Peripheral Privacy Notifications for Wireless Networks

Braden Kowitz
Carnegie Mellon University, HCII
5000 Forbes Ave.
Pittsburgh, PA
kowitz@gmail.com

Lorrie Cranor
Carnegie Mellon University, ISRI
5000 Forbes Ave.
Pittsburgh, PA
lorrie@cs.cmu.edu

ABSTRACT

When using wireless networks, some chats, web searches, and other information are broadcast out onto the local network. Other users on the same network may intercept and read this information. Unfortunately, without detailed knowledge of underlying technologies, many users are unable to properly evaluate the risks involved in everyday communication tasks. This study aims to develop techniques for allowing users without technical backgrounds to form more accurate expectations of privacy. We have developed a method for notifying users when their computer leaks such information. A large projected display placed in a common workplace shows excerpts from network traffic. A two-week trial was conducted to measure the effects of the display. Data was collected from network traffic monitoring and two paper surveys, which were conducted before and after the trial.

Categories and Subject Descriptors

H.5.m [**Information Interfaces and Presentation**]: Misc. K.4.1 [**Computers and Society**]: Public Policy Issues – *Privacy*.

General Terms

Design, Experimentation.

Keywords

Privacy, Wireless Network, Electronic Communication Privacy, Peripheral Display, Privacy Enhancing Technologies

1. INTRODUCTION

Many laptops in use today are equipped with wireless network capabilities. With the growing ubiquity of wireless networks, people are using the Internet wirelessly at home, at the office, at airports and at coffee shops. When untethered, users go about their daily business of browsing the web, checking email, chatting with instant messages, and all sorts of other kinds of communication made possible by the Internet. Unfortunately, many of these users remain unaware that they could be leaking private information when on a wireless network. Using simple software, anyone with a wireless card can eavesdrop on the web searches, browsing habits, instant messages, and even web-based emails of other wireless users. The goal of this project is to better inform people when their personal information is being leaked into the public space.

We begin by taking a quick look at the current state of wireless networks and cryptography. Then, we examine several models of privacy in order to compare the characteristics of wireless networks against the larger context of users' personal privacy. We briefly explain the complexities involved in defining privacy policies, and how unintended information leaks may take place even in the presence of strong encryption.

In order to notify users of information leaks, we propose the use of a large format peripheral display. We describe the design rationale for the display along with some of the implementation details. Finally, we discuss an experimental protocol to study the effects of the display, and report on the results from the study.

2. BACKGROUND

2.1 Information Leaks on Wireless Networks

2.1.1 Wireless Networks

Wireless networks are based on small radio transmitters and receivers, known as radio modems. When a user of a wireless device navigates to a webpage, the wireless device broadcasts out a request for a webpage with its radio transmitter. A wireless access point will receive this transmission, relay the request across the Internet, and then broadcast back the requested webpage.

Although this system works very well, there are some interesting side effects. Due to the fundamentals of radio technology, broadcasts can be overheard by any radio receiver that is within range. This means that messages sent over wireless networks are easily overheard by nearby computers. It is relatively easy for users of wireless networks to intercept webpage requests, instant messages, and other data sent by nearby users. While this is common knowledge in the Computer Science community, many users of wireless networks find this behavior surprising. There is reason to be concerned: a recent survey indicated that 21% of home users could access their neighbor's WiFi network from their own homes [13]. In the absence of encryption, private web searches, emails, and instant messages may all be at risk to public exposure.

2.1.2 Information Leaks

We send many messages over computer networks. Some of these messages are explicit, such as emails, instant messages, and web page requests. Other messages, such as SMB protocols,[1] happen without direct user intervention. Many of these messages contain

WPES' 05, November 7, 2005, Alexandria, Virginia, USA.

[1] SMB, or Server Message Block, protocol is commonly used to remotely access files and services over a TCP/IP network.

information about the user of the machine. When information reaches the hands of an unintended recipient, we consider it an information leak. Also, when the user does not realize that a particular piece of information is being transmitted, that is also considered an information leak.

2.1.3 Cryptography

When radio transmissions are broadcast, anyone with a nearby receiver can listen in on the conversation. As we have seen above, this may not always be a desirable characteristic. Fortunately, cryptographic techniques can be used to scramble the message before transmission. The promise of cryptography is that only the intended recipient can decipher broadcasted messages.

Applying cryptographic techniques to broadcast networks is nothing new. Nearly a decade ago, Smith et al. identified the problem that attackers may be attached to a media network in the same way as any other user. They then described a flexible cryptographic framework within which users can carefully and dynamically manage the recipients of broadcast based communication [17]. Indeed, this trend continues with many modern communication systems. Web browsers and email clients routinely use Secure Socket Layer (SSL) technology to protect messages. Skype, a maker of popular peer-to-peer internet-telephony software uses end-to-end encryption to ensure the privacy of its users [11]. These are just a few examples of Privacy Enhancing Technologies (or PETs) that can help users protect sensitive communication when using wireless networks.

Unfortunately, personal computers still broadcast a large amount of unencrypted messages on wireless networks. Most common web searches, instant messages, and web-based email services all operate without message-level encryption. If you use any of the following communication tools while on a wireless network, your private messages are at risk of being intercepted by other nearby users.

- Google Search, MSN Search, Yahoo! Search
- AOL Instant Messenger, MSN Messenger
- Google Groups, Yahoo! Groups
- GMail by Google, MSN Hotmail, Yahoo! Mail

Of course, the lack of encryption is not due to gross negligence of these companies. There is a real cost to providing the computing power necessary to run the cryptographic algorithms that protect privacy. Because of this cost, many common modes of communication are not protected from eavesdropping.

A viable approach to this problem is for end users to encrypt all communication traveling over wireless networks. One simple way to do this is for local wireless networks to use WEP (wired equivalent privacy) encryption. Although WEP has known vulnerabilities, its use can help prevent unauthorized users of a network from ease-dropping on the communications of network members. Unfortunately, configuring WEP properly can be very difficult for users [7]. A recent survey conducted by the WorldWide WarDrive project concluded that 67% of wireless networks did not use WEP encryption. [13] Another option is for individuals to use Virtual Private Network (VPN) technology to protect communication. Although VPN technology is widely available from corporate and academic IT departments, it can be difficult to setup and run for personal use. In many cases, users do not have reasonable access to tools for encrypting their communications.

Including cryptography in everyday communication systems is essential to protecting the privacy of users. But, until cryptography is ubiquitous, much of our private communications will be unprotected.

2.2 MODELS OF PRIVACY

We are interested in investigating existing models of privacy to better understand how new communication systems fit into the current landscape of personal privacy.

2.2.1 Privacy Boundaries

Social psychologist Irwin Altman views privacy as a boundary regulation process. The boundary is between the public and private, and can be thought of as levels of social withdrawal. We dynamically change the boundary to be appropriate in the context of different situations. In the real world, we use physical constraints to enforce this boundary. For example, offices afford a level of privacy because people cannot see through walls [15].

In networked information spaces, physical constraints do little to help define privacy boundaries. Pallen and Dourish [15] attempt to extend the idea of boundaries to information spaces. They define three boundaries of concern:

- **Disclosure Boundary** – In order to be an active participant in this networked world, we must disclose a certain amount of personal information.
- **Identity Boundary** – In the physical world, identity is not a concern. We know with whom we are talking. But, as we use technology to mediate communication, the identity of senders and recipients becomes much less certain.
- **Temporal Boundary** – What is said in informal contexts is not meant to be a permanent record. When even ephemeral communication is digitized, we may not be able to escape a permanent record of our actions and thoughts.

Under this model of privacy, participants need to be aware of these boundaries. But, more importantly, they must be able to regulate these boundaries as needed. With current communication systems, users may not be able to do either very well. For example, instant messages on a wireless network may reach any number of recipients, and be recorded easily for later playback. Users may be unaware of their current level of disclosure, and have no control over the identity of recipients or the permanence of the conversation. We choose technology to mediate our human-to-human communication. But in doing so, the chosen technology has removed from us some control of these boundaries.

2.2.2 Capture / Surveillance Model

We are now, more than ever before, communicating through mediating technologies such as email, instant messages and mobile phones. It is in this situation that Philip Agre's model of privacy as a capture begins to apply. He redefines our notions of personal information privacy in a novel linguistic context. According to Agre, the real world is rich with data. When we meet with someone, we share words, but also subtle inflection and body language. In this world, privacy invasions can be modeled as a kind of surveillance: a surreptitious invasion into one's personal space. But, when we choose technology to mediate communications, our grammar of actions change. No longer are we afforded the richness of reality. Instead, actions are limited to what can be represented by a string of bits. We do this willingly because of the power of bits to be transmitted with little effort.

But because our actions can now be represented in the grammar of computers, they are more susceptible to interception and storage [3].

By viewing privacy under the lens of Agre's capture model, we see that our choice of communication technology may have a profound impact on our expectations of privacy. In the real world, the presence of a video camera or tape recorder helps to shape a lower expectation of privacy. It is common knowledge that these devices may record our actions and reproduce them for others. But digital communication systems operate very differently. Our own choice of communication channel (such as phone or instant message) is now responsible for shaping our expectations of privacy.

The problem with this new model is that there are a vast multitude of digital communication methods, each having their own complex privacy implications. As an example, consider desktop email applications. For a user to understand the level of privacy she should expect on a wireless network, she must dig deep into the connection settings to see if SSL is enabled. Even if this process is understood, switching to a different medium, such as a web based email client, completely changes the process for determining the security level of the communication channel. Beyond the individual application, encryption on the wireless network itself may also change the level of security. Even within the relatively simple task of reading email, small details of how the task is performed can drastically change one's expected level of privacy.

Without understanding the details of the underlying technology, users may find it difficult to know what information is being exposed to the world of capture. If users do indeed have misconceptions about these disclosures, then they certainly cannot make an informed consent to participate in the system. That is, they cannot make an accurate cost-benefit analysis between participation in a system and the involved risk to privacy [19].

2.2.3 *Social Translucence*

Erickson and Kellogg define the concept of *Social Translucence* in digital systems. Humans are social creatures, and draw information from the world by watching what others do. But, online systems are often opaque; we have no knowledge of other's actions. Erickson and Kellogg believe that translucent systems can help "… support coherent behavior by making participants and their activities visible to one another" [8]. The authors are careful, however, to highlight the importance of constraints in such a system:

- The system should exercise constraints on transparency.
- Users should be aware of these constraints.
- All users should have a shared awareness of the constraints.

Let us compare the current state of common unencrypted WiFi networks against these standards of social translucence. There are most definitely constraints in the system: signal attenuation applies a physical constraint and encryption provides relatively strong opacity. But there are many ways in which the system remains transparent. Performing a web search, sending an instant message, or receiving web-based email are all transparent actions. Such constraints are certainly acceptable; we can design communication systems to be as transparent as desired. However, it is essential that users understand the extent of the transparency. Unfortunately, many wireless network users wrongly assume that their personal communications are opaque. The larger problem may be that there is no shared awareness of constraints. If all participants in a system believe their actions are opaque, then there is little avenue for abuse. But technologically adept users may better understand the weak constraints and use this disparity in understanding to take advantage of other users. For example, a network specialist would be easily able to listen in on the chat conversations of most wireless users. Shared awareness, as Erickson and Kellogg point out, is important for accountability.

2.3 PRIVACY PREFERENCES

At first glance, information leaks may appear to be a simple cryptography issue: if we could only encrypt all communication, then there would be no remaining privacy concern. However, the landscape is much more intricate. In our networked world, computers are constantly broadcasting out information about us. In many of these cases, the user is not aware that these broadcasts are taking place.

For example, most web browsers, when requesting a new page, also transmit the last page the user has visited. The behavior helps in directing ad revenue and in most cases the policy does not much effect end users. Some people may not mind this policy at all, while others regard it as always being an invasion of their privacy. So, how does a system designer decide if this policy is appropriate?

It turns out that making these types of decisions is very difficult. In fact, designing user interfaces for privacy may be a "wicked" problem, in that it is inherently complex [5]. Users report many reasons why they are concerned about privacy on the Internet. Data clustering reveals that Internet users can be partitioned into three groups: privacy fundamentalists, the pragmatic majority, and the marginally concerned. But, even within these groups, individuals regard certain types of personal information as more or less private than others [6]. So it is very hard (if not impossible) to find default privacy policies that are agreeable to all users.

Unfortunately, managing these policies is made even more complex by the fact that privacy preferences are highly dependent on context. The information we are willing to release about ourselves changes from situation to situation. For example, the web browser policy of transmitting the last page visited probably does not bother most people when browsing from a search engine to a public library. However, the perception of the policy probably changes if the user is traveling between a job search site and a current employer's email system. In this context, the once reasonable policy may no longer represent the wishes of the user.

Indeed, it is hard to specify what personal information should be presented about a user in differing contexts. One way to handle this ambiguity is to prompt the user about how to proceed every time a privacy policy decision must be made. Many people are familiar with the all but extinct dialog prompt, "Are you sure you want to accept a cookie?" The problem with this technique is that the cost of interruption is high. Many applications make default policy assumptions because providing a notification would be too intrusive to the task at hand. Also, since privacy is not an active consideration in most social situations, computer interfaces should not interrupt users with privacy prompts for each new context [5].

There are many examples of policies that affect the privacy of users, yet cannot be applied universally or clarified repeatedly by the user. It is in these cases where we may also be leaking information into the world. These leaks are not caused by inadequate security systems, but the inability of our computing systems to correctly interpret our changing privacy preferences.

3. PROJECT GOALS

The aim of this project is to better inform users when personal information is being leaked into the public space. In some cases an unintended disclosure is made because an application does not support encryption. Other times, a disclosure may happen because a software program assumes privacy settings for a user. In either case, we are attempting to improve the recognition of disclosure boundaries when using wireless networks. Helping users to understand the information that is being exposed to the world of capture should better enable them to make accurate cost-benefit analyses of their participation in computing networks. Through privacy notifications, users may be able to form a shared understanding as to the level of social translucence inherent in differing communication channels. This project aims to deliver such notifications in a non-intrusive way. In some cases, the user may not care about a disclosure. In other situations, sensitive communication may need to be switched to a different medium, such as a telephone call or face to face meeting.

4. PERIPHERAL DISPLAY DESIGN

Presenting notifications of leaked information is a difficult problem because the user is already involved in the primary task of sending or receiving information. So, we view these notifications as peripheral information, which is not central to a user's task, but can help a user to learn more, do a better job, or keep track of less important tasks [12]. This type of information is often communicated to a user though peripheral displays. The "stoplight" displays seen at the recent presidential debates are an excellent example of peripheral displays. They are designed to help the user to pace himself while speaking under time constraints. We aim to build a similar system that peripherally notifies wireless users when their information is leaked into the public sphere.

It is possible for users to peripherally monitor textually presented information such as headline-tickers. Maglio and Campbell look at various ways to display peripheral text to minimize distraction while maintaining a level of comprehension. There are large changes in interruption costs for different methods of displaying scrolling text. In general, horizontal continuous scrolling affects primary work the most. A discrete horizontal scroll, where the text stops when fully presented, proves to be the best choice. Audio feedback was also explored, but turned out to be a larger distracter [12]. To mimic this design, our display introduces text by fading in with a slight animation to draw attention. The text then inconspicuously fades out very slowly.

4.1 Large Format

We have chosen to construct our peripheral display as a large format projection onto a section of wall in a public area. This setup has the benefit that the notifications become integrated into the building environment, much like the wireless network itself. By using a projected display, we avoid the need to install software directly on users' computers.

In addition to these benefits, there is some evidence that users may be able to peripherally monitor large format displays better than smaller displays of equal visual angle. Given the same size of retinal image, subjects have been found more likely to glance over and read words on a wall-sized display than a personal monitor. The intuition is that people regard walls as public spaces. If this is so, then there should be less social stigma attached to viewing information displayed on a wall [18].

4.2 Balancing Notification and Privacy

In order to generate privacy notifications, we capture traffic traveling on unencrypted wireless networks. A naive implementation of a notification display would be to show every captured message on the public display. For instance, one could display every instant message chat or web search along with the name of the sender. Each user would definitely identify the message as their own. But at the same time, displaying the entire message and sender would clearly create a privacy risk to the user.

Defcon, an annual hacker conference, has featured a display of network traffic called the "Wall of Sheep." The display is used to show usernames and passwords that have been intercepted over the wireless network. But, even at a conference of hackers, the privacy of the others is respected enough to only list the first few letters of each password.

Hudson and Smith examine several useful techniques for modifying information so that it can be made publicly available. In a public network-camera application, user motion is not shown directly, but instead indicated by black blocks that slowly appear and disappear over a static image of the workspace. Group members can see if others are in the office, without necessarily knowing the visual details. By disclosing motion detection information rather than full video, the technique alleviates privacy concerns, while preserving useful information about presence. A similar technique was used with "shared audio" in which conversations were muffled to a point that the words are unintelligible, but the speaker can still be identified by intonation and rhythm of the voice. These techniques provide useful data without disregarding users' privacy. In each technique the type, resolution, or quantity of data is adjusted to strike a careful balance between utility and privacy [10].

Our initial plan to balance these concerns was to display short text snippets of two or three words from each message. Snippets were to be selected based on the individual word's usage frequencies. In order to evaluate this design idea, the proposed selection algorithm was fed messages from a corpus of 6000 instant messages. It quickly became apparent that there is a tradeoff between selecting high or low frequency phrases. Low frequency phrases generally related better to the content of the conversation and afforded better recognition. The high frequency phrases were more generic, but offered better privacy.

After some experimentation, it became obvious that selecting consecutive words from each message would present major privacy concerns. Even phrases that contained commonly used words could reveal personal information. For instance, take the phrase "Mark is single." These three words all have a high frequency in the English language, so may be assumed to be generic. The name "Mark" would not be recognized by a computer as a proper noun without applying natural language processing techniques to analyze the phrase. So, while statistically this phrase looks very generic, it contains private information that should not be made public.

4.3 One Word, with Color and Style

To build a notification display capable of preserving privacy, we decided to limit the amount of information displayed to a single word. This means that for each message received, only one word is selected to be displayed. Upon receiving a chat message or web search, the computer splits up the message into a set of words. Words that are not in an English dictionary are removed from the list. Some proper nouns and profane words are also removed from the list. Then, the longest of the remaining words (if any) is chosen for display. The sender of the message is not shown on the display.

This technique provides privacy to the user. To most observers, words will appear on the screen as if by random. But if a particular user has just sent a message, she may notice a recently used word on the display. Eliminating the sender, receiver, and conversational context will hopefully preserve good characteristics of the information, such as recognition by the user, while preventing unwanted disclosure.

We take two additional steps to help the user identify the word as their own. First, a word appears on the screen immediately after a message is sent. So if a user performs a web search, a word from that search may be displayed even before the results are returned. This creates an effect of temporal causality. The second technique is to display words with a different font face and color for each user. This does not directly identify the source of a message. But, users should be able to better recognize which words originated from their computer when those words are presented in a consistent manner. The disadvantage to assigning each user a customized style is that an alert observer may be able to discover the link between the visual style and the user. To compensate for this, we have allowed only three font faces and 12 individual colors, for a combination of 36 possible visual styles. Because users are assigned to styles randomly, more than one user may share a single visual style.

We believe that this display provides utility to the user while mitigating possible privacy risks. By paying attention to these notifications, users may be able to generalize from the current situation and deduce which common tasks leak information onto the local network. Our current prototype display produces notifications for outgoing AOL Instant Messenger chats and web searches with Google, Yahoo, and AOL.

4.4 IMPLEMENTATION

When a computer is connected to a wireless network, it receives all broadcasts from the surrounding local area. Most computers look at each message on the network, and throw out the message if it is not addressed to the computer. By modifying this behavior, a computer can easily listen to all messages transmitted within the local area.

4.4.1 Multi-Channel Networks

Many wireless networks are relatively simple and function on only one of several available channels. With these networks, almost any computer can be set up to monitor all of the network traffic. However, many large-area wireless networks use a number of access points on separate channels. Devices on these wireless networks automatically switch to the access point (and channel) with the greatest signal strength. Our university uses such a system with three individual channels. In order to monitor traffic of all users, we specially equipped a machine with three separate WiFi cards and antennas. This setup enabled us to monitor traffic across all of the available network channels.

4.4.2 Data Path

Our peripheral display is implemented using Ethereal, an open source protocol analyzer [9]. Ethereal connects to a network and reassembles packets through its knowledge of common network protocols. The peripheral display uses Ethereal to capture and decode outgoing instant messages as well as HTTP GET requests.

Data from Ethereal is read by a simple Ruby [16] script, which parses the raw messages and extracts a list of words from each message or web search. At this point, the sender's IP address is processed though an MD5 hash. This procedure is meant only to act as a blind so that experimenters needed less direct access to the IP addresses. Later, traffic can be correlated with survey results without having to store the IP address directly.

4.4.3 Selecting Words

In order to have the desired display characteristics, the list of potential candidate words goes though a series of filters. The first filter removes words that match some basic profanity rules. This filter is based on the FCC's profane broadcast restrictions. The second filter removes words that are under 5 characters or over 12 characters in length. The third filter is a rate limiter, which prevents messages by the same sender from being displayed in rapid succession. The rate limiter is in place to keep a single user from flooding the display.

One word is chosen from the list of remaining candidate words. The goal is to pick the word that is most unique in the English language. Initial attempts at using word frequency tables resulted in disappointing word selections. The display presently picks the word with the greatest number of letters. This seems to be a good heuristic for selecting words that evoke recognition from users.

The word to be displayed, along with a hash of the sender's address, is sent over a UDP network socket to a Java application, which is responsible for presenting the word on the display. The sender ID is used to pick a unique color and font for a particular sender. The color is picked out of a small palette, and the font is picked from "monospaced", "serif", or "sans-serif." This way, all notifications for a user will be presented in a consistent color and font. Hopefully this will help users recognize their own alerts from background traffic.

5. EXPERIMENTAL STUDY

5.1 Permission

When intercepting personal communications of others, it is imperative to understand the legal ramifications as well as any policy mandates. After careful examination we concluded that our study did not violate Federal statutes on interception of electronic communication [1,2]. However, our campus policies and computer science department have placed tighter restrictions on acceptable behavior with regard to the campus network [4, 14]. Fortunately, we were able to discuss this project with members of the administration and were eventually given special permission to monitor the campus wireless network for the purposes of this study. To ensure participants were well informed of the risks involved with this study, we sought formal approval through our Institutional Review Board. It is vitally important that researchers take these basic steps before performing similar research.

5.2 Selecting the Space

A large atrium was the initial proposed location for the peripheral display. The atrium was located near the computer science building and featured a food court. Students, faculty, staff, and visitors commonly use the wireless network in the atrium space.

Before deploying the display in a public space, it was necessary to get the approval from Carnegie Mellon's network administration and institutional review board (IRB). After meeting with these groups, it became clear that we would be required to give wireless users notice of the peripheral display's workings. Seeing a word from a private conversation presented on a public display could make a person feel uncomfortable. From the standpoint of the IRB, this risk is real, and needs to be managed. However it is not obvious how to properly give notice to all participants in a public wireless network. Sending out a mailing to individuals in the school of computer science would cover most people. But, it would not inform off-campus visitors or students from other departments. One way to provide notice would be to place signs on all doors leading to the atrium. But the wireless network can be reached from outside of the building, so the signs would not give notice to everyone.

There are clearly risks involved in deploying the peripheral display in a public location. But, a public display has some notable benefits. For one, a public deployment would be able to reach more people. Seeing a word from leaked information presented on a large display communicates well the notion that some private information is in fact flowing into the public sphere. The display simply acts as a rebroadcast from the public medium of radio waves to the public medium of a projected display.

Trying to evaluate the effectiveness of the peripheral display in the atrium setting proved to be too difficult. Instead, we chose a graduate student lab where students share an open workplace. This allows us to deploy the system in a semi-public location, and elicit feedback from users who give informed consent to participate. The students using this lab were not computer science or engineering students.

5.3 Study Design

We tested the peripheral display described above with a small group of participants who work in a shared space. Eleven out of approximately 24 people in the space volunteered to take part in the study. We found from an initial survey that nearly all participants were frequent users of web browsers, chat clients, and wireless networks. Six of the subjects used AOL Instant messenger, the IM protocol detected by the display.

The display was installed in the participant's workplace for a period of two weeks and captured network messages only from users who volunteered for the study. During the second week, the display presented privacy notifications as described above. However, in the first week, the display was configured slightly differently. Instead of displaying a notification message, it would instead select a random word from a chat corpus and delay the presentation for a few minutes. The purpose of this procedure was to adjust users to the presence of the display without actually providing privacy notifications. We ran surveys before the trial, after the first week of acclimation, and after a the second week of notifications.

Surveys were designed to measure participants' comfort level when "discussing private matters" through various communication channels. We compared perceptions of privacy in IM chat, email, phone calls, face-to-face and other mediums. The survey also measured comfort level when using the Internet at different locations, such as "at home" or "in the office." In addition to the surveys, the sign recorded a log of every message that was leaked on the network. The following data was logged for later analysis:

- Timestamp (day and time)
- Message type (instant message or web search)
- Hash of the IP of the sender.
- Word to be displayed (not all messages generate a displayed word)

This data was recorded to detect if instant messaging or web searching declined over the two weeks as a result of the sign's presence. We reasoned that if participants felt they had less privacy on the network, then they would occasionally refrain from sending instant messages or searching the web. Because of this, we expected to see a small decline in network usage between the two weeks

5.4 Results

Participants reported on the surveys that they were most comfortable discussing private matters face-to-face. For communication at a distance, participants reported that they were more comfortable discussing private matters over the phone than with emails and instant messages. We did not see any significant difference in reports between corded phones, cordless phones, and mobile phones.

Participants also reported that they were more comfortable at home than on campus when "discussing private matters over email and chat" and when "searching the web for private information." There was no significant difference in the results between comfort levels on a wired or wireless network.

Since the survey were given at the start and end of the trial, we could compare the results to determine if the peripheral display had an effect on participant's perceptions of privacy. We were unable to detect any significant change in participants' comfort level across communication mediums or locations. While network usage did decrease in the second week, the change was not significant.

There were, however, some interesting comments on the open-ended portions of the surveys. Three of the participants were able to correctly articulate some of the methods of communications that were monitored. When asked how the words on the sign were generated, they responded:

- *"From our computers; chat windows and browsers"*
- *"Through IMs and maybe other internet based programs"*
- *"From Google search bars, iChat"*

In addition, several participants noted a change in their expectations of privacy:

- *"I DID become much more self conscious of what I was writing when chatting with friends even though I didn't feel I was chatting about anything private."*
- *"[Instant Messaging] felt less private. It wasn't that anyone could get any context from the words, but it did make me feel less 'secretive'. "*
- *"I feel like my information / activity / privacy are not being protected as much as before. seems like someone can*

monitor or get my information from my computer, or even publish them."

While this is indeed promising, we are careful to point out that participants may not have discovered that the network and communication medium were insecure. Instead, they may have attributed the change in perceived privacy to the display's presence. The survey asked if the participant's behavior had changed and if the change would persist after the display was removed. One participant answered the question this way:

"Hmm, not sure. Probably not. Now that words are gone, I'll go back to the same."

Future work should look for better ways to communicate that the primary privacy risk is associated with individuals' use of the wireless network, rather than the peripheral display.

6. NEXT STEPS

We believe that presenting information leaks in a peripheral display could yet prove to be a valuable technique for helping users maintain privacy across varied communication mediums. In the future, it may be possible to test the peripheral display in slightly different fashions. There is a great power in the context of presentation. User opinions may have changed differently if there was no detailed consent form, or if the display was presented on the user's screen rather than on the wall. Many of these directions are worth exploring. In the future, we would like to test this display in a large public space to explore the effect with a broader population. One possible improvement would be to provide a method by which users can secure their data. For example, a web address could be posted along with the display where users could find out more information about the project, and choose to install VPN software or other privacy enhancing technologies. With a setup like this, we could measure how many users went to read the information, and what percentage took actions to secure their messages.

7. ACKNOWLEDGMENTS

Many thanks to Rob Reeder, Dawn Dowling, Charles Bartel, Mary Ann Blair, Alex Darrow, Janette Fong, and all of the HCI students who helped with this project.

8. REFERENCES

[1] 18 USC 2511. "Wire and electronic communications interception and interception of oral communications". Public Law.

[2] 18 USC 2701. "Unlawful access to stored communications". Public law.

[3] Agre, P.E. "Surveillance and Capture: Two models of privacy". *The Information Society* 10 (1994): 101-127.

[4] *Carnegie Mellon University Policies*. Carnegie Mellon University. 5 Oct. 2004 <http://www.cmu.edu/esg-cat/>.

[5] Cranor, Lorrie and Mark Ackerman. "Privacy Critics: UI Components to Safeguard Users' Privacy". *Conf. Human Factors in Computing Systems CHI'99* 2 (1999): 258-259.

[6] Cranor, Lorrie, Joseph Reagle, and Mark S. Ackerman. *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*. 14 Apr. 1999. AT&T Labs-Research. 23 Sept. 2004 <http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm>.

[7] Cynthia Kuo. Vincent Goh, Adrian Tang, Adrian Perrig, Jesse Walker. Design and Evaluation Method for Secure 802.11 Network Configuration. Unpublished manuscript 2005.

[8] Erickson, Thomas, and Wendy Kellogg. "Social Translucence: An Approach to Designing Systems that Support Social Processes". *Transactions on Computer-Human Interaction* 7 (2000): 59-83.

[9] *Ethereal: A Network Protocol Analyzer*. 18 Nov. 2004 <http://www.ethereal.com/>.

[10] Hudson, Scott, and Ian Smith. "Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems". *Proceedings of the 1996 ACM conference on Computer supported cooperative work* (1996): 248-257. <http://doi.acm.org/10.1145/240080.240295>.

[11] Leyden, John. *Skype launches Pocket PC software*. 10 Sept. 2004. The Register. <http://www.theregister.co.uk/2004/09/10/pocketpc_skype/>.

[12] Maglio, Paul, and Christopher Campbell. "Tradeoffs in Displaying Peripheral Information". *Proceedings of ACM CHI 2000 Human Factors in Computing Systems* (2000): 241-248.

[13] Metz, Cade. "The Trouble With Wireless" *PC Magazine* 19 Apr. 2004.

[14] *Network use policies - SCS/CMU Computing Facilities*. Carnegie Mellon University. 5 Oct. 2004 <http://www-2.cs.cmu.edu/~help/networking/net_use.html>.

[15] Palen, Leysia, and Paul Dourish. "Unpacking 'privacy' for a Networked World". *Proceedings of the conference on Human Factors in Computing Systems* (2003): 129-136. 5 Oct. 2004 <http://doi.acm.org/10.1145/642611.642635>.

[16] *Ruby: The Object-Oriented Scripting Language*. 15 Nov. 2004 <http://www.ruby-lang.org/en/>.

[17] Smith, Ian, Scott Hudson, Elizabeth Mynatt, and John Selbie. "Applying Cryptographic Techniques to Problems in Media Space Security". *In Proceedings of ACM Conference on Organizational Computing Systems*. 8 (1995).

[18] Tan, Desney, and Mary Czerwinski. "Information voyeurism: social impact of physically large displays on information privacy". *Extended abstracts on Human factors in computing systems*. (2003): 748-749.

[19] Turow, Joseph. *Americans & Online Privacy: The System is Broken*. June 2003. Annenberg Public Policy Center of the University of Pennsylvania. 9 Sept. 2004 <http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf>.