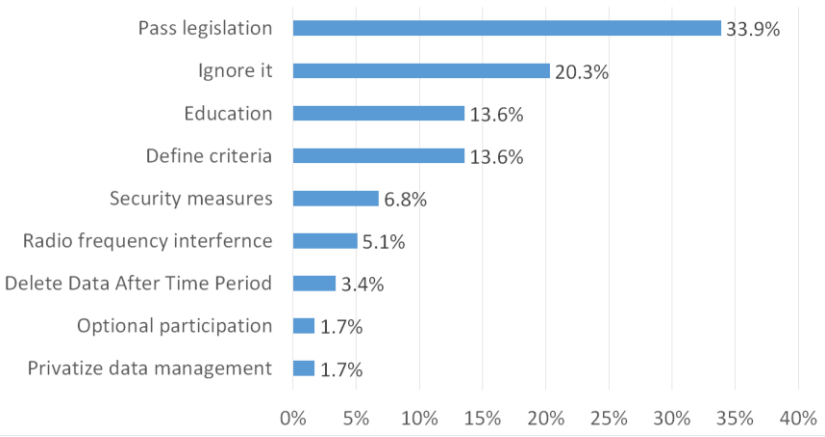
Figure 20: Concern Levels of Government Tracking



The respondents showed they were moderately to highly concerned with the issue of RFID being used as a tool that the government could use to track people. There were 13.9% of respondents that rated this concern as extremely important and 15.2% that stated this concern had no importance.

There are significant differences in average levels of concern towards the government using RFID to track people when grouped into age demographic. The group of respondents aged 18-30 are less concerned than the groups aged 31-45 and 46-65 years old about the government tracking people.

Figure 21: Effective Ways to Address Government Tracking

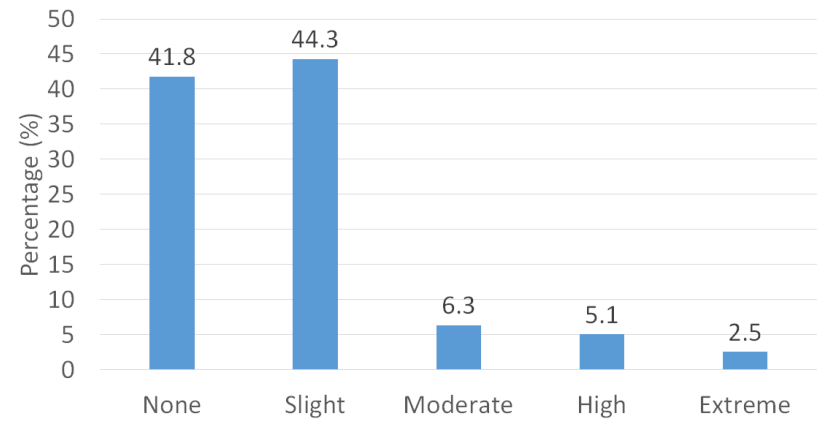


Respondents were asked to offer their verbatim ideas as to the most effective way a government organization could reduce this concern and passing legislation was the most common response.

The second most common response was to ignore it and the next two options were education and by defining the criteria of surveillance. Appendix A shows the detailed verbatim comments for this question.

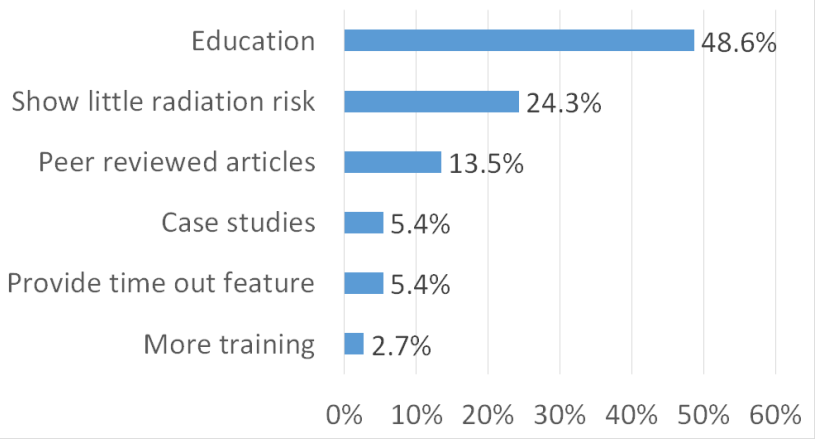
Concern #4 Radiation Risk:

Figure 22: Concern Levels of Radiation Risk



The Mean level of concern for this issue was 1.81 and was the lowest concern overall. The concern levels did vary by sub-groups. The levels of concern were significantly lower if the respondent was involved in RFID, was Caucasian, from a large company, or if they were more educated.

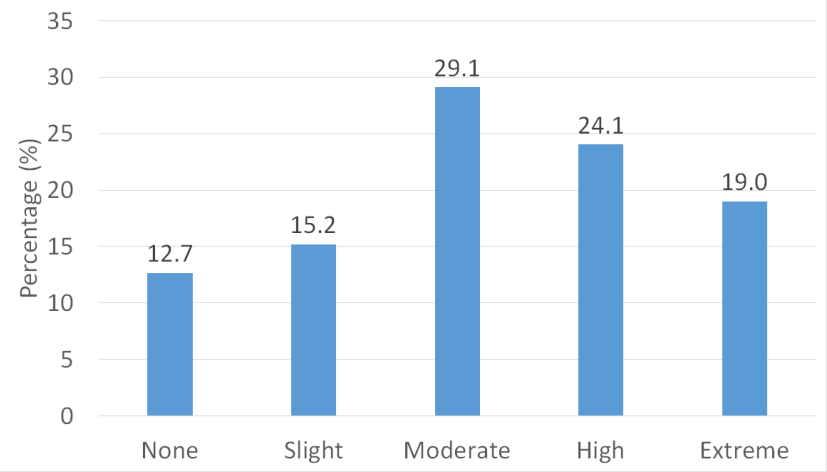
Figure 23: Ways to Address Radiation Risk



Education was the most effective way to address this concern. Proving there was little radiation risk was the second most effective way listed in the open ended response section.

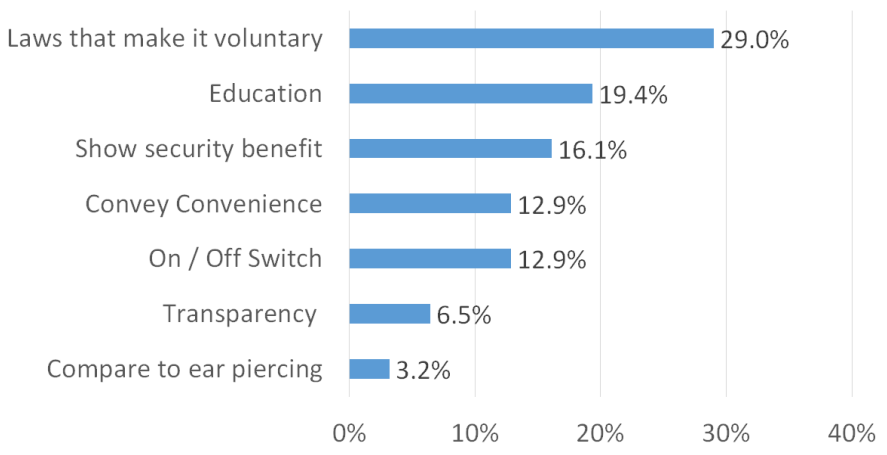
Concern #5 Implantable RFID Chips:

Figure 24: Concern Levels of Implantable RFID Chips



The Mean level of concern for implantable chips was 3.26 showing an overall moderate to high level of concern. Independent sample t-tests showed non-caucasians are significantly more concerned than caucasians about this issue.

Figure 25: Effective Solutions for Implant Concerns



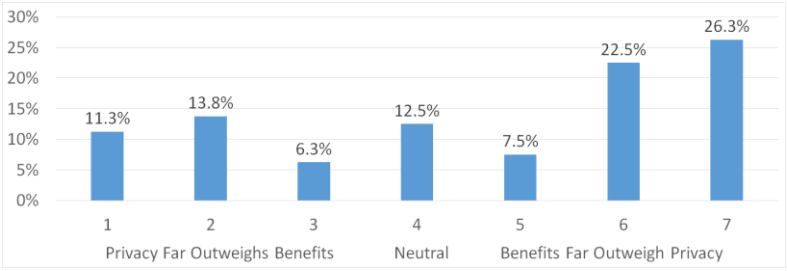
Forming laws to regulate would be the most effective solution for the concern of implantable RFID chips.

Case Studies

Respondents were offered two case studies of possible deployments of RFID people tracking applications to evaluate. The description of each case and how respondents responded to them is below.

Case Study #1 Student Tracking: A School issued student ID cards with RFID chips. Allowed administration to: Track attendance, Improve safety, Provide parent oversight.

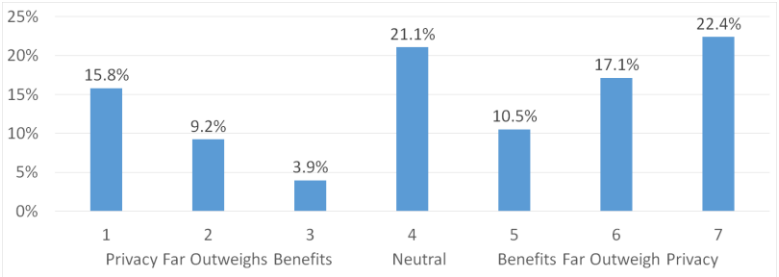
Figure 26: Privacy Concerns Vs. Benefits: Student Tracking



The mean score was 4.64 showing an overall assessment of a slight benefit for tracking school children. 71% thought parents would support the tracking. Non-caucasians were significantly more concerned about theprivacy issues than Caucasians.

Case Study # 2 Oil Platform Employee Tracking: A large number of contractors working on a construction job were provded RFID tags to: Track attendance, Improve individual and group safety.

Figure 27: Privacy Concerns Vs. Benefits: Emp. Tracking



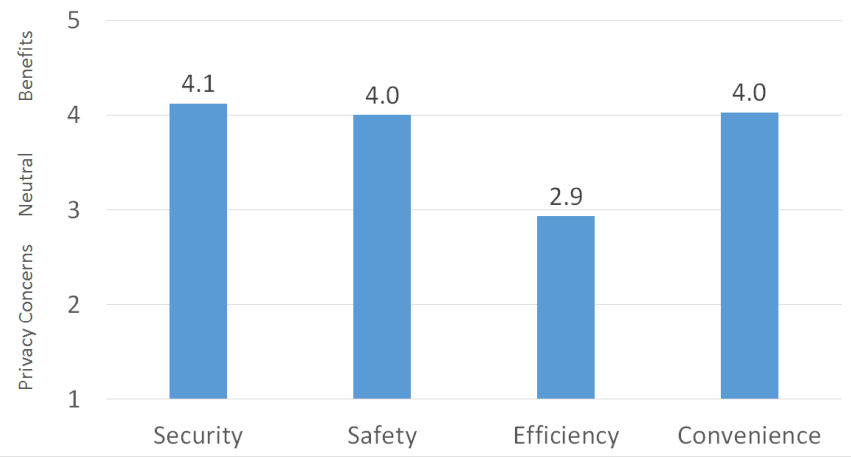
The mean score was 4.42 showing a slight benefit compared to a concern. Non-caucasians were more concerned and respondents in small firms were more positive about benefits. 54% of respondents did not support employee tracking.

Privacy Concerns Vs. Benefits:

Respondents were asked to balance various benefits of RFID - security, safety, efficiency and convenience, with their concerns for privacy. The benefits were described as follows:

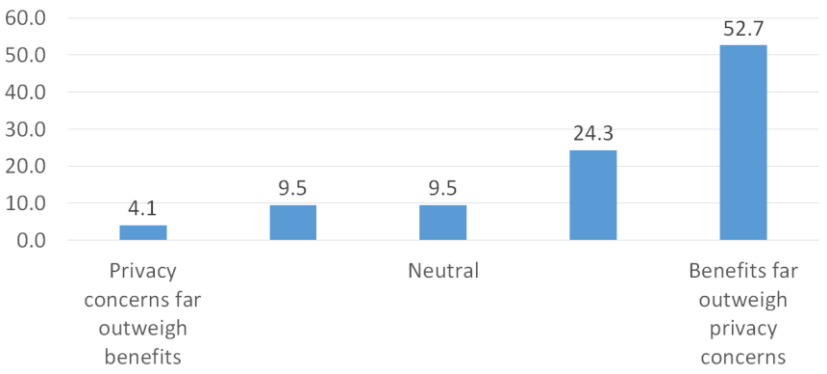
- **Security:** RFID trackers can prohibit unwanted guests from obtaining access to restricted areas.
- **Safety:** Employees can be accounted for quickly in an emergency situation using RFID..
- **Efficiency:** Employees can locate coworkers quickly using real time RFID location tracking and avoid wasting time.
- **Convenience:** RFID tags can be placed in a vehicle to allow access to toll roads, communities and parking without having to stop

Figure 28: Privacy Concerns Vs. Selected RFID Benefits



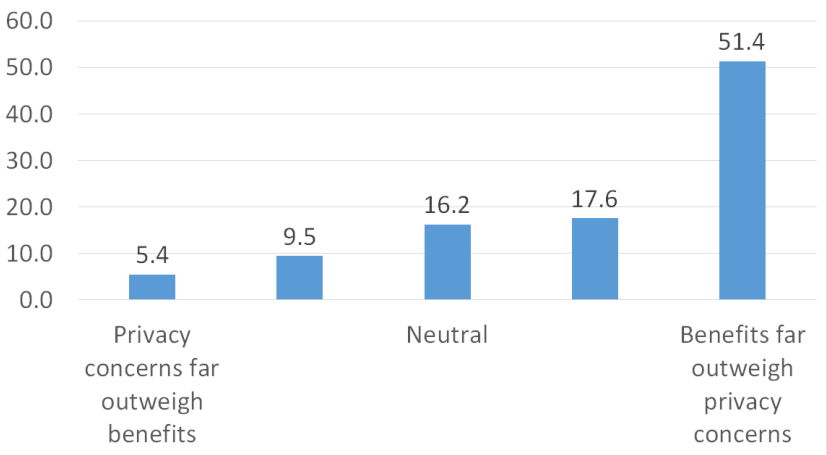
Respondents generally felt that the security, safety and convenience benefits outweighed their respective privacy concerns, but were more ambivalent about the efficiency benefit as stated. The following four figures show the frequency distributions for each of these benefit/concern tradeoffs.

Figure 29: Privacy Concerns Vs. Security



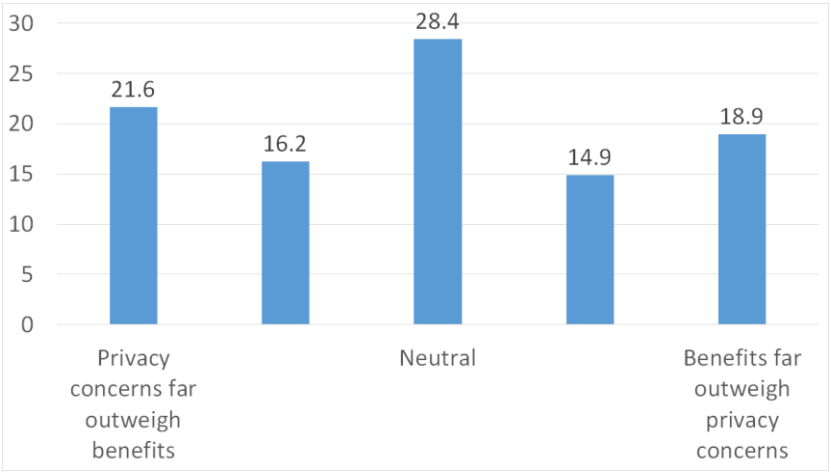
Majority of respondents felt the security application had far greater benefit than concern for privacy.

Figure 30: Privacy Concerns Vs. Safety



Majority of the respondents felt the safety application of RFID had far greater benefit than concern for privacy.

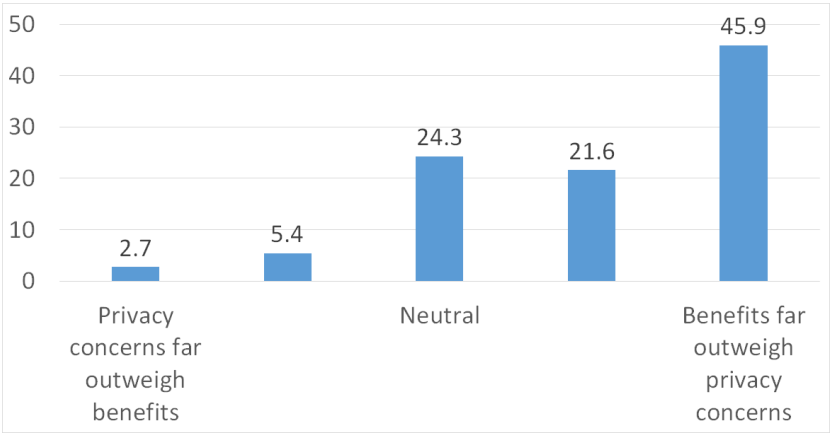
Figure 31: Privacy Concerns Vs. Efficiency Benefits



Respondents were mainly neutral towards the Efficiency benefits of RFID technology. This application of RFID was the lowest rated on the scale of concern to benefit.

Respondents seemed most ambivalent about the Efficiency vs. Privacy tradeoff.

Figure 32: Privacy Concerns Vs. Convenience Benefits



Majority of respondents felt the convenience benefits far outweighed the privacy concerns of this application of RFID technology.

Chapter Six
Conclusions and Recommendations

In conclusion, we find that there are varying perceptions of the privacy concerns and benefits of RFID use based on demographic grouping of respondents. Analyzing further, hackers skimming data is the largest concern of respondents and must be addressed by security solutions companies. However, this is less of an issue for respondents who come from the industry, are younger, are from smaller companies, or have less education. It's the older generation that are more concerned with hacker skimming and government tracking than the younger generation. We can also determine that radiation risks are not a significant concern for this sample. When analyzing what intervention respondents find best for addressing RFID concerns-education, case histories, and employee opt out options ranked highest. Looking at demographics, non-caucasians are significantly more concerned about both student and the employee-tracking application cases than caucasians. Also, we found that respondents are generally strongly positive towards the security, safety, and convenience benefits of RFID but are more neutral about the efficiency benefit.

Regarding recommendations, firstly, this survey must reach more end users to gauge perceptions of people tracking technology outside of the security industry with greater significance. We were limited by the number of respondents, as well as the sample frame from which respondents were drawn, i.e. contacts and social media followers of Telaeris. We recommend that Telaeris peruse other sample frames such as the Security Industry Association, and other non-security related associations. Using this survey template, we suggest continuing the collection of responses so as to "increase the power of the test" of differences among demographics concerning RFID benefits and concerns. In particular, the attitudinal differences we uncovered based on ethnicity should be explored further.

In conclusion, the PLNU BUS 625 Marketing Research Class and Dr. Harry Watkins deeply appreciate the support of those who were solicited and completed this survey. We believe this information provides valuable information on how Telaeris can best serve and educate moving forward. Our results should

help aid in the future endeavors of Telaris Inc. and provided us invaluable experience in helping us to hone our craft.

Thank You!

Appendix A – Verbatims Questions 3 - 5

Question 3: Please list any applications you are aware of which use RFID technology to track people.

Used with Security System for Security Live tracking of employees through facilities Cell phones used to track children by parents

Access control systems, event performance monitoring (e.g., marathons), location monitoring for safety/security purposes

Express Entry from TELAERIS Q-People from QUDRA TECH

Visitor Management System

Most RFID tags that have a unique chip id, or an encoded unique item identifier have this potential, whether this is the purpose of the application or not. I say this as Project Editor of the European standard EN 16571, which specifies a procedure for a pivacy impact assessment. Specific tracking applications include RFID in: theme parks, neo-natal units, and some nursing homes. The other obvious one i any form of access control that requires continual monitoring.

Emergency Evacuation and Personnel Muster Accountability Visitor

Location Monitoring Employee Time and Attendance Facility Safety

Access Control Museums Guard Services

Vehicle access. User badging for access control. Tracking children in hospitals. There are LOTS and lots.

Almost every access control system XPressEntry Aeroscout NFL shoulder pads

Health Care, Hazardous Environments, Mustering, Time and Attendance, Traffic Patterns, Man Power utilization, Safety, Compliance Tracking, Many more.

Wireless locks

Point of sale, access control, healthcare, assest management and wayfinding systems,

Indoor positioning Indoor navigation building optimization workforce optimization

We use RFID as access control. Also if an investigation is conducted we use RFID to assist in the investigation.

EmergenZ Evac from www.offsitevision.com

EZ Pass toll system

Access control readers.

Prison Security Guard application and staff tracking in Healthcare

Ultra wide band to triangulate position. Prox and contactless Access control to track use at RFID readers. UHF tags to track people and assets.

Passports, driver license, credit cards, toll roads, access control,

GAO

Cameras

None that are active other than having an ID card with RFID and long range reader might be used.

OSVH EmergenZ Evac

access control, time and attendance

Target's Cartwheel Application (and in store tracking of Cartwheel App users) American Airlines Baggage Tags Walmart RFID Product Tracking

ID Badges, security anklets for felons, cell phones

EMV payment cards, access control cards, recently read an article where a Scandinavian company is implanting RFID devices into employee hands for access control.

Building access cards.

Question 4: Please list any benefits that tracking people using RFID technology might provide.

Better security Better safety Improved speed of access
It works, passively

Company security for data and staff security Tracking locations of agents

1-Secure Facilities 2-Managing people access to Areas and monitoring them. 3-Elimintate any threatening possibilities

Where the tracking is time and space limited, e.g. a theme park. It can help track lost children and optimise the experience by reducing wasted time. In nursing homes for the elderly with memory problems, it can be used to trigger alarms near exit points.

Safety Revenue enhancement Accurate Access Control Facility Security

Passive scanning is more convenient and accurate than a person checking credentials.

Increase safety Automate time keeping Better process visibility

Visibility and validation.

Events of who has entered should something go missing

If tied to physical and intellectural property, can be very affective in protecting that property or performing forensics in the event of an incident concerning that property. Very useful in physical access control to areas or secure spaces. Also useful fr logical access control to workstations and enterprise networks, also providing protection for intellectual property.

workforce optimization building optimization with HVAC and lighting
mustering, active shooter prevention

In using this ability we have been able to provide video of its usage and thus identify suspects. Travel patterns are also looked at.

Live accountability mustering and time and attendance.

Speed -- just bring the card or tag into the reader's RF field.

Robust and safe identification (using desfire)

Safety as well as integration to other system like Nurse Call

Business intelligence to determine contamination based on having been in area. Safety evacuation knowing exactly where someone is. Brick and mortar retail experience For traffic in stadium and airport Security, convenience, efficiency

Track their whereabouts in a secure facility, use these as alarm point counting

EMERGENCY

In places where people work alone and might be in a large facility after hours emergency response could benefit. In a way finding system that is active and individuals need to know where they are by GPS or electronic mapping at kioskes. Finding lost patents who don't know how to help themselves. Keeping babies in hospitals from being removed or moved away from an approved area without the mother. vehicular traffic could be tracked if vehicles had HID. Train cars are counted and managed with RFID. I beieve cattle are tagged with RFID to keep track of production.

Life Safety

access control, payroll, employee tracking

You can study customer behaviour and asset customers with the data. Knowing where people are in an emergency. Knowing how to treat people that are hurt. Being able to track people who disagree with you politically so that you can make them politically unimportant. Being able to track people and what they buy and look a so you can direct market to them in stores. 'Benefit' is in the eye of the beholder.

Authentication that the person or at least their card was present.

Quick authentication. If implemented properly can be secure

Automated time-card generation,

Question 5: Please list any concerns regarding the use of RFID technology to track people.

Yes - people are concerned about implantable RFID chips There is a concern about governments tracking people and managers tracking employees

Over active security can be a concern for employees.

The main concerns from the work that we did to develop EN 16571: * the complete lack of understanding by operators of RFID technology for applications like access control. Often the last secure technology is chosen. * the lack of transparency by vendors f known vulnerabilities that enable tracking and therefor the appropriate use of counter measures * Sometimes the regulations can be crazy. I know of a case in the Netherlands where prisoners had to give permission for the use of RFID, but the same systes integrator could install the system in a meat processing factory with no requirement for employees to consent. * The issue of the need for consent is still generally ignored We've definitely prioritized ease of use over security. Most credentials can be freely read and spoofed by anyone with some knowledge.

One might say... Big brother is always watching But im not that one Until i just wrote it now

Employers and agency can track people's whereabouts. The tollway systems can now track when and where you are along with your rate of speed. Firms that perform data mining can obtain pssession of this information for insurance companies and sales agencies

privacy concerns

privacy concerns

If they don't comply with carrying a badge, lanyard or bracelet you will not track them properly. That is why our software allows for reconciliation by visual confirmation and entry at any mustering location.

Need for cooperation of the cardholders -- they must present the card or tag to the reader.

Privacy invasion.

Exposure to radio waves even if considered safe by government standards. No way to turn off based on needed privacy. Unique credential for each application.

I am concerned that records may be used as circumstantial evidence but perceived as more valid because they are 'digital'

Privacy

This system is not well accept by Union

I think there is an inherent problem when too much outside oversight of individual activity is recorded or followed in any way. It is the ultimate in Big Brother watching that takes away a freedom we have come to expect. I fear that with cell phones we lready are giving up our freedom of someone tracking us. When it comes to putting anything permanently in or on our bodies to track us or our finances or any other personal or otherwise private information I am completely apposed.

Opt In/Opt Out- I am not sure that places like Target provides me the end user of the application with an opportunity to be adequately informed about the data collection that occurs, how they use that data, and how they store that data (in aggregate or i discrete files about me). Being able to track people who disagree with you politically so that you can make them politically unimportant. Being able to track people and what they buy and look at so you can direct market to them in stores.

Others can access personal information without your knowledge or permission.

Violation of the individual's privacy rights.

Appendix B – Verbatims Question 8 - 12

Question 8: Tracking people by RFID could be used by management to monitor where employees are and what they are doing. Other effective ways for this concern to be addressed:

If you are doing what you should be doing, what's the issue

The above concern is too restricted. Many employess worry about the tracking of access control systems, rather than the ID technology.

Undertake an RFID privacy impact assessment and declare the summary to stakeholders

Tracking is only available where there is infrastructure. Most companies that require some RFID badging can require you to sign off on knowing where you're located for the sake of safety and security. I truly consider this a non-issue. Employees don't hav to wear their badges outside of their offices if they feel uncomfortable!

Provide options and policies for employee to monitor actually what the employee is monitoring.

Use technology to make the building occupant experience more delightful

If I am paying you to work I as an employes have a right to know where you are.

Set up employee committee to monitor use of the data, for publication to the people.

Outlaw RFID for tracking people.

Educate that an employer has certain rights while employee is on site. not interested in following employees

Hire people who don't follow the "get paid to take a shit" work life. (spend all day on the toilet, daily)

Only use it for In/Out of the building

Hide it

Provide a clear policy on what happens to the data after collection (aggegrate/discrete) and how long the data is kept

Determine ROI on RFID

Be up front with employees & show the report

Don't use the technology. Trust your employees.

ID information is in a closed loop system that does not share data

Question 9: Hacker could skim individual's private data from RFID cards and tags. Other effective ways suppliers could address this data privacy concern:

Because RFID is hardware based, any inherent vulnerabilities remain in the protocol. The industry needs to support the equivalent of CERT to fix issues

make building occupant experience more delightful

Outlaw the use

Do not put private data on the card

Don't use it

Show the data up front so they are informed & not speculating

Provide two factor authentication required to read the tags.

Question 10: RFID is a tool that the government could use to track people. What ways could a government organization reduce this concern?

Pass appropriate legislation

Implementing security measures

1-Radio frequency interference 2-Hacking RFID chip informations 3-Cost of RFID tags

I believe they are probably already monitoring the public via RFID technology

Provide an RF shield for the tracking device.

Require a search warrant before using it.

Set criteria for which tracking is allowed, similar to criteria used for tapping phones etc.

Define exactly how and when this information can be monitored and/or collected. Provide legal protection for individuals consistent with existing privacy laws. (Not counting the Patriot Act, as I think that is a violation of reasonable expectation of prvacy).

If you aren't doing anything wrong no harm if you are it's cheaper than around the clock surveillance
Education

RFID (used in ACS applications) tends to be short-range and so ID is only vulnerable within a short range of a reader. Most systems today are not centrally networked - including government ACS systems, although US has a desire to network all government AC systems. Although the interchange of ACS info can be restricted those who have tracking concerns are unlikely to trust governments not to abuse it, especially as security services want the abilities to reduce terrorist threats - which is over-stressed ontheir part in my opinion.

I assume the question is about covert monitoring of any RFID application rather than of a government implementation. The effort to monitor, say a library RFID system, to see what books are read is high compared to accessing the library's database. If we re talking about implementations such as drivers licences, vehicle tracking which is beginning to take off etc, then the government needs to be more transparent about the objectives and the length of time that data is retained.

Not sure. People don't trust the government.

Establish and enforce policies against this practice.

Government organizations don't have the resources or desire to track people using RFID. That's just silly blathering nonsense.
Invest in education

They need to stay out of it.

They can put policies in place to prevent the use of tracking people.

Optional participation.

Make it a criminal offense for anyone in government to use privately assigned RFID technology to track people.

They can't reduce this concern unless they stopped installing RFID tags in ID cards.

Limited access and ethics. Strict punishment for misuse. This tool is extremely useful for law enforcement

Your mobile phone is used more then rfid. Like the car passes such as E-Zpass, you can put them in rf shielded bags and not be tracked.

Education of the application

Pass laws and establish Executive branch policies against such practices.

We are overt about our desire to track people and vehicles, we are exploring using the technology to track vehicle progress through our facility. If you are up front and don't hide the use of the technology for this purpose I think people will be less cocerned.

Make the use of tracking technology a felony punishable by revocation of corporate charter.

In today's climate, impossible

Laws, policy against tracking individuals. FOIA disclosures. Opt out options (RFID blockers). Option to change credentials at will. Option for pseudonymous registration

Be fully open and honest with how any information is being used.

Public records of how often this data is subpoenas

You cannot track people everywhere they go without a massive infrastructure built to support full time tracking all across the country or world

let them know it is site specific

Implement practices where location information is deleted after entry verification occurs going into buildings. For example, you might check that individuals entering a government building are not on a watch list, but those who pass the scan have their etry/exit information deleted after a certain length of time. You can also educate the public about what RFID technology they control and what they don't (do they even have access to credit card RFID chips).

Have a specific policy in place.

Face & bio-metrics or dna is a bigger risk

Tell people they are not doing that and if it is determined ANY section of government is that they are prosecuted and held accountable

Can't in my opinion. This should not be done.

Education on the capabilities of RFID

Legislatively by passing laws limiting its use. By issuing rules limiting its use By giving state and federal courts broad jurisdiction over the use of "RFID evidential rules".

limit the use of rfid to mission critical situations

Demonstrating how the data is collected, used, and stored.

Demonstrate an understanding of public concerns. Offer a clear and defined path to have the data collected erased. Demonstrate a clear and defined path to show how erroneous, or incorrec, data can be corrected.

If they have areas in facility that have classified documents / or any type of physical devices.

Show how it helped prevent a major issue. Show where people have been stopped. Show what is tracked and what matters.

Make sure the EVERYBODY from the President on down is tracked with the same technology. Or just not use it.

Unfortunately once the government or any other body has your information it is impossible to control completely. The government was even able to hack the Apple security when it wanted.

Assure privacy rights are maintained, databases are limited access. privatize management of these transactions

Question 11: RFID tags and readers could pose a radiation risk. WHat other ways could an organization that deploys RFID technology reduce this concern?

Provide a programmable "time-out" feature.

Some people think Wifi routers are dangerous too. Might want to show how strength of RFID radiation compares to any number of other things, like cell phones and the sun.

Education

Education

Use graphs showing the amount of radiation from RFID vs other everyday objects.

I'll sell you some tinfoil hats while we're at it.

Rfid seminars. Teach them about the tech being used

education

Over Hyped to the extreme, if people just understood how much RF was all ready in the air the would be scared to death.

By educating it's users

Radiation awareness trainng

Provide peer reviewed medical journal articles to concerned employees to alleviate their fears regarding exposure to radiation related to RFID technology.

Independent studies and certifications from FCC and other reputable organizations.

education

Long term case studies

MSDS sheets and comparisons to other technology. Mobile phones emit much higher levels of energy for operation.

Education on radiation facts rather than myths

Provide educational materials

Distribute unemotional study results to the people, comparing radiation levels for the frequency of the RFID equipment with other common RF applications.

Not use it to track people.

EDUCATION IS KEY

Identify RFID hot spots - signal strength drops off with distance from reader. Provide education regarding human body reaction to RFID frequency radiation.

Did you know that bananas contain approximately 45 micrograms of radioactive potassium? That being said, check out this handy dandy chart by xkcd in regards to the amount of radiation we could potentially be exposed to over a given period of time. https:/xkcd.com/radiation/

Backup with scientific data.

Honestly, not much. Educating individuals

Explain what materials block the emissions and how far they radiate.

Education of the risks to consumers.

More studies

Limit where the readers are located.

Don't use it

Education, and ways to protect agains any type of radiation.

Show the concerning device compared to other normal things in daily life. Educate properly

Educate people.

Unless there is scientific indisputable proof there will always be opinions one way or the other.

Education, availability of low cost RF radiation monitors, testimonials.

education

Question 12: Implantable RFID chips could be used as universal identification for everything from security to payment.

Matrix, here we come

Hacking RFID chip information

Provide a programmable "on-off" feature.

Don't do it.

Wrong question to ask me, I've been waiting for this for years. Please let me wave my arm at the grocery checkout to pay my bill! Seriously though, alleviating concerns ... I think once people see how

convenient it is for the early adopter they will come round.

Not use this method of tracking

If it can provide a means of ID theft bring it on

Education

The question is badly put. I suspect the concern is 'if deployed could implantable RFID chips be abused for unintended/authorised purposes'. Unfortunately most users put too much trust in the installers/manufacturers, who often have back-doors (designed fr testing and to assist technical support) to the technology that can be abused. In my experience few adopters tend to worry about such concerns, although their employees might.

RFID is only justified to identify medical implants, where other options might require invasive medical procedures. The use of RFID with embedded sensors has some potential benefits.

don't know

Encourage laws that make implantable RFID chips totally voluntary.

Why is this a concern at all?

Enforce that they do not do that. Only the willing can implant chips in their body

education

Very effective use of the technology but get this past acceptance and religious views would be hard to do.

I don't believe they can

Non-participation

I doubt that there would be enough people out there who would consent to having an RFID chip implanted into them. I know I certainly would not!

This concern is valid and organizations should allow opt-out option. It currently is used on animals and military as a replacement of dog tags for special forces. As one authentication method combined with Iris, fingerprint, or Facial Recognition their id and assets would be more secure.

Convenience

Transparency about how they do use this technology.

This is an invasive technique that must be limited to voluntary use only (that is, to the individual's advantage).

NOT DO IT!

Read Revelations in the Bible.

RFID is often read only, but if compromised an implantable solution seems extreme. Make technology reprogramable but provide security against attack. On/off switch through bio mechanism.

don't know - not a techie.

Concern? My only real concern is that this becomes a thing. Yes, of course it will have to come with security protocols in place that would prevent thieves/hackers from "scanning dat ass" for your private/financial identity. Assuming those protocols wouldbe put in place, I think waving your hand over a 'reader' in a particular method would be a lot more efficient and safe than having a card that is legible and/or able to be physically stolen. I've had credit cards(wallets) stolen twice in the last 5 yeas. It was a miserable pain in the ass to get everything back to normal. The only way you'd be able to get that information from implanted RFID is by "scanning dat ass" (and getting past security protocols in place)...if you're going to try and physically teal the limb that contains the chip, I'm going to fight for it. If it were to get stolen I'd be dead anyway so not like I'd give a sh*t about it anymore.

Clearly state the pros and cons - make the person being implanted with RFID chip choose what he/she wants

RFID systems are secured system, even more secure then the numbers on your social security card

Compare it's effects to more common procedures such as ear piercing, tattoos, artificial hip or knee surgeries, etc. Also emphasize the person's control over the process, the chip after it's put in and the location/maintenance of it.

reassurance to user base of exact use of equipment.

Don't implant them in people

I should never have to have any technology or other item forced into my person especially if it could be used for tracking.

Don't use it

For use with animal identification, fine, but certainly not with humans.
don't do it

Best practices demonstrated.

This does create privacy issues. To be completely disconnected, you could just leave the devices somewhere. An implant is forced.

Not do it. This is a chip that could always track you that you couldn't opt out of. This is sort of like slavery.

closed loop systems that are not universal.

Make it optional.

Appendix C – Verbatims Cases 1 & 2

Case 1: How do you think parents would react to this plan? Would they support it? Why or why not?

Yes - better safety and knowledge of student's whereabouts.

It would be viewed favorably

We already working on such solutions for our dealers in Middle East.

Now a days, schools in ME really concerned about this solution and also parents are looking for this solution to be deployed.

SUPPORT. FIND THOSE DAMN KIDS

Personally, I think this is a "great" idea, but I don't have any children. I think you might get a 50% parental support. The other non-supporting 50% would be concerned about "BIG GOVERNMENT WATCHING US" syndrome.

I think parents would support it.

Not sure. As a new parent, part of me likes the comfort this would provide. I could understand how other people might consider this overkill or related to the "nanny state." There is also the fear that a hacker could locate specific children for kid nappig or worse. Possibly favorable, if the emphasis was on increased student safety. If a parent disagrees either home school or find a private school As a parent of an elementary school student and a middle school student, I'd support it.

A variation of this was addressed in UK a little while ago, where biometrics was intended to be used. The Home Office and ICO issued an advisory paper (PAS) on adopting biometrics, with a strong suggestion biometrics should only be used when it can be jusified - unlikely in such a situation. Items 1 & 2 are required under 'duty of care' requirements. Item 3 always seems a step too far - how do you provide info to one parent without that parent also receiving info wrt other students - this comes down to ho secure/onerous would the log-in for parents be?

Fortunately my children are adults, so here is how I would advise them about my grandchildren. I think the #1 is a US issue that we don't have in Europe. Funding in the UK is per child on the roll, not by

attendance. The problem with the #2 and #3, is tht like the majority of attendance applications, there is no off-switch so the child can be tracked outside the school. Unless access to the tag required an encrypted key at the RFID protocol level then I would advise against this. Simply having encrypted ata, unless updated each time, does not help. The air interface transmits bit and if these are the same each time from a child's ID, it is a means of identifying the child.

They should want the technology for Safety reasons

Inform them ahead of time and remind them of the plan and I think, for the most part, they would support. Offer them an opt out if they want.

I think parents would react positive to this plan. They would support it because they can keep track of whereabouts of their kid without use of cell phone that has GPS.

I would think that most would support it. However, a vocal minority might raise a stink!

They want it but don't want to admit they want it

SHOULD NOT allow

Parents should support it, if it enhances safety for their children.

Most parents are more concerned about safety than privacy for their children. If this is clearly sold as a safety device for their children then you can get parents on board.

The majority would likely be ok with it. The minority would be louder.

Should be well received, if there was a cost it would not be supported in Georgia, too expensive/invasion of privicy

It should be a none issue but media has over pitched the capabilities that these devices can actually be tracked.

If the children security increase, i think parents agree.

Yes. So they could know there kids where abouts

It would be a split. The information that will be provided will be for all the positive things that RFID can do, however, they probably would not mention that hackers and child predators can also follows the students location if they get access to the actve servers, which will most likely be on the cloud. The school would not admit that there are individuals in other parts of the world that make a living from hacking into systems such as these. The parents would support it in theory because of the bullet 2 and 3. Parents are very ptotective of their children and with todays incidents at educational facilities, parents would welcome the thought of additonal protection.

Probably a majority would support but only marginally out number the non-supporting parents. Parents and students will see it as an invasion of privacy. Some parents will see it as beneficial in truancy issues.

I don't think that many parents would approve of electronic tracking of their children. It's a little too "Big Brother" for most people. Maybe younger ones.....teens will resist..... Ray C
if there parents are educated they will embrace this. If they are progressive and vote Democrat, they will fight this

Privacy concerns will outweigh safety benefits

might support it, it is a lot of power that could have a negative impact if used improperly.

Most parents would support this if educated on exactly how it works and that it is restricted to in-school tracking. There will be a vocal minority who will have issues and concerns no matter what is done. I think most parents would like the program

We sell to the Education Market and it is widely embraced not only for the students but all entering the buildings.

I think they would support this function of RFIDs because of security. Some would approve and others would be appalled. Some parents would want to know where their child was at every moment, especially special needs children. Many would not want their child tracked by anyone outside the family unit

I have no issue with the approach

Parents should support it. The advantages are obvious. The need is to assure that data is safe, secure and controlled.
If the school doesn't know the students' locations, it should be closed down.

For those that see the benefits this is a good thing. For those who opposite everything will consider this as another way to control people. Overall I think people will see the benefits.

Yes; safety first but plan on a lot of lost cards and an admin nightmare

As a parent of 5, I would strongly support this technology.

Sounds like a great idea; few parents would actually monitor.

Supportive no issues

Most will support it for benefits. Who bares cost of replacing cards when children lose them - parents won't want to because financial benefit lies mostly with school. Some will not support it due to medical concerns, religious concerns, or even privacy cncerns.
I think if would provide an added layer of trust for the parents in knowing the school would be doing everything in their power to keep thier children safe.

I think opinions are split. I would want anonymous group data. And public records of how often it is used on individuals

Honestly I don't really know.... I do know this: Kids aren't dumb.... No no no....Let me rephrase that... Kids become less dumb around middle school. You'll still have kids skipping class/school, they're just going to put their ID tag on somebody elses booksack so it always appears to be in class.

Conservative parents would freak out. But overall, tracking children ONLY within the school premises should not be an issue.

A lot of parents would not be in support of this as it seems to be a huge society problem of "government tracking"

most would probably go for this exteme invasion of privacy. The children are not there voluntarily but parents and citizens of this country are gladly giving up their freedoms and privacy in the name of security.

I think parents would support it because they would be comforted knowing their child is easier to keep track of in an emergency and the school would know if they left campus without permission or didn't arrive as expected. However, as a parent, I'd be sketical as to it's efficacy since it's only as good if the children have the tag with them at all times. Otherwise, you're really just tracking their backpack or where they last lost the card.

Support

I like the overall merits of these options but I see plenty of room for abuse. Tracking bathroom time to tally up. Tracking automatically tardiness even the smallest amounts.

No support in most areas. Most areas are not prone to activities that would put the children in a situation causing a "tracker" to be deployed. Selling the unit as an attendance measure could work.

I would not like it. I don't want ANYONE to know where my child is at such a granular level. If it was within 100 yards maybe, but not to within a few feet knowing their location. Too much possibility for abuse even if it is done with the best intentios.

If students were required to carry or wear a wrist band, or a back pack or a uniform with an RFID tag that seems OK. but it should never be connected to the person in a way it could not be removed.

The parents would love it until they understood how kids cheat the system. And parents hate the idea that teachers and administrators are likely to overly depend on the system and make bigger mistakes in the care of their children. The bad thing is you ar relying on children to use the system properly.

No problems with kids having cards with RFID tags, but totally against implanted RFID chips. Understand that clever kids could "game the system" by asking a friend to carry their card for the day, while they went elsewhere - aka "Ferris Bulers Day Off". his could also allow one kid to take a test for another kid, and so on, and so on . . .

some people will fear this is a over reach of government into personal lives

i do not believe that children could adequately comprehend the implications of this technology, nor should they have their privacy invaded by an entity outside of their family.

It depends, some parents may be alright with it, others may not. Some that might not, may feel it is a violation of their private lives, others may sense that the data could fall into the wrong hands and could result into having a child held for ransom.

Most would, but a few loud ones won't (just like everything else - the few always cause the problems) If they don't like it, go to private school.

They would not react well unless it was well thought out and VERY carefully laid out to them. Even then it would be iffy. People don't like being tracked.

Provide the security in a closed loop system to protect privacy.

Parents would react positively, provided that downside risks are averted. Parents would support it provided that they are confident that such tracking is well vetted.

some would love it as an assist to their child care and/or as a control feature for them over their children. Others would hate it, thinking it another way for government and business to stick their noses into other peoples lives and privacy.

Case 2: How do you think employees would react to this plan? Would they support it? Why or why not?

no - don't like managers snooping

Generally favorably

Of course Employees will not like that. They don't like to be tracked and monitored but this application is mandatory to monitor them and to be sure about work flow.

FAIL

Personally, I don't think many contractors would support this plan at all. Rationale: I have worked too many years without constant oversight...OR why was I hired if you don't trust me??...OR I'm already a team player and don't need to be micro-managed!!

I think employers would support this.

It probably depends on the type of work. Coal miners might appreciate this more than auto mechanics given the different level of risk they face. Some employees won't like it no matter what, but most will probably get used to it being the price of being emloyed.

Uncertain.

They should

Support it especially since it involves safety

Items 1 & 3 are common benefits put to contractors of any ACS system, whether RFID is used or not. Item 2 would only be beneficial in lone-worker situations (which should only be used sparingly) and only if the location of the user can be provided. Radio okens have been used for this purpose for many years.

It depends on the work situation and how presented. I gave an earlier example of workers in a meat processing factory - no justification. One of the earliest examples that I know on in the 1980s, was this type of application for miners. They had no panic utton, but as they moved from zone to zone they were tracked. In an emergency those that were safe could be quickly accounted for, Those that were missing were in a known zone. Therefore #1 is unacceptable but a by-product of the system. It can be resolvd by a legal undertaking not to do so.

Support

Smart and loyal Employees should support it for safety reasons Dumb and un-loyal Employees will not support it as they try to cheat the systems

Not well. Big brother.

I think employee would react positive to this plan if they already wears employee badge. To them having a RFID tagged employee

badge of same thickness will be transparent to them or to their wallet thickness.

The employee reaction to this would depend heavily on corporate culture in the particular company. If it is a top-down, big brother type of culture, this would be very concerning. If it is a culture where employees feel valued and trusted, then it would b less concerning.

Revolt, mutiny

They wouldn't support it... it's too "Big Brother"-ish and gives no loyalty or trust to the employer/ employee.

Well... today i watched a large number of construction workers "moo" as they walked through an active portal. They didnt seem to hate being tracked. They seemed to not like being "herded" trough a tunnel. probably would not like it, would not support it and would feel it is an invasion of their privacy

It is a must have actually in todays business climate.

No they would not support this. They will not like this at all. Very few employees want to be tracked in such a manner. Safety is an important aspect of construction however, there are methods currently in place for safety. The safety issue is more criticl in minng and oil refinaries. The employees would not support it as I probably wouldn't. The perception would be that the employer lacks trust in the employees.

This could be beneficial however, for accountability in the event of an emergency.

I think that unions would be opposed to the use of RFID technology to track employees.

Nope.....we are not robots...

It should be formally described as a condition of employment.

Employees would not want their actions (or lack) monitored. That being said the business benefit far outweighs the risk.
wouldn't like it, because of the "big brother" mentality that would accompany it.

Most employees would not have an issue if the same RFID would allow them to control access control systems throughout the building. Again, education is key. Explaining that in an emergency, when seconds count, we can locate everyone

The workers would not care. The employees that just try to get over will not want this.

At first they react negatively. Once you explain the benefits, even the unions accept it as a life safety solution with benefits.

I'm not sure if employers would see that the benefits outweighed the concerns for this application.

Tracking for safety issues might be accepted. Tracking for time and attendance is not a good use of technology in this application.

I have no issue with this, but employees might. Don't go places at work you're not supposed to be and no issue!

The workers should accept this application. The advanbtages for the workers are obvious. These are adults -- explain the use of RFID, and how it will be used, and how it helps the workers.

It doesn't seem too difficult to have employees punch in. A radio panic button would also seem easy ti implement without RFID. If there is an emergency, identifying a particular person would not seem to be of the essence. It's a solution in search of a poblem.

(In Finland) Safety features are at least most welcome. In private sector this could boost efficiency. In public sector this is more challenging.

No; Big Brother

At first, employees may have concerns. However, once implemented and trained properly, employees will no longer have the concern.
not support it; big brother

People will get used to it

Union employees are very reluctant to adopt tracking technologies.

That is a hard one, especially point 1..I would say if you are an hourly person it would be no different than punching a time clock. Points 2 and 3 though sound resonable to me.

Mostly support

Heavy industry would more-than-likely be very supportive of a system like this. Insurance premiums would(should) plummet
Employees should support if the RFID application will make the group more efficient. Any employee that has a problem with the application is probably lazy.

For safety reasons, I believe employees would support such a system because it is how they will get paid, and also keep everyone more safe.

good

Again, really open for abuse especially from business owners tracking employees. Most business are trying to micro manage people to death to accomplish tasks that would normally take two. Why would anyone want to give up the little privacy you have for mior boost in safety for the employee.

Employees (especially union) will hate it, putting it in the "Big Brother" bucket. Industrial settings could paint it as a safety measure. They would not like being tracked throughout their day. No matter how management spun it this would not be an easy pill to swallow. It would take years for this to become a standard.

They would not. At least not the ones that are suspicious and might not always act like they are working. The good employees should not care, as long as these tags were carried, like a card, not implanted. I'd send sub contractors in my place with my I.d. And do other things creating risk issues. You need a dual authentication system to verify the I.D. as the person who is supposed to be there.

MOST employees would NEVER support the plan. Besides the "big brother is watching" image, the information could also be used or disciplinary purposes. The unions would fight it. Just ask the cops! Not happy when, at the end of a watch, their sector Sergeat asks "Why did you and Unit 53 spend 38 minutes at the Dunkin Donuts on 6th Street?" Personally, I think that it is an idea that has merit, especially the panic button idea.

only if the pay was equal to the invasion of privacy, a personal decision.

I do not see how the application as described above- of an extreme event occurring- could be used to justify the monitoring.

I think an honest worker would not care either way. I think ones that work in a dangerous environment would be in favor of it, like those in a mine.

Support it - NO. Does it matter - NO. Employees that don't like it are the ones not working anyway. If an employee has a problem, they are not compliant & fired themselves. Good employees that do what they are paid to do, will be fine. // But management cn't go over board on production levels too.

Depends on the implementation, and the motivation. If the choice was do it or leave, you would still get some that would leave. It would be better only #2 and #3 were implemented, and #3 could only be used in an emergency, requiring documentation and ful disclosure to the workers that it was being used (sirens, lights, etc) and full disclosure later as to why it was used and by whom.

Some people do not want to have "Big Brother" watching them at all times. If people are willing to have added benefits it should be a choice.

Employees would support this plan, provided that there are enough personal advantages to outweigh the corporate advantages.

Some may like it for the benefit of tracking hours (no time cards to handle) and for general safety. Most would not like it due to privacy issues.

Author Profiles

Nick Cesare

Marketing / Digital Communications

Elmira College

Kevin Londerholm

Biology

Cal Poly, San Luis Obispo

Kale Simpson

Exercise and Sports Science

Point Loma Nazarene University

Max Wicklund

Applied Health Science

Point Loma Nazarene Univesity