

# The Wi-Fi Privacy Ticker: Improving Awareness & Control of Personal Information Exposure on Wi-Fi

Sunny Consolvo<sup>1</sup>, Jaeyeon Jung<sup>1</sup>, Ben Greenstein<sup>1</sup>, Pauline Powledge<sup>1</sup>, Gabriel Maganis<sup>2</sup>,  
& Daniel Avrahami<sup>1</sup>

<sup>1</sup>Intel Labs Seattle  
Seattle, WA 98105, USA  
{sunny.consolvo, jaeyeon.jung,  
benjamin.m.greenstein, pauline.s.powledge,  
daniel.avrahami}@intel.com

<sup>2</sup>Department of Computer Science  
University of California, Davis  
Davis, CA 95616, USA  
maganis@cs.ucdavis.edu

## ABSTRACT

Anyone within range of an 802.11 wireless network (“Wi-Fi”) can use free software to collect the unencrypted web traffic of others on the network. However, many Wi-Fi users are completely unaware of the risk that this creates. This work aims to improve users’ awareness about what they expose to others on Wi-Fi networks and provide them with some control. Our system, the *Wi-Fi Privacy Ticker*, displays information about the exposure of sensitive terms that are sent to and from a user’s computer and prevents the unencrypted transmission of terms from the user’s computer that she has identified as highly sensitive. In a three-week field study with 17 participants, we found that the Wi-Fi Privacy Ticker improved participants’ awareness of the circumstances in which their personal information is transmitted. We show that this heightened awareness contributed to changes in their behavior while on Wi-Fi.

## Author Keywords

Wi-Fi, wireless network, privacy, peripheral displays, ticker, awareness, control, data exposure, data leaks.

## ACM Classification Keywords

H.5.2. User Interfaces: Evaluation/methodology, Graphical user interfaces (GUI); H.5.m. Information interfaces and presentation (e.g., HCI); Miscellaneous.

## General Terms

Design, Security

## INTRODUCTION

It has become alarmingly easy to learn a lot about someone when she uses an 802.11 wireless network (i.e., Wi-Fi). First, people routinely use Wi-Fi from public places such as cafés, hotels, airports, and even auto shop waiting rooms. While the number of Wi-Fi networks that use encryption is rising at home and work, it is typical for public Wi-Fi hotspots to be completely open or to apply basic security

schemes that provide little to no protection for the user<sup>1</sup>. Second, in order to use many web services, a user must provide personal data such as an email address and password, her name, or her ZIP code. Consider, for example, what she provides to set up and use her favorite social networking site or web-based email. Regrettably this information is often transmitted without encryption, or “in the clear,” by websites [4]. Third, tools for eavesdropping on Wi-Fi network traffic are freely available and easy to use [12]. This means that unless data are explicitly encrypted by websites or routed through a network that encrypts its traffic—such as a *Virtual Private Network (VPN)*—anyone with a computing device who is within range of such a network can read and interpret all web traffic on the network. This makes it increasingly easy to track and aggregate user information over time, which reduces the barriers for attacks such as identity theft, stalking, or corporate espionage.

As prior research has shown, many Wi-Fi users are completely unaware of this risk. In a recent study [7], we found that Wi-Fi users understand practical details of using Wi-Fi and have concerns such as people looking over their shoulders or “clever hackers” breaking into their computers. However, they lack awareness of the potential visibility of their communications. Results from that study suggest that once the threats have been explained, users appear to be willing to do something to mitigate the threats.

In this paper, we present the *Wi-Fi Privacy Ticker*, a system that aims to improve users’ awareness and provide them with some control over what they expose to others on Wi-Fi networks. In a style similar to that of a stock or news ticker, the *Wi-Fi Privacy Ticker* displays information about the unencrypted exposure of terms that the user has asked it to monitor (Fig. 1). In addition, the system outright prevents the unencrypted transmission of terms that the user has identified as being highly sensitive.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*UbiComp '10*, Sep 26–Sep 29, 2010, Copenhagen, Denmark.

Copyright 2010 ACM 978-1-60558-843-8/10/09...\$10.00.

---

<sup>1</sup> Such security schemes include web-based authentication with no data confidentiality or *Wired Equivalent Privacy (WEP)*, on which it is trivial to eavesdrop on other users when on the network, as well as break the security to get onto the network [1].



**Figure 1. The Ticker display sits above the user’s task bar. The call-outs show some of the terms and indicators that are currently visible; from left to right: Watch List term, “patriciaticker@webmail.com,” was sent out in the clear by “eventplanningsite.com,” and “<Patricia’s password>” was sent out in the clear by IP address “123.45.67.89;” the Wi-Fi Network Status Indicator reflects that the user is currently connected to an “Open Network.”**

We report findings from a three-week field study with 17 participants who ran the Wi-Fi Privacy Ticker during their normal Wi-Fi use. Through the analysis of usage logs, surveys, and interview responses, we show that the Wi-Fi Privacy Ticker improved participants’ awareness of the circumstances in which their personal information gets transmitted. We also show that this heightened awareness contributed to changes in their behavior while on Wi-Fi.

Our work provides two key contributions: (1) a novel system that improves users’ awareness of and control over data exposures on Wi-Fi by allowing them to monitor information that they have identified as sensitive; and (2) we show that a real-time awareness display can improve users’ understanding of the risks of using Wi-Fi in the wild.

The remainder of this paper is structured as follows. After discussing related work, we describe the Wi-Fi Privacy Ticker, our early experiences with the system, and the three-week field study. We follow with key study results and a discussion, including opportunities for future work.

## RELATED WORK

We discuss two areas of research that are particularly relevant to the Wi-Fi Privacy Ticker: explorations of users’ understanding of and behavior on Wi-Fi, and technologies that improve user awareness and control of Internet use. We also describe recent commercial solutions that improve awareness of privacy risks associated with Internet use.

### Understanding & Behavior on Wi-Fi

Kindberg *et al.* explored the process of connecting to public Wi-Fi networks [5,6]. In a recent study [5], they investigated the concepts of physical and virtual linkage as a means of helping the user connect directly to a legitimate public Wi-Fi network (e.g., provided by a café), rather than to or through an attacker. In a task-based study conducted on the University of Bath campus, 28 participants attempted to connect to a Wi-Fi network provided by a fictional café that was set up for the study. While this work and the Wi-Fi Privacy Ticker share a goal of improving privacy on Wi-Fi, they address different risks.

In a four-week exploratory study with 11 participants recruited from the general public [7], we investigated users’

understanding of wireless networking, their concerns related to Wi-Fi use, and their existing practices to mitigate those concerns. To protect themselves, participants performed actions such as tilting or dimming their screen, sitting with their laptop angled toward the wall, and using antivirus software and firewalls. They were not, however, aware of risks such as the visibility of their unencrypted communications. This left the participants with a false sense of security because they thought that they understood the risks and had taken appropriate precautions.

The Wi-Fi Privacy Ticker was designed based on results from our exploratory study [7]. It aims to improve Wi-Fi users’ awareness of threats such as the visibility of their unencrypted communications and provide them with some control over the exposure of their data.

### Improving Awareness & Control

Kowitz and Cranor’s public peripheral display [8] improves users’ awareness of the visibility of their communications by projecting words that are sent in the clear over Wi-Fi onto a wall in a public area. The prototype was installed in the shared workspace of a graduate student lab where 11 lab occupants participated in a two-week field trial. The Wi-Fi Privacy Ticker was inspired by and extends this idea with a display that resides on the user’s device and also tracks terms of interest, details of prior exposures, and prevents the unencrypted transmission of highly sensitive terms.

Friedman, Howe, and Felten’s *Mozilla Cookie-Watcher* [3], which resides in the sidebar of the user’s web browser, displays in real-time when the user’s machine receives a cookie. It also allows the user to edit a cookie’s expiration date or delete the cookie. The researchers performed a lab-based usability study with eight participants recruited from the University of Washington’s student and staff population. Stoll *et al.*’s *Sesame* [14] provides users with a ‘behind-the-scenes’ view of their system so that they may make informed decisions that require system-level knowledge. In a task-based lab study, 20 undergraduate students used either Sesame or a popular commodity firewall to help them determine whether a given situation posed a security threat.

While the Mozilla Cookie-Watcher, Sesame, and the Wi-Fi Privacy Ticker share a goal of providing the user with awareness and control as it relates to her use of the Internet, the projects address different risks.

### Commercial Solutions

Several recent commercial solutions help improve users' awareness of privacy risks associated with Internet use. For example, when the user attempts to connect to an open Wi-Fi network in Windows 7, the operating system (OS) displays a message that information sent over the network might be visible to others, and a shield icon appears near the signal strength display for the network<sup>2</sup>. The *Google Dashboard*<sup>3</sup> summarizes personal information (e.g., email contacts, web search history) associated with the user's Google account. It categorizes information based on the application that collected the information (e.g., Gmail, Google search, etc.). *Little Snitch 2*<sup>4</sup> is a Mac OS X application that notifies the user when a program attempts to establish outgoing connections, allowing her to block unwanted attempts by network programs to send data out.

Commercial solutions such as these suggest a growing need to provide users with improved awareness about and control over their Internet use.

### THE WI-FI PRIVACY TICKER

Our system, the *Wi-Fi Privacy Ticker*, resides on the user's laptop and works as follows: the user provides terms for the system to monitor (e.g., her name, email addresses, passwords, ZIP code, etc.); when she uses Wi-Fi, the system monitors her network traffic; when it detects that one of her terms is being sent or received in the clear by a website, that term is shown on a peripheral "ticker" display (Fig. 1) and added to an archive. User-control is provided by preventing terms that she has identified as being highly sensitive from being transmitted in the clear.

Next, we describe the Wi-Fi Privacy Ticker's network monitor, control mechanism, ticker display, archive, and important considerations for protecting users' data.

#### The Network Monitor

The Wi-Fi Privacy Ticker<sup>5</sup> can monitor any network communications originating from or sent to the user's computer by hooking *NtDeviceIoControlFile*, a Windows system call, which handles network-related requests<sup>6</sup>. For

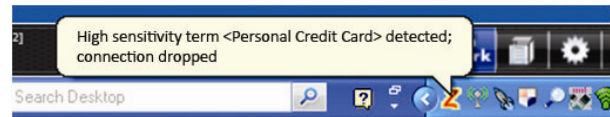
<sup>2</sup><http://windows.microsoft.com/en-us/windows7/How-do-I-know-if-a-wireless-network-is-secure> {verified 8 June 2010}

<sup>3</sup><http://www.google.com/support/accounts/bin/answer.py?answer=162744&hl=en> {verified 8 June 2010}

<sup>4</sup> <http://www.obdev.at/products/littlesnitch/index.html> {verified 8 June 2010}

<sup>5</sup> We implemented the Wi-Fi Privacy Ticker prototype on Windows XP SP3.

<sup>6</sup> <http://msdn.microsoft.com/en-us/library/ms648411%28VS.85%29.aspx> {verified 8 June 2010}



**Figure 2. When the system “zaps” a term, a stylized ‘Z’ appears in the user’s system tray and a balloon tip explains what happened. The zapped term also appears in the *Ticker display* with a strikethrough.**

the three-week field study, we configured the network monitor to inspect network communications from the Internet Explorer and Firefox browsers. The network monitor scans the intercepted communication content for the presence of *Watch List* terms using pattern-matching rules that were hand-coded for each type of term (e.g., street address, email address, first name, password, etc.).

#### The Control Mechanism

The system's control mechanism, the *Zapper*, automatically drops the user's connection to a website when a term that she has identified as being highly sensitive is about to be sent out in the clear. We implemented the *Zapper* in the Windows kernel. The *Zapper* works closely with the *Network Monitor* (described above) and closes the socket device handle (TCP connections) when it detects a highly sensitive term in the socket's "send" buffer, thereby immediately terminating the user's connection to the website. The system "zaps" terms on networks that do not employ encryption (i.e., what we call *Open Networks*) or use the WEP encryption scheme (i.e., *Closed Networks*). Terms are not zapped on WPA- or WPA2-enabled networks (i.e., *Secure Networks*) or if the user is using a *VPN*<sup>7</sup>.

To indicate to the user that a term has been "zapped," the term appears in the *Ticker display* (described below) with a strikethrough (e.g., "~~<Personal Credit Card>~~"), and a balloon tip appears in her system tray to let her know that the connection was dropped (Fig. 2). Obviously, the system cannot prevent terms from being received in the clear—in that case, the term appears in the *Ticker display* without the strikethrough (e.g., "<Personal Credit Card>") so that the user knows that her term may have been exposed.

#### The Ticker Display

The Wi-Fi Privacy Ticker uses a common metaphor—a ticker display—to communicate real-time updates to the user. However, instead of communicating stock prices or news headlines, it provides real-time alerts of potential data exposures resulting from web browser use while on Wi-Fi. The *Ticker display*, a single-line display of continuously scrolling text that moves at a constant rate horizontally from right to left [10], sits above the user's taskbar at the bottom of her screen. We implemented the *Ticker display*

<sup>7</sup> The system considers WEP-enabled networks as *Closed* rather than *Secure* because the security they provide is well known to be weak [1]. As vulnerabilities in other Wi-Fi security protocols come to light, they would also be categorized as *Closed Networks*.



**Figure 3. A tool-tip reveals that “www.eventplanning.com” sent *Watch List* term “<Work ZIP Code>” to five 3<sup>rd</sup> party sites. The darker shade and ‘::’ surrounding the term remind the user that she is on a *Secure Network* or *VPN*.**

using the .NET Windows Presentation Foundation (WPF)<sup>8</sup>. Using the WPF’s storyboard animation, when a term that the Wi-Fi Privacy Ticker monitors is sent or received in the clear, it slowly scrolls across the *Ticker display* (Fig. 1). If no monitored terms are detected or the user is not using Wi-Fi, ‘—’ moves across the *Ticker display* to indicate that the system is working; this does not necessarily mean that nothing is being transmitted to/from the user’s device.

**Terms.** Two categories of terms are monitored: (1) *Watch List* terms that the user specifies, and (2) search terms (i.e., searches on Google, Bing, or Yahoo!)<sup>9</sup>. Color reflects the term’s sensitivity level (red for high, orange for medium, yellow for low, and gray for search terms). When the user sets up a *Watch List* term, she assigns a sensitivity level and selects if the term itself (e.g., patriciaticker@webmail.com) or the description that she provides (e.g., “<my webmail address>”) should be displayed (Fig. 1). The user may add, edit, or delete terms in her *Watch List* at any time. Her *Watch List* is managed in her *Preferences*, which is accessed from a button on the *Ticker display*.

For each term, the Wi-Fi Privacy Ticker indicates whether the term was sent (‘out’) or received (‘in’), the number of times the term was sent/received within a short time window, and the domain name (or IP) of the server communicated with<sup>10</sup>. Additionally, if the user hovers over a term, a tool tip will reveal additional details (Fig. 3).

Terms in the user’s web traffic are often exposed faster than they can be scrolled onto the *Ticker display*, thus a backlog of terms waiting to be displayed can develop. We devised several rules to prioritize the display of terms in this queue. First, terms appear in the order in which they are detected; however, a term’s sensitivity level takes precedence over the detection order. For example, a highly sensitive term will appear promptly in the display, even when the queue is backlogged with lower sensitivity terms. Search terms have the lowest priority. Second, the *Ticker display*’s queue has a

<sup>8</sup> <http://msdn.microsoft.com/en-us/library/ms754130.aspx> {verified 8 June 2010}

<sup>9</sup> If the user’s search term matches a *Watch List* term, it will be treated as a *Watch List* term.

<sup>10</sup> To obtain the domain name of the server, we parse the connection’s HTTP request headers if available. Otherwise, we perform a reverse DNS lookup to resolve the IP address. If the lookup fails, we display the IP address itself.

time-out: a backlogged term is dropped after waiting in the queue for 90 seconds. During pilot testing, we found that 90 seconds represented a good compromise between providing a comprehensive record while avoiding staleness. Any *Watch List* terms that are dropped from the queue are logged in the user’s *Archive* (described below).

**Network encryption.** In addition to *Watch List* and search terms, the *Ticker display* reflects what encryption the Wi-Fi network provides<sup>11</sup>. This may reveal, for example, that the user’s personal email address is being sent in the clear, but she is on a *Secure Network*. Even though terms sent over a *Secure Network* are unlikely to be exposed to others on the network, the system makes this distinction so that the user knows that her data is being protected by the network, not the website. If she were to use the same website on an *Open* or *Closed Network*, her data would be exposed.

When a term is sent in the clear, it appears in the *Ticker display* regardless of any network encryption. When on an *Open* or *Closed Network*, terms appear in bright shades of red, orange, yellow, or gray (Fig. 1). However, when on a *Secure Network* or if the user is using a *VPN*, her terms appear in darker shades of red, orange, yellow, or gray, and are preceded and followed by ‘::’ to indicate that the network, not the website, is providing some protection (Fig. 3). In addition, the *Wi-Fi Network Status Indicator* on the *Ticker display* continuously reflects if the user is connected to an *Open Network*, *Closed Network*, *Secure Network*, *VPN*, or is not using Wi-Fi (i.e., *Wi-Fi Off*) (Fig. 1).

### The Archive

The user may review past exposures in the *Archive*. It is accessed via a button on the *Ticker display* and contains a list of all of the *Watch List* terms that have been detected; it does not contain the user’s search terms. The user can sort, aggregate, and visualize her term exposures in a variety of ways, for example, by a particular term (e.g., “patriciaticker@webmail.com”), term type (e.g., “email addresses,” “passwords,” “last names”), sender/receiver (e.g., “www.websearch.com”), date of exposure, and so on.

The *Archive* includes any *Watch List* terms that were detected while the *Ticker display* was minimized or that were dropped from the queue for time-out reasons.

### Considerations for Protecting Users’ Data

Systems that collect and store personal data must provide adequate protection for the user. Although the Wi-Fi Privacy Ticker collects minimal information on particularly sensitive term types when possible (e.g., collecting the last four digits of the user’s social security number rather than the entire number)—and the user chooses which types of terms to monitor, the user’s *Watch List* terms, if exposed to

<sup>11</sup> The system periodically probes the network interface(s) and collects information about the type of network to which the device is connected (e.g., Wi-Fi, VPN), the SSID, and the types of Wi-Fi security (e.g., WEP, WPA, WPA2).

others, could put her privacy at risk. To mitigate this risk, the Wi-Fi Privacy Ticker implements three security features. First, the user's *Preferences* (i.e., where she manages her *Watch List*) are password-protected. Second, particularly sensitive term types—passwords and the last four digits of her social security number—are never shown in the clear, even where she manages her *Watch List*. Third, the database in which the system stores the user's terms remains encrypted on her machine. The first two security features are intended to prevent others who may have access to the user's machine from accessing her *Watch List* through the application. The third security feature is intended to prevent accidental or malicious leaks of her *Watch List* terms and other usage data from the database.

### EARLY EXPERIENCES WITH THE SYSTEM

Once implementation was complete, we tested the Wi-Fi Privacy Ticker against popular websites to see how exposed personal data would be reflected to users. Our examination included creating accounts, logging in and out of the accounts, and simulating regular site visits.

Among 10 of the popular websites that we tested (amazon.com, cnn.com, ebay.com, evite.com, facebook.com, linkedin.com, nytimes.com, twitter.com, tripit.com, and washingtonpost.com), we found that:

- four sites did not encrypt any user credentials (i.e., neither username *nor* password) during login,
- one site sent the user's ZIP code (e.g., 98105) and city (e.g., Seattle) out to multiple 3<sup>rd</sup> parties, whether or not she was logged in to the site, and
- one site sent out the username (which was also the user's email address) to affiliate sites.

Next, we describe the three-week study of the system.

### 3-WEEK FIELD STUDY OF THE WI-FI PRIVACY TICKER

A three-week field study (N=17) illustrated the impact of the Wi-Fi Privacy Ticker on awareness and behavior.

#### Study Procedure & Data Collection

At the beginning of the study, each participant completed a consent form and background survey. The survey asked about basic demographics, computing at home and work, their home network, online activities, and opinions about Wi-Fi. After completing the background survey, they received instructions via email for installing the software. No training was provided, however participants received a two-page quick start guide and a user manual.

Each participant used the Wi-Fi Privacy Ticker prototype on their laptop for three to four weeks, during which they completed five surveys. These surveys asked about activities or events that may have affected their Internet use (e.g., travel, deadlines, illness, etc.), where they had used Wi-Fi (e.g., home, work, café, hotel, etc.), and their experiences with the system (e.g., technical or usability difficulties, what they learned, what surprised them, and what discussions, if any, they had about the Wi-Fi Privacy

Ticker). All surveys included multiple choice and open-ended questions and were administered online.

We also collected data logs from the field use. These logs included interactions with the Wi-Fi Privacy Ticker (e.g., changes to the *Watch List*, viewing the *Archive*, or minimizing the *Ticker display*), the types and labels of *Watch List* terms that were set up, how often and to which server *Watch List* terms were transmitted in the clear, the types of networks visited (e.g., wired, open, WEP, WPA, or VPN), and the URLs visited. We used the HTTP Analyzer software<sup>12</sup> to record HTTP request and response headers. The logs were stored in an encrypted database on each participant's laptop and processed locally to filter out sensitive data such as the raw text of *Watch List* terms before transmission to our secure server for analysis<sup>13</sup>. At the end of the study, the software and logs were removed from each participant's laptop.

Finally, we conducted an end-of study interview with each participant either in person or over the phone (average duration: 48 minutes). We used survey responses to guide each interview. Interviews were audio recorded and transcribed. We used open coding [15] to analyze the transcripts and open-ended responses to the surveys. We used custom Perl scripts to parse and analyze log data. Participants were compensated for their participation.

### Participants

Twelve men and five women, aged 28-51, were recruited from our company via a posting on the company's intranet. All were regular Wi-Fi users who used Wi-Fi in multiple places and were willing to run the Wi-Fi Privacy Ticker on their laptop for three-weeks. We recruited from within our company since we were interested in studying attitudes and behaviors of users who have the option of using a VPN to protect themselves when connected to an open network – our company's employees must use VPN to access corporate email and other company resources from outside their offices. An added benefit was that the professionally-supported laptops provided a reasonably uniform and stable system environment for our early-stage prototype.

The 17 participants represented a well-educated population, with 10 having pursued an education beyond a Bachelor's degree<sup>14</sup>. Their areas of study included accounting, business, chemical engineering, computer science, electrical engineering, and health sciences. The study was conducted in November and December 2009. To minimize the potential bias of within-company recruiting, no participants

---

<sup>12</sup> <http://ieinspector.com/> {verified 8 June 2010}

<sup>13</sup> For each *Watch List* term that a participant added, we created an MD5 hash (<http://www.ietf.org/rfc/rfc1321.txt>, ver. 8 June 2010) and transmitted only the hash and associated labels for analysis.

<sup>14</sup> One had a certificate, two had "some college," four had a Bachelor's degree, two had some work at the Master's level, six had a Master's degree, and two had a Doctorate.

**Table 1: Top 10 *Watch List* term types, in order of the number of participants who set up at least one term of the type. Also listed is the total number of unique terms set up per type with a breakdown of the sensitivity levels. Some participants set up more than one term per type.**

Term Type	# of Participants	# of Terms per Type	# of Terms per Sensitivity Level		
			High	Med	Low
Email address	17	28	1	13	14
Password	16	30	19	9	2
Social Security #	14	14	10	3	1
Street address	13	15	2	7	6
Birth date	12	13	3	5	5
ZIP Code	12	14	0	1	13
Last name	11	11	0	5	6
First name	10	16	0	2	14
Username	9	13	2	4	7
Credit Card #	6	11	5	6	0

were recruited from the research branch of the organization to which our lab belongs, knew anyone on the research team, was familiar with the project, or worked in the same site as our lab. In addition, participants held a variety of job types (including accounting, administration, engineering, marketing, research & development, and sales) and were dispersed across eight work sites in six states in the U.S.

### Participants' *Watch Lists*

At the beginning of the three weeks of system use, participants set up *Watch List* terms (they were able to add, edit, or delete terms at any time). The participants set up a total of 186 unique *Watch List* terms with an average of 10.9 terms each (min: 4, max: 21). All participants set up an *email address* as one of their terms; 16 participants set up at least one *password*. In many cases, participants set up more than one term of the same type (e.g., they often set up more than one email address, password, or first name for the system to monitor). Table 1 shows the 10 most popular types of *Watch List* terms set up by the participants.

Nine participants assigned at least one of their *Watch List* terms as having high sensitivity. Not surprisingly, terms of type *password* and *social security number* were most likely to be assigned as high. As Table 1 shows, the assigned sensitivity levels per term type varied, though no *ZIP codes*, *last names*, or *first names* were assigned as "high." Several participants included *Watch List* terms about others (e.g., the names or email addresses of their spouses or children).

### RESULTS

The Wi-Fi Privacy Ticker was generally well received by participants, many of whom asked to continue to run the software after the study<sup>15</sup>. In this section, we present key

<sup>15</sup> Based on these requests, a standalone version of the software that does not transfer any data off the user's machine and does not

**Table 2: Top 10 sites to/from which participants' *Watch List* terms were transmitted in the clear (regardless of network encryption). Actual site names have been replaced with categories, however each represents a single site, where "site" is foo.com, which may have multiple web services such as map.foo.com, search.foo.com, and so on.**

Site	% of Total Matches (out of the 353 sites observed)	<i>Watch List</i> term types matched						
		Email Address	First Name	Last Name	Password	Street Address	Username	ZIP Code
Web search & portal	22.39%	●	●	●		●	●	●
Social networking	21.07%	●	●	●	●	●		
Sports	16.66%	●	●					
Newspaper	6.41%	●						
Company	3.81%		●	●			●	
Airline	2.83%		●	●				
eCommerce (apparel)	2.53%	●	●	●				
eCommerce (technology)	2.09%		●	●				
Manufacturer	1.35%	●	●	●				
Auction	1.34%		●		●		●	●

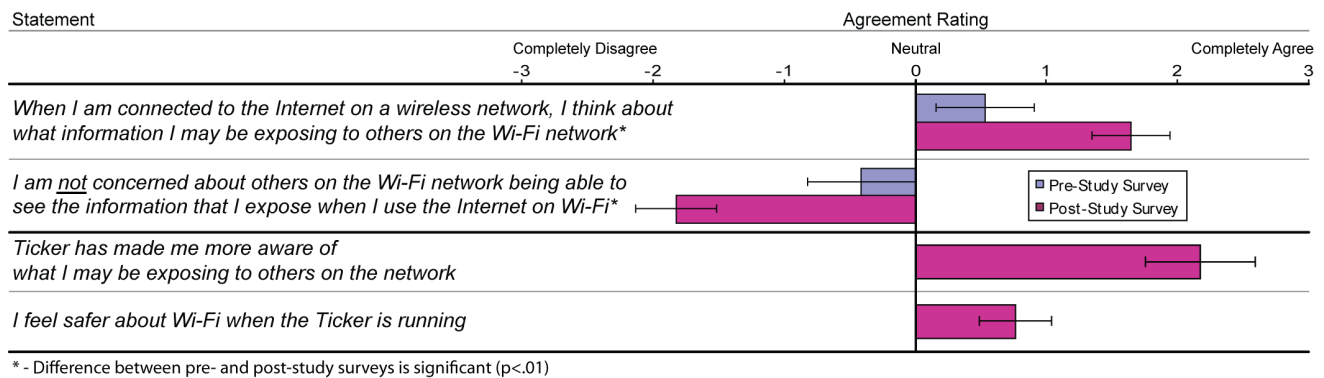
results, focusing on the exposure of participants' *Watch List* terms, their change in awareness, their change in behavior, and their experiences with the *Archive*.

### *Watch List* Term Exposure

During the study, *Watch List* terms were transmitted in the clear 521,181 times across all of the participants. In addition, an average of 1,054 unique search terms (min: 63, max: 3,239) were detected for each participant. However, the number of times their *Watch List* terms were transmitted in the clear varied dramatically per participant (anywhere from 454 to 208,142 times per participant). Upon closer examination, we found that one participant included a company name in his/her *Watch List*; that single term resulted in 128,273 exposures. Even when we discount this outlier, however, a large variance remains because information exposure depends on which websites were visited, how often, and what types of terms were being monitored. Table 2 shows the top 10 unique sites (out of 353 total sites observed) to/from which *Watch List* terms were transmitted in the clear (regardless of network encryption)<sup>16</sup>. Note that our definition of "site" is foo.com, which may offer multiple web services such as map.foo.com, search.foo.com, and so on.

log data that was needed solely for the study (e.g., URLs visited) was made available to participants after the study was completed.

<sup>16</sup> This only counts sites for which the website name was resolved through HTTP-request headers.



**Figure 4. Participants’ average agreement rating with statements about data exposure on Wi-Fi and the effects of the Wi-Fi Privacy Ticker. The top two statements were rated at the beginning and end of the study. The bottom two statements were rated at the end of the study only. The ratings show an increase in awareness by the end of the study.**

We made two important observations from the details supplemented from the HTTP Analyzer logs that we collected for the study. First, personal data was transmitted with high frequency. The primary reason that we observed for this frequency is that the websites in the participants’ logs often included personal data (e.g., email address and/or ZIP code) in the cookie(s) that they set in participants’ browsers. These cookies were embedded in every HTTP request made to the website. Even infrequent visits to a website can result in a large number of HTTP requests, as to fetch each image, script, and sometimes advertisement banner on a single webpage requires a separate HTTP request. Furthermore, many websites (e.g., the *Web search & portal* and *Social networking* sites in Table 2) employed automatic refresh, which triggered the browser to periodically send a request to the website to check for any updates (e.g., a news feed, status updates, or new email).

Second, we observed that many websites sent personal data in the clear. Our analysis revealed that at least 48 sites (i.e., 13.6% of the 353 sites observed) transmitted participants’ email addresses without using any encryption. More alarmingly, participants’ passwords were transmitted in the clear to 11 sites (3.1%). Although some of those exposures could be due to false positives (e.g., for participants who used dictionary words as passwords), we verified that three of the 11 sites encrypt neither the login name *nor* the password. The high frequency of personal data being transmitted in the clear is concerning, as it increases the potential for these data to be sniffed.

### Change in Awareness

Perhaps our most exciting result was that the Wi-Fi Privacy Ticker improved participants’ awareness of the potential visibility of their unencrypted data. As they explained,

[The Wi-Fi Privacy Ticker] *is making me think more about Internet security and what types of data are being shared online but ‘behind the scenes.’* {Participant 10, or ‘P10’}

*I used to think [using the Internet] was like a TV where I just consume content. I didn’t realize the extent to which I broadcast information.* {P12}

*I was not aware of the amount of information we share through the Internet without knowing what information will be exposed and who might be collecting it.* {P14}

In surveys at the beginning and end of the study, participants rated their agreement with two statements concerning attitudes toward information exposure on Wi-Fi. In the final survey, we also presented them with two statements related to the effect of using the Wi-Fi Privacy Ticker. As Figure 4 shows, after having used the Wi-Fi Privacy Ticker for three weeks, participants’ ratings indicated that they thought more and became more concerned about the information that they potentially expose to others on the network than they did at the beginning of the study. A two-tailed paired t-test comparing responses at the beginning and end of the study found that ratings changed significantly ( $t(16)=4.6, p<.001$  for the first statement, and  $t(16)=-3.5, p=.003$  for the second).

Participants’ rating of the statement “*Ticker has made me more aware of what I may be exposing to others on the network*” (with an average rating between ‘Agree’ and ‘Completely Agree’), further highlights the effectiveness of the Wi-Fi Privacy Ticker for increasing awareness. Finally, as the rating of the last statement, “*I feel safer about Wi-Fi when the Ticker is running*” shows, participants felt only moderately that the Wi-Fi Privacy Ticker made them safer. This is, in fact, positive since the system’s focus is to increase awareness and educate, rather than to provide overall safeguards (with the exception of the *Zapper*, which is meant to provide safety for highly sensitive cases).

**Network encryption.** A favorite feature for participants was the always-visible *Wi-Fi Network Status Indicator* (Fig. 1). They commented that connecting to Wi-Fi often happens automatically, and the indicator sometimes revealed that they were not connected to the network to which they thought they were connected (e.g., instead of being

connected to the secure employee network at work, they were on the open guest network). It also helped keep them mindful about what types of online activities were appropriate, given the protection provided by the network (e.g., “It makes me more aware of my connection and if it is safe to be entering passwords, etc.” P2).

**Mental Models.** The *Ticker display* helped participants form more accurate mental models of the circumstances in which data get transmitted. For example, several participants had not understood that data, such as their login name (which is frequently also their email address), ZIP code, or city, were often transmitted via cookie(s) before they logged in or typed in any text fields. For example,

*Websites seem to get my username or email when I'm not logged into them. {P16}*

*...you haven't put anything in or you're not doing anything and then you can see the little thing pop up [a term] and it's like, 'how are they even doing that if I'm not putting anything in?' It's just not something you really think about. {P3}*

Similarly, participants were surprised to learn that their data were often transmitted when they had the browser minimized. Another common revelation was that every character they type into a text field could be transmitted, even before they hit the submit button. For example,

*...every single character as I was typing, it was being transmitted...it was interesting that if I type in something and I backspace out of it and I retype it, <websearch> is basically getting the entire thing of, you know, what's going back and forth in that. So whatever my second thought is or something. {P1}*

Participants were not particularly bothered by this particular exposure and decided that it was how <webSearch> provides search suggestions. However, even technically savvy participants pointed out that they had not thought about how what they were typing could be transmitted before they pressed a button or hit the enter/return key.

The types of data that were transmitted often surprised participants who did not have strong technical backgrounds. However, for the more technically savvy participants, the Wi-Fi Privacy Ticker simply confirmed their suspicions about the types of data that were transmitted. Yet even they were surprised by the frequency of the transmissions. A participant explained,

*I have learned how much information-gathering certain sites are conducting. I knew this was going on, but the amount and frequency of the information was surprising. {P6}*

**The Zapper.** Two participants had terms zapped a total of seven times (four *password* transmissions and three *username* transmissions were zapped). During the interviews, we learned that several participants were not aware of the *Zapper* (including participants who set at least one term as highly sensitive). They did not notice the

description of the *Zapper* where they managed their *Watch List*, and many did not read the documentation that we provided. However, when we described the *Zapper* during the interview, they responded positively.

### **Change in Behavior**

Many participants told us about changes they made when on Wi-Fi as a result of their new and improved awareness. We summarize those changes here, though we point out that these results come from three to four weeks of system use and therefore do not suggest long-term behavior change.

Perhaps the most dramatic change was that one participant upgraded the encryption of his/her home wireless network. However, more representative of the types of changes that participants made were that they started using VPN for certain activities (e.g., “I'm checking my bank account + more sensitive stuff over vpn at home,” P4), they were more careful about the types of networks they used to access certain websites (e.g., “I am sure that I am on my closed home network or on the <company> work network before I access the <newspaper website>,” P8), they did not stay logged in to social networking sites as long as they used to (e.g., “I stay logged into <socialNetworkingSite> for less total time,” P17), and they started to close their browser windows more frequently (e.g., “I make sure to close my browser all the time now,” P16). They were also more cautious of providing their personal data to websites (e.g., “I've been more cautious giving personal information online,” P14) and started to look for evidence of the website providing some protection (e.g., “I pay more attention to sites that have gold locks when personal information is being entered on a webpage,” P15).

Another interesting change was that several participants started to educate their friends and family (and sometimes co-workers) about what they had learned, often using the *Ticker display* to illustrate their points. For example, while visiting friends and family over the U.S. Thanksgiving Holiday, P6 spoke in depth with his/her mother, spouse, and a few friends about “the surprising amount of information that is passed in both directions.”

### **The Archive**

At the end of the study, we asked participants about the *Archive*. Fourteen of the 17 participants opened the *Archive* at least once (it was accessed an average of three times each). For many, the contents emphasized the frequency and amount of data that was being exposed. As P6 described, “I learned how often terms are passed and was shocked.” A technically savvy participant commented,

*There is much more activity on some websites than I expected. It seems a lot of tracking information and advertising uses many different hosts than the one I connected to as the webserver. {P16}*

### **DISCUSSION & FUTURE WORK**

The results from our study revealed improvements in participants' awareness of the potential visibility of their unencrypted communications that led to changes in their

behavior when on Wi-Fi, such as increased attentiveness to the types of networks they were using and what activities were appropriate to perform on those networks.

Throughout the design, development, and evaluation of the Wi-Fi Privacy Ticker, we learned many considerations about developing such systems and opportunities for future work. In this section, we discuss ideas about improving the control mechanism, extending the concept of the Wi-Fi Privacy Ticker, and providing more education to users.

### Improving the Control Mechanism

As mentioned above, we chose to implement the *Zapper* functionality as a kernel driver since it would enable us to easily extend the Wi-Fi Privacy Ticker to work with any network application. However, doing so meant that we were not able to implement one of our design ideas. Following recommendations for improving the design of phishing indicators [2]<sup>17</sup>, upon the detection of a high sensitivity term, we wanted to pop up a window to alert the user of what was about to happen and ask her if she would like the Wi-Fi Privacy Ticker to drop her connection to the website or proceed with sending the term out in the clear. If the user did not respond within a short timeframe, the system would zap the term unless she had specified otherwise in her *Preferences*. Unfortunately, we learned that we were unable to ask the user to individually confirm the zapping of each high sensitivity term, as suspending kernel operation to wait for user action can easily crash the OS.

Because we were not able to implement our original idea, we decided to implement a global rule to always zap high sensitivity terms when on *Open* and *Closed Networks*. However, during the interviews, we discussed options about how to improve the *Zapper*. In general, participants thought that we implemented the *Zapper* in a reasonable way, which could serve as a default, though several participants speculated that they would want the option to set additional rules. Some wanted to specify on which type of network to zap (e.g., *Open*, *Closed*, *Secure*, and/or *VPN*). Others wanted more control, for example, to set rules for individual terms (e.g., zap this particular password on any network, but other high sensitivity terms only on *Open* or *Closed Networks*) or individual networks (e.g., don't zap on my home's *Closed Network*, but zap on other networks). However, as Palen and Dourish have argued, rule-based systems are notoriously complicated [11]. Thus, this remains a challenging opportunity for future work.

### Extending the Ticker Concept

During the interviews, in addition to discussing ways to improve the *Zapper*, we also talked with participants about how to improve the Wi-Fi Privacy Ticker in general. Some participants were interested in the system automatically

detecting when personal data was transmitted, even if they had not added the term to their *Watch List* (e.g., detecting that a password was sent in the clear without the participant having to add that password to his/her *Watch List*). Participants also valued the idea of the system monitoring additional applications such as instant messaging, iTunes, and other browsers (e.g., Safari and Google Chrome). Furthermore, some participants suggested developing a version of the system that could be used by parents to monitor and help keep their children safe on the Internet. They thought that it might be a good compromise between giving their children some autonomy while being responsible parents. With this idea, the parents would want access to the child's *Archive*, be able to set up *Watch List* terms, and potentially even have a copy of the child's *Ticker display* running on the parent's device. A similar idea was raised regarding participants' aging parents.

Other well-received ideas involved changing or augmenting the user experience. For example, one idea was to provide similar functionality as a browser extension, which would enable the system to collect more data on the circumstances in which exposures occur (e.g., information exposure through a cookie sent *prior* to login). Another idea was for the system to expand the types of data it monitors to include files, photos, videos, etc. For example, the system could monitor particular files (e.g., *patriciaBirthday2010.png*) or objects within files (e.g., *files with images containing Patricia's face*). Finally, there was interest in developing a similar system for mobile phones. Such a system would need to monitor data such as GPS coordinates, contact information, and other data stored on/transmitted by the phone (e.g., images and video from the camera, audio from the microphone, etc.). These ideas are opportunities for future work.

### Providing Education

During the intra-study surveys and end-of-study interviews, participants provided feedback about how to improve privacy awareness and control technologies like the Wi-Fi Privacy Ticker. Most notably, participants asked what they could do to protect themselves. As P15 suggested,

*It would be nice to know what to do with the results – stop visiting certain sites, use VPN, what actions should I take to prevent identity theft, phishing, etc.? {P15}*

Some interesting techniques have been developed to educate users about phishing attacks, such as *PhishGuru* [9] which helps users learn how to avoid phishing attacks by enticing them to fall for simulated phishing emails, and *Anti-Phishing Phil* [13] which uses a game to educate users about phishing. These approaches show promise and serve as inspiration for systems like the Wi-Fi Privacy Ticker.

In addition to those recent techniques, ideas that were well received by participants involved the system making suggestions based on the user's activities. For example, the system could suggest terms the user might want to add

<sup>17</sup> Egelman, Cranor, and Hong's [2] recommendations include interrupting the user's task with an active warning, providing clear choices for how to proceed, and failing safely such that the user can only proceed with her task after reading the warning message.

based on what other users find interesting (e.g., *home street address* or *child's name*) or changes the user might want to make to her settings (e.g., if the system detects that her password is being sent in the clear, it could suggest that she change the sensitivity level to “high” so that the control mechanism could provide some protection). Participants also liked the idea of system-provided safety tips. For example if the system detects that a password is sent in the clear, it could suggest that the user make sure not to reuse that password for any “important” sites such as banking or ecommerce. Another idea was to offer a feature that would highlight the elements of a webpage that are encrypted.

Finally, we note that the Wi-Fi Privacy Ticker focuses on data exposure through eavesdropping on the Wi-Fi network. We recognize that there are other possibilities of data exposure along the path, such as data collection by ISPs or service providers. Improving user awareness and control of such risks remains an opportunity for future work.

## CONCLUSION

In this paper, we described the *Wi-Fi Privacy Ticker*, which helps users become more aware of the unencrypted transmission of terms that they have identified as being important to them and outright prevents the unencrypted transmission of terms that they identify as being particularly sensitive. Through the analysis of usage logs, surveys, and interview responses from a three-week field study with 17 participants, we showed that the Wi-Fi Privacy Ticker improved participants' awareness of the circumstances in which their personal information gets transmitted and that this heightened awareness contributed to changes in their behavior while on Wi-Fi. We then discussed opportunities for future work, including ideas about improving the control mechanism, extending the concept of the Wi-Fi Privacy Ticker, and providing more education to users.

Moving forward, we continue to explore how to improve users' awareness of privacy risks associated with the increasingly networked world and ways to provide them with control over their data.

## ACKNOWLEDGMENTS

We would like to thank the study participants, as well as our friends and colleagues who supported this work—particularly Cherie Anderson, Emily Cooper, Pedja Klasnja, Reji Kumar, Anthony LaMarca, Barbara Nelson, Patti Sarr, Anmol Sheth, Josh Smith, and David Wetherall. We also thank the reviewers for their helpful feedback.

## REFERENCES

1. Borisov, N., Goldberg, I., & Wagner, D., “Intercepting Mobile Communications: The Insecurity of 802.11,” *Proc. of MOBICOM '01*, Rome, Italy, (2001), pp.180-9.
2. Egelman, S., Cranor, L.F., & Hong, J., “You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings,” *Proc. of CHI '08*, Florence, Italy, (2008), pp. 1065-74.
3. Friedman, B., Howe, D.C., & Felten, E., “Informed Consent in the Mozilla Browser,” *Proc. of HICSS '02*, Vol, 8, Hawaii, USA, (2002), pp. 247-56.
4. Jung, J., Sheth, A., Greenstein, B., Wetherall D., Maganis, G., & Kohno, T., “Privacy Oracle: A System for Finding Application Leaks Using Black-Box Differential Testing,” *Proc. of CCS '08*, Alexandria, VA, USA, (2008), pp. 279-88.
5. Kindberg, T., Bevan, C., O’Neill, E., Mitchell, J., Grimmett, J., & Woodgate, D., “Authenticating Ubiquitous Services: A Study of Wireless Hotspot Access,” *Proc. of UbiComp '09*, Orlando, FL, USA, (2009), pp. 115-24.
6. Kindberg, T., O’Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D., & Jay, T., “Measuring Trust in Wi-Fi Hotspots,” *Proc. of CHI '08*, Florence, Italy, (2008), pp. 173-82.
7. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B., LeGrand, L., Powledge, P., & Wetherall, D., “‘When I am on Wi-Fi, I am Fearless:’ Privacy Concerns & Practices in Everyday Wi-Fi Use,” *Proc. of CHI '09*, Boston, MA, USA, (Apr 2009), pp. 1993-2002.
8. Kowitz, B. & Cranor, L., “Peripheral Privacy Notifications for Wireless Networks,” *Proc. of the WPES '05*, Alexandria, VA, USA, (2005), pp.90-6.
9. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., & Pham, T., “School of Phish: A Real-World Evaluation of Anti-Phishing Training,” *Proc. of SOUPS '09*, Mountain View, CA, USA, (2009).
10. Maglio, P.P. & Campbell, C.S., “Tradeoffs in Displaying Peripheral Information,” *Proc. of CHI '00*, The Hague, The Netherlands, (2000), pp. 241-8.
11. Palen, L. & Dourish, P., “Unpacking “Privacy” for a Networked World,” *Proc. of CHI '03*, Ft. Lauderdale, FL, USA, (2003), pp. 129-36.
12. Pogue, D., “How Secure is Your Wi-Fi Connection?” *New York Times*, (Jan 4, 2007). <http://pogue.blogs.nytimes.com/2007/01/04/04pogue-email/>, {verified 7 March 2010}.
13. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E., “Anti-Phishing Phil: The Design and Evaluation of a Game that Teaches People Not to Fall for Phish,” *Proc. of SOUPS '07*, Pittsburgh, PA, USA, (2007).
14. Stoll, J., Tashman, C.S., Edwards, W.K., Spafford, K., “Sesame: Informing User Security Decisions with System Visualization,” *Proc. of CHI '08*, Florence, Italy, (2008), pp. 1045-54.
15. Strauss, A., & Corbin, J., *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, SAGE, Thousand Oaks, (1998).