https://doi.org/10.48009/2_iis_2013_375-381

Issues in Information Systems
Volume 14, Issue 2, pp.375-381, 2013

RAISING AWARENESS:
ARE WE SHARING TOO MUCH PRIVATE INFORMATION?

Adnan Chawdhry, California University of Pennsylvania, chawdhry_a@calu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu
David M. Douglas, Robert Morris University, douglas@rmu.edu

ABSTRACT

Sharing information has allowed civilization to develop and society to grow and prosper. In the not too distant past, the retention of information has been the source of collective control over the masses of humanity. The Information Age has immeasurable changed this once stronghold of the elite. As users of the convenient and ubiquitous electronic devices that connect to our world and beyond, we often unwittingly and unintentionally share personal information with those we do not know. The oversharing of information and how it is collected and who collects it is the source of power. As users of these communication devices, we need to be aware of how this information is used. This study investigates how a group of university students in 2013 use and understand how they willingly or unwillingly allow their communication devices to share personal information with others and the potential effect this sharing has on their digital lives.

Keywords: Privacy, Information Technology, RFID, QR codes and Geotagging, GPS

INTRODUCTION

As we connect to our world thorough our mobile and stationary electronic devices we share information. As the old adage proclaims, information is power. Today, even the most trivial piece of our personal information is worth money to someone. More often than not, it is unknown to us with whom we unwittingly share our information with or which entity silently and tirelessly collects and sorts our digital data. Data miners, private organizations, and government agencies willingly pay for this information. How or where they receive this information matters little. Much is to be gained from the bits and pieces of our digital detritus. Once these digital fragments are gathered and sorted, reliable and accurate digital dossiers of our private and public life can be formulated. Perhaps, these digital dossiers might provide lifesaving information to a first responder in an emergency. Conversely, it could just as easily be used to damage a person's reputation or steal a lifetimes worth of savings. To do either, is only a click away to those with the wherewithal. Our exposure and willing participation has become ubiquitous. Chiefly, as a matter of convenience or perhaps one really does not care who sees or uses ones digital life. We willingly agree to the terms and conditions of use established by the application creators and network providers of our electronic appendages. Regardless of the ill or good that may evolve from our unintentional sharing of our lives, our digital life is now scattered in bits and bytes across the seamless Internet never to return or be deleted. The Digital Pandora has been released.

.

LITERATURE REVIEW

Many users of social network sites are aware of the possible pitfalls of failing to secure their personally identifiable information using the privacy settings of the site. However, what about the personally identifiable information placed in the photos that these individuals place online? With the circulation of cheaper GPS enabled cameras, the risks of unknowingly exposing personally identifiable information increases.

A possible drawback to users sharing their photos is the unintentional sharing of personally identifiable information along with a photo via the EXIF (Exchangeable Image File Format) header. Personally identifiable information has been defined in the 2007 OMB Memorandum [2] on *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone or combined with other personally identifiable information.

With geo-locating hardware (GPS receivers) being added to cell phones and cameras, some of the pictures that are available on TwitPic contain embedded information (longitude and latitude coordinates) about where the picture was taken. Cyber-criminals can take advantage of the information that is available in these photos [7].

In a study conducted by Ullrich [11], his team tested prevalence of EXIF headers in photos from TwitPic. His team wrote a script to capture 15,291 images. Scripts are miniprograms, or a series of commands that are issued to carry out a specific repetitive function (Evans). One might think of a script as a macro, which is often found in office productivity software. A second script was written to analyze the information obtained from the pictures. Of the 15,291 images that were analyzed, 399 images included location of the camera when the picture was taken and 102 pictures included the name of the photographer. Most of the pictures were being uploaded from cell phones with the majority of pictures coming from the iPhone [11]. In addition to the visible information in a digital photo, it contains an EXIF header.

The EXIF header contains many pieces of information about a photo. The majority of the fields contain benign information such as EXIF version, manufacturer of the camera, model of the camera, and the software on the camera. However, many people may not know that this same header contains fields that can contain personally identifiable information such as the date, time, owner of the device, and GPS location [10][7]. Once an individual posts a photo containing this information online, it is easy to use a mapping service such as Google Maps to discover the location by typing the longitude and latitude coordinates which can be found within the EXIF data.

Geo-location hardware is now embedded in many cell phones such as the iPhone and Blackberry and high-end cameras such as the Cannon Rebel and Nikon 5000 DSLR. The GPS receivers enable the phone or camera to record the GPS location in the EXIF header automatically. The use of this technology “denotes the marking of digital resources with geographical coordinates mostly used for images” [9]. With the increased use of mobile devices and cameras, geotagging has increased in popularity. Nations [8] defines geotagging as marking a video, photo or other media with a location. A digital photo is geotagged when the device can capture the location of where the photo was taken and adds the GPS coordinates to the EXIF header of the photo. Besides GPS coordinates, the date and time in which the photo was taken, the kind of camera and the camera settings to include shutter speed, image stabilization and image format can be recorded in the EXIF header [7].

The June 2013 edition of *Consumer Reports* magazine provided details and made projection on cell phone safety from its January 2013 survey of adult Internet users. The survey was comprised of 3,036 adults who used the Internet. Of those selected adults, 1,656 smart-phone users were asked questions about privacy and security. Virtually all smart phones contain a feature known as location tracking. Although some consider it useful in providing services tailored to the user’s needs, it also has can compromise the users privacy. According to the survey 70 percent of the smart phone users wanted to turn the location feature off but did not know how [3].

With more than 100 million Americans who use smart phones, privacy and unintentional sharing of information is a concern. Smart phones not only connect to the Internet, they can be used to pay for goods and services, check personal finances, and be used as an electronic boarding pass at transportation terminals. Additionally, we routinely send and accept text messages and photos from our smart phones. However, we seldom consider that our connectivity just might be jeopardizing our privacy. For instance, Apple and Google have the ability to track your activities bases on your phone location and unique identification [3].

Applications, also known as “Apps,” also raise concerns for privacy and the unintentional sharing of information. It has been estimated that there are over one million apps available for smart phones. Since many of these apps are free or low-cost, they are tempting to install on your device with little or no afterthought [3].

Individuals can take simple steps to protect personal data that require little effort or time. First, make sure you install apps with caution and use reputable sources such as Google Play or Amazon Appstore. Second, beware of insecure Wi-Fi networks. Open Wi-Fi networks can easily be intercepted. Third, watch out for text spam. Text spam can contain links to websites that automatically download malicious software to your phone. Fourth, disable or turn off location tracking. Turn it on only when needed, for instance when in need of directions. Fifth, when recycling or selling an older phone remember to remove memory cards, restore factory settings, and delete all sensitive data [3].

Quick Response codes (QR codes) are two-dimensional bar codes that contain a combination of alpha and numeric characters and feature URLs that direct users to sites where they learn more known as mobile tagging [1]QR codes are used to represent data, scanned and parsed by mobile devices. This technology has become a very popular marketing tool. The problem with this new technology is that mobile users scan unauthenticated data from posters, billboards, products, business cards and more. By scanning unauthenticated information, attackers can lure users to scan codes that will direct them to malicious websites [14].

A 2012 study conducted by Carnegie Mellon investigated the viability of QR code initiated phishing attacks, otherwise known as QRishing [14]. The researchers monitored user interactions with QR codes to observe is users actually visited the scanned website. Additionally, posters were distributed containing QR codes across 139 locations to observe the application of QR codes for phishing. Throughout a four-week period, the posters were scan by 225 individuals who visited the associated website resulting in 85% of users visiting the associated URL. More than 75% of users who scanned the QR code did so out of curiosity and less than 4% scanned the QR code because the information seemed useful [14].

Another current concern of privacy and the authorized and unauthorized use of personal information are RFID (radio frequency identification) devices. These devices can range in size from a small book to smaller than a grain of rice. Privacy advocates are concerned that the ubiquitous uses of these devices are a threat to civil liberties and consumer privacy. RFID technology and its surveillance capability follows the subject, collects personal information, and revels that information to data collectors as the subject moves through time and space.

Privacy activists have concerns about RFID technology, its surveillance capabilities, and their rights to digital privacy. Existing information and communication technologies such as RFID allow both commercial and government sponsored surveillance systems to construct digital files on people and objects as they move through time and space. RFID systems have the ability to covertly collect this data in real time on a person's identity, location, and activities and electronically store and share that information with those with the ability or authorization to access it [5].“Indeed, not only does the profile that RFID technology helps construct contain information about where the subject is and has been, but RFID signifiers travel with the subject in the physical world, conveying information to devices that otherwise wouldn't recognize her, and that can take actions based on that information[13].”

Digital dossiers set the person apart from the masses and confirm a person's individual passions and proclivities. These in turn could be used by the state to predict a person's future behavior (good or evil) and by businesses to determine individual spending habits [12]. Automatic identification and data collection (AIDC) systems are changing the world and altering how businesses, governments, and people are interpreting the concept of privacy.

RESEARCH METHODOLOGY

As we introduce new technologies throughout the world, individuals are finding more convenient ways of doing tasks that were once done manually. However, with this convenience comes a need for awareness so that individuals understand the benefits and risks of using a particular technology. The purpose of this study was to determine the students' understanding of these technologies and the potential risks while evaluating the students' willingness to change their behavior after learning about potential privacy concerns. The study explores the following two research questions:

RQ1: Do students understand the privacy risks associated with the use of technology?
RQ2: Are students willing to change their behavior based upon data privacy awareness?

The study examined students at a small mid-Atlantic University during the period of February 2013 through April 2013. The research utilized a quantitative methodology to assess the students' awareness and desire to modify their behavior. The population chosen for this study was comprised of undergraduate and graduate students enrolled in on-campus and online programs of study. Undergraduate students and graduate students were surveyed in order to gather data from students 18 years of age and older. A total of 138 respondents completed the survey.

The survey was designed to obtain information on various technologies used by adults including: mobile computing devices, GPS linked photographs, Quick Response (QR) codes, and Radio Frequency Identification (RFID) tags. The survey was conducted using SurveyMonkey.com, an online tool, to gather and organize data. This data was imported into SPSS for further analysis. This study used Chi-square with a statistical significance at the .05 margin of error with a 95% confidence level to determine students' awareness and willingness to modify behavior. The study was a convenience sample-surveying students from all departments within the university which include the School of Arts and Humanities, Business, Science and Match, Engineering, Computer Science, Information Technology, Criminal Justice and Psychology.

The survey instrument consisted of 28 closed-ended questions and one open ended question for further understanding of participant comments and responses. The first four questions focused on student demographics; which included gender, age, education, and degree program. Questions 5 to 18 asked students if they were aware of the capabilities associated with mobile devices, GPS linked photos from cameras or cell phones, and RFID. They were then asked a follow up question in regard to their willingness to change based upon 5 choices (Very Likely, Somewhat likely, Neutral, Somewhat Unlikely, Not Likely). The next 10 questions discussed a student's understanding of privacy risks associated with using technology. Students were provided with three scenarios to help answer the questions. The final question asked the students about their willingness to change their behavior after completing their survey and, if so, how they are planning to modify their behavior.

RESULTS

The survey responses were analyzed to assess the students' awareness of technology privacy risks and their willingness to change their behavior. Of the respondents, 67% were female students and 37% were male students. Additionally, the students ranged in ages from 18 to 62, with the mean age of approximately 25, median age of 21 and a mode of 20 years of age. The breakdown of students to their level of education was 9.6% were Graduate Students, 6.6% were freshman, 21.3% were sophomores, 33.8% were juniors, and 28.7% were seniors. Finally the breakdown of respondents per program of study included:

Table 1. Breakdown of Students per Program of Study

	Percent
Arts & Humanities	13.0
Business	21.7
Computer Science	2.2
Education	7.2
Information Systems	2.2
Information Technology	.7
Psychology	26.1
Response	.7
Science & Math	15.2
Undecided	1.4
Other (Please complete	9.4
Total	100.0

Those who responded with "Other" included responses such as Social Work, Law, Dual Degree, School Counseling, Sports Management, Communications, School Psychology, Geography, Commercial Music Technology, Parks and Recreation Management, Computer Engineering, and Creative Writing.

As a follow up to the above background questions, the survey asked the participants if they were a member of a social media site. Of the participants 89.7% said they belonged to a social media group which included Facebook, Twitter, YouTube, Foursquare, LinkedIn, and Google+. Additionally, 97% said they owned some kind of mobile computing device (Cell Phone with or without Internet, Laptop, Kindle, iPad/Tablet PC, iPod Touch, and GPS), while 3% did not.

Table 2: Categories of Awareness

Categories Of Awareness	YES	NO
Use cell phone to take photos.	92.6%	7.4%
Embed GPS coordinates in photos.	74.5%	25.5%
Turn off location tracking.	80.1%	19.9%
QR codes can convey information on time you scanned the code.	36.5%	63.5%
RFID exists in passports, licenses, clothing, and tags.	43.8%	57.2%

The survey asked questions related the use of their cell phones, taking photos, QR, and RFID. These questions included:

1. Do you use your cell phone or smart phone to take photos?
2. Are you aware that many cameras embed the location of where the photo was taken in the form of GPS coordinates?
3. Are you aware that you can turn off location tracking on your phone?
4. Are you aware that Quick Response (QR) codes can convey information such as what time you scanned the code and from what source (e.g. computer screen, magazine, signage)?
5. Are you aware that Radio Frequency Identification (RFID) tags are embedded in many objects such as passports, licenses, clothing and tags which contain personally identifiable information?

After the respondents answered the questions above related to their awareness of various technologies, they were asked to rank their willingness to change their behavior in regards to these technologies. Each follow-up question started with "Now that you know this information, how likely are you to change" and the participants were asked to rank their "willingness" in one of five responses (Very Likely, Somewhat Likely, Neutral, Somewhat Unlikely, and Not Likely). These responses are detailed below.

Table 3: Likeliness of Changing Behavior

Categories Of Awareness	Very Likely	Somewhat Likely	Neutral	Somewhat Unlikely	Not Likely
Change behavior when using a camera or cell phone.	13.2%	12.5%	32.7%	10.2%	31.4%
Change habits of scanning QR codes with your cell phone.	13.4%	11.9%	35.8%	10.3%	28.6%
Change the way you interact with RFID.	19.1%	18.3%	32.1%	8.8%	21.7%

Lastly, the study also aimed to determine if a statistical correlation existed between the technologies above and the likeliness of the respondents to change their behavior. These results were analyzed using chi-square as described in the methodology. When doing this analysis, the study evaluated the participants' responses to their awareness of each category in comparison to the willingness to change their behavior. Using SPSS, the data was analyzed and was considered statistically significant if it tested at .05 or less and was within a 95% confidence intertval. From the analysis, the results had a value of .000 which shows a very strong statistical significance between a person's awareness of the technology and their willingness to change their behavior. In other words, there is evidence to support that respondents who are now aware of the potential of each technology are likely to change their behavior. These results were well beyond the expectations of the study and therefore valuable to the study and its findings.

Table 4: Chi-Square Analysis

Technology	Chi-Square Value	Degrees of Freedom	Significance Level
Camera or Cell Phone	143.798	10	.000
QR Codes	147.472	10	.000
RFID	155.516	10	.000

DISCUSSIONS

The first research question was "Do students understand the privacy risks associated with the use of technology?" This question was designed to address whether students were aware of the capabilities of technologies that they use on a daily basis. Based upon the results, the most familiar technology that students were aware of was the use of a GPS enabled device such as a smart phone or other mobile computing device. Students were asked if they were aware that cameras and phones embed the location of where the photo was taken. Approximately 92.6% of the respondents utilized a cell phone to take pictures, 80.1% were aware that the location tracking services can be disabled, and 74.5% knew that photos are embedded with certain GPS enabled device. These results illustrate that participants are aware of the capabilities GPS-linked devices for taking photos. One interesting thing to note is that of the participants who noted they were aware that the location services could be disabled / turned off, only 23.8% said they were willing to change their behavior when using a camera or a smartphone. Although a little surprising that such a small amount would change their behavior, it leads the researchers to believe that the remainder are neutral or do not find that the GPS-linked photos violates their privacy.

Students were also asked if they were aware that RFID tags are embedded in objects such as passports, licenses, clothing which can contain personally identifiable information. Additionally, they were asked if they were aware that Quick Response (QR) codes convey information such as the time they scanned an object and what source (computer screen, magazine, signage). On the converse side, 43.8% of the students knew of the risks associated with RFID and 36.5% were aware of the risks related to QR codes. A possible explanation for low percentages related to these two technologies, as compared to the photos taken with GPS-enabled devices, could be attributed to the fact that QR codes and RFID are still relatively new in comparison to GPS technologies.

The second research question was "Are students willing to change their behavior based upon data privacy awareness?" This question focused on the respondent's willingness to change their behavior using the above technologies once they were now presented with the potential risks associated with usage. For the purposes of this analysis, "willingness to change" will be defined as "Very Likely" and "Somewhat Likely." In regards to GPS-linked photos, only 25.5% of the respondents illustrated a willingness to change their behavior when using this technology while 41.6% were unlikely to change their behavior. Participants responded that only 25.3% of the respondents would be willing to change their behavior with QR codes while 38.9% were unwilling to change their behavior. Finally, 37.4% of the respondents were willing to change their behavior in relation to RFID while 30.5% concluded they would not be willing to change their behavior.

CONCLUSIONS

The first step in bringing about change is making sure there is awareness. Until technologies are highly integrated within our society, individuals do not often seek out the risks associated with that technology, rather just concentrating on the benefits for themselves. This study illustrated that technologies such as QR codes and RFID, which are somewhat integrated into our everyday lives, don't seem to have a widespread awareness of its risks. Although the results of awareness among GPS-linked photos, QR codes, and RFID were fairly in line with our expectations based upon the familiarity of these technologies and their widespread use, the results of "willingness to change" were a little shocking. Given the lower percentages for "willingness to change," one could conclude that individuals are not as concerned about the privacy risks linked to these technologies or the lack of familiarity with the technology itself influenced participants towards not willing to change since they are not integrating that technology into their everyday lives.

REFERENCES

1. 7 Things (Educause, 2009). 7 Things you should know about QR codes. Educause Learning Initiative. Retrieved on May 1, 2013 from http://net.educause.edu/ir/library/pdf/ELI7046.pdf
2. Clayson, J. (2007). Safeguarding against and responding to the breach of personally identifiable information retrieved on January 6, 2010 from http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
3. CR Investigates. (2013, June). Keep your phone safe: How to protect yourself from wireless threats. Consumer Reports 78: 6, 18-22
4. CyLab-12-022. Retrieved on April 10, 2013 from http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12022.pdf
5. Douglas, D.M., & Paullet, K.L. (2010). RFID ubiquity and privacy loss concerns: An analysis of a Pennsylvania university. *Issues in Information Systems*. Vol. XL. No. 1.
6. Evan, A., Martin, K., & Poatsy, M.A. (2010). Technology in Action. (6th ed.). Upper Saddle River, N.J.: Pearson/Prentice Hall.
7. Flinn, M.B., Teodorski, C.J., & Paullet, K.L. (2010). Raising Awareness: An examination of embedded GPS data in images posted to the social networking site twitter. *Issues in Information Systems,* Vol. XI, No. 1.
8. Nations, D. (2010). What is geotagging? Retrieved on April 17, 2013 from http://webtrends.about.com/od/glossary/i/what-geotagging.htm?p=1
9. Razavi, M., & Iverson, L. (2009). Improving personal privacy in social systems with people tagging.
10. Twitter is a Real (Anonymous, 2010). Twitter is a real-time network powered by people all around the world that lets you share and discover what's happening now. Retrieved on May 1, 2013 from http://twitter.com/about
11. Ullrich, J. (2010). Twitpic, Exif & GPS: I know where you did it last summer. Retrieved on March 16, 2013 from http://isc.sans.org/diary.html?story/id=8203
12. Vaidhyanathan, S. (2008, February 15). Naked in the nonopticon: Surveillance and marketing combine to strip away our privacy. *The Chronicle Review.* B7-B10.
13. Weinberg, J. (2006). RFID, privacy, and regulation. In S. Garfinkel & B. Rosenberg (Eds.), RFID, application, security, and privacy (p. 88). Upper Saddle River, NJ: Addison-Wesley.
14. Vidas, T., Owusu, E, Want, S, Zeng, C, & Cranon, L. (2012, November 2). QRishing: The susceptibiloity of smartphone users to QR code phishing attacks. Carnegie Mellon University