At Least Tell Me: User Attitudes Toward the Inspection of Encrypted Traffic

Scott Ruoti, Mark O'Neil, Daniel Zappala, Kent Seamons
Brigham Young University
Provo, UT 84602
ruoti@isrl.byu.edu, mto@byu.edu, zappala@cs.byu.edu, seamons@cs.byu.edu

ABSTRACT

This paper reports the results of a survey of 1,976 individuals regarding their opinions on TLS inspection, a controversial technique that can be used for both benevolent and malicious purposes. Responses indicate that participants hold nuanced opinions on security and privacy trade-offs, with most recognizing legitimate uses for the practice, but also concerned about threats from hackers or government surveillance. There is strong support for notification and consent when a system is intercepting their encrypted traffic, although this support varies depending on the situation. A significant concern about malicious uses of TLS inspection is identity theft, and many would react negatively and some would change their behavior if they discovered inspection occurring without their knowledge. We also find that there are a small but significant number of participants who are jaded by the current state of affairs and have no expectation of privacy.

Author Keywords

Security, Privacy, SSL/TLS, Notification

ACM Classification Keywords

H.1.2. Models and Principles: User/Machine Systems—*human factors*; H.5.2. Information Interfaces and Presentation (e.g. HCI): User Interfaces—*user-centered design*

INTRODUCTION

Users are largely unaware that some corporations inspect their employee's encrypted traffic to filter malware and viruses, prevent the leak of intellectual property, and block harmful websites. This common practice is usually accomplished with a network device that acts as a TLS (aka SSL) proxy, sitting in the middle of the communication between a browser and web server where it can intercept, decrypt, inspect, then re-encrypt and forward on the user's traffic to its original destination. Users are also largely unaware that their personal firewall software may use the same technique to check their encrypted traffic for malware.

Despite these benevolent uses of this technology, there are a variety of real-world scenarios, ranging from suspicious to malicious, where inspection of encrypted traffic is documented as having occurred.

Reports have notified the public that both Nokia and Lenovo used TLS proxies to decrypt customer (not employee) traffic for reasons other than security. Nokia decrypted cell phone data, allegedly to improve performance on their cellular network [15]. Some Lenovo laptops came with third party software that inserted ads into encrypted data [17]. Weaknesses in the adware implementation left users vulnerable to attack from malicious outsiders. Public outcry caused both companies to stop accessing encrypted traffic.

Government surveillance has been reported to use similar methods [19]. A report from 2011 showed that Iran monitored 300,000 citizens online using a stolen certificate from Diginotar, a company that is trusted to certify legitimate websites [6].

Two recent measurement studies show that TLS proxies account for about 1 in 250 encrypted connections on the web [9, 16]. The vast majority of these monitored connections are for benevolent purposes, but a small percentage appear to be adware, grayware, and otherwise suspicious activity.

The use of TLS proxies is controversial, even among security experts. Some experts are accepting of the practice within corporations because of the necessary benefits to protecting the corporate network. Other experts strongly oppose the practice and consider the TLS system broken because proxies can sit in the middle of TLS connections without user knowledge.

Currently, browsers and users have no method for distinguishing between benevolent and malicious TLS proxies, and the user is entirely unaware that an organization or attacker is intercepting encrypted traffic. Even when a TLS proxy is present, the browsers displays a reassuring lock icon that could mislead users to assume they are communicating directly and securely with the website.

In this paper, we seek to understand user perspectives on the inspection of encrypted traffic. To this end we surveyed 1,976 people across two surveys regarding their

Under submission to CHI 2016.

opinions of TLS proxies. The results of the first survey of 1,049 individuals showed a surprising willingness by participants to accept the inspection of encrypted traffic, provided they are first notified. Based on the results of the first survey, we conducted a second survey of 927 individuals to further explore user attitudes towards inspection of encrypted traffic in specific situations.

Our contributions from these surveys include the following insights:

- User opinions toward TLS proxies are nuanced. Many express concerns about privacy and identity theft from hackers (75.8%) or surveillance by the government (70.9%). Yet there is broad, general acceptance of TLS proxies when used by employers, schools, etc (71.7%).
- Most participants indicated support for inspection of encrypted traffic as long as they were first notified of it (90.7%). Likewise, participants indicated strong support for legislation requiring notification or consent (83.2%).
- When asked about specific situations on the second survey, such as when accessing the Internet at work, a school, a café, or at home, support for TLS proxies ranges from 65% to 90% of participants. This includes those who accept it, those who desire notification, and those who desire both notification and consent. Support for TLS proxies without notification or consent is strongest at elementary schools (45.9%) and at businesses when employees are using company-provided computers (47.9%). In nearly all the scenarios we posed, only a small minority of participants indicate that using TLS proxies is never acceptable. The exception is when the government is conducting surveillance, in which case 47.5% say that this is never acceptable.
- We identify personas based on participants' responses regarding TLS proxies. Three personas have some similarity to the Westin categories [21, 13]: the pragmatic majority (76.5%), the privacy fundamentalist (17.0%), and the unconcerned (1%). Interestingly, a fourth category, the jaded persona (5%) opposes proxies but believes there is nothing they can do to stop the practice.
- Many users would have a negative opinion toward the owner of a network that used a TLS proxy (60.8%), though for some (34.2%) it would depend on who the owner was and how they were using the technology. Some would change their behavior on the network, either discontinuing to use it (17.2%) or changing which sites they visited (6%). Though these latter numbers are somewhat low, these are self-reported through an open response question, so they are likely conservative.

Users want notification when inspection of encrypted traffic is occurring, and the opportunity to give consent or refrain from using the network if they disagree. This represents a challenge for the usable security community to design interfaces that help users make choices that align with their security preferences.

RELATED WORK

There have been prior studies that survey user's attitudes about their online security and privacy. No prior study has looked specifically at user attitudes toward the inspection of encrypted traffic.

Shay et al. [18] surveyed users about their attitude and experience with compromised email or social networking sites. They used Amazon Mechanical Turk and found many respondents gave high quality responses to open response questions. They discussed implications for security mechanism designers. Likewise, our work has significance for the designers of mechanisms to inspect encrypted traffic.

Anton et al. [1] surveyed users in 2008 to see if their attitudes on privacy concerns had changed from the same survey administered in 2002. They found that the top three concerns of U.S. users were information transfer, notice/awareness, and information storage. While the top three concerns had not changed, their level of concern had risen. The top three concerns for European users were the same but in a different order; notice/awareness came in third place. Concerns for notice/awareness are important to both groups, and was a prominent factor in our surveys.

Kumaraguru and Cranor [13] provide a detailed summary of 30 privacy surveys conducted by Westin over a period of many years. It provides the details of several privacy indexes that he created from his surveys. Westin was the first to categorize respondents into the categories of privacy fundamentalist, pragmatic, and unconcerned.

Woodruff et al. [22] examined how well users' classification by the Westin Privacy Segmentation Index predicted their actual behavior. They found that although many participants were classified as privacy fundamentalists, their actions in hypothetical situations were not consistent with this classification. Similarly, we find that even though a significant portion of our participants consider TLS proxies an invasion of privacy, they are still willing to allow the use of TLS proxies because of their perceived benefits. Additionally, while we classify participants into groups with the same names as Westin's categories, we do so by looking at how participants indicate they would react to hypothetical situations and not using any of Westin's several privacy indexes.

We used Amazon Mechanical Turk (MTurk) to recruit survey participants. MTurk has become an increasingly popular method for gathering participant data for usability studies and user surveys [2, 3]. Buhrmester et al. found that MTurk participants are significantly more diverse than typical American College samples and that data obtained from MTurk studies is at least as reliable as those obtained via more traditional methods [4]. Kittur et al. used MTurk participants to classify Wikipedia

entries and found that that they could produce results equivalent to expert raters [12].

TLS PROXIES

In this section we first provide a broad overview of TLS proxies. This description is an exact duplicate of what was seen by the participants in our study. We then give additional technical details about how TLS proxies work.

Basic Description

When you connect to the Internet you do so through some organization's network. For example, at home you connect to your Internet service provider's (ISP) network, while at work you connect to your employer's network. To protect your information from others on the network you can create secure connections to the websites you use (HTTPS). This is done automatically for you when you log into a website. The secure connection encrypts your Internet traffic so that no one else can view or modify your communication with the website (see Figure 11).

Figure 1.

The network you use to connect to the Internet can also be set up to use a system called a TLS proxy. TLS proxies sit in the middle of your secure connection to the websites you view (see Figure 2). At the TLS proxy your Internet traffic is decrypted and the web proxy can view and modify it. Afterwards, the TLS proxy will then re-encrypt your traffic and forward it along. This is done silently and without the knowledge of you or the website you connect to.

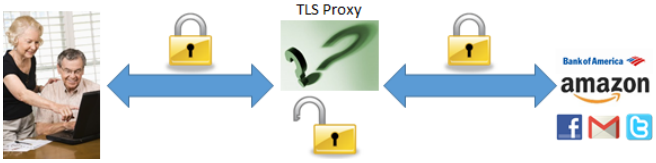

Figure 2.

TLS proxies can be set up by the organization that controls your Internet (for example, your ISP, school, or employer) and also by malicious attackers. TLS proxies have many different uses:

Protective	**Malicious**
Blocking malware and viruses	Stealing passwords
Protecting company secrets	Identity theft
Blocking harmful websites	Tracking government dissidents
Catching malicious individuals	Spying (for example the NSA)
	Censorship

Technical Details

When a web browser attempts to validate the identity of a website, it relies on certificate authorities (CAs) that digitally sign certificates vouching for the identity of servers. Web browsers authenticate a site by validating a chain of trust from the site's certificate back to one of a set of trusted root certificates. These certificates comprise the *root store* and are typically bundled with the operating system or browser.

This validation system is currently being co-opted by the use of TLS proxies that act as a man-in-the-middle (MitM) for TLS connections (e.g., [9]). A TLS proxy can issue a *substitute certificate* for any site the user visits, so that the user establishes an encrypted connection to the proxy rather than the desired web site. The proxy can then decrypt and monitor or modify all user traffic, before passing it along via a second encrypted channel to the desired web site. For example, when a user attempts to create a secure connection to Amazon by requesting Amazon's certificate, the proxy intercepts this request, generates a certificate for Amazon, and sends this substitute certificate back to the user's machine. The user's machine will then create a secure connection to the proxy (instead of Amazon) and send all of its data to the proxy, which has full access to it before forwarding it on to Amazon's servers.

To avoid browser warnings that self-signed substitute certificates would trigger, TLS proxies have substitute certificates signed by a CA certificate that the user's machine trusts. The most common way to do this is to install a new trusted root certificate on the user's machine, either through a custom system image, using an enterprise PKI system, or when a device is manufactured. A malicious individual can use malware to likewise install a new trusted root certificate, or she may gain control of a root certificate authority. A government interested in surveillance may either own a certificate authority outright or have the power to coerce an authority into granting them certificates for domains they do not own [14].

METHODOLOGY

In February 2014, we conducted an online survey of people in the U.S. and India using the Amazon Mechanical Turk (MTurk) crowdsourcing service. Our analysis of the open-ended questions in this survey indicated that participant feelings toward TLS proxies varied depending on the situation in which they were being used. To better understand user preferences in specific situations we conducted a second MTurk survey in February 2015. Our Institutional Review Board approved both surveys. The entire survey and all data and results are available at [redacted].

First Survey

We collected data for our first survey on Wednesday, February 12, 2014 between 7:50 AM and 5:22 PM (PST). Each participant could take the survey once and received

$1 USD as compensation upon completing the survey. In total 1,262 people completed the online survey.

Survey Contents

The survey begins by gathering demographic information. It then instructs participants about TLS proxies and their uses, both benevolent and malicious (see **Brief Description**). Participants were then asked to share their opinions. These questions surveyed participant opinions as to whether TLS proxies were a breach of their privacy and whether there were acceptable uses for TLS proxies. Participants were also asked their reasoning for why TLS proxies should or should not be allowed. Lastly, participants were asked which parties they were concerned about using TLS proxies and what, if any, measures should be used to regulate their use. We then queried participants as to how they would personally react to having a TLS proxy on a network they use to connect to the Internet. This section included two open-ended questions, the first asking them what concerns they might have and the second asking them how it would affect their opinions of the organization running the TLS proxy. Finally, participants were given a chance to express any remaining comments they might have.

Survey Development

Our primary concern in developing the survey was to help users understand the uses of TLS proxies on a non-technical level. We used language that was informative and neutral in tone, allowing participants to form their own opinions. In preparation for writing the description of TLS proxies, we examined the literature but existing descriptions of TLS proxies were not neutral in tone and would unduly bias participants. We talked with businesses that sell proxies (i.e., Blue Coat, Symantec) and read opinions from privacy advocates to better understand both sides' opinions. Based on the information in these sources, we composed a draft of our description of TLS proxies and tested the quality of this description using a convenience sample of six individuals from our university who were not a part of our research group to ensure it was balanced and understandable. Based on feedback from the convenience sample, we updated our description of TLS proxies. We then conducted a pilot survey using MTurk to ensure that we would get meaningful and thoughtful results. This pilot survey was IRB approved and included 80 participants. Responses from the pilot survey are not included in our results.

Qualitative Data Analysis

To better understand participants' opinions regarding TLS proxies and to avoid biasing their responses, we included several open-ended questions in the survey. For each question, we created a codebook to categorize participant responses. One researcher reviewed all the participant responses and created the initial codebooks. The codebooks were then modified through discussion with the coders.

After coding was completed, all of the coders met together to discuss the data. As part of this discussion they were encouraged to identify themes that they had seen in the data. Particular attention was paid to the themes that they felt the codebook did not adequately cover. Coders also shared responses that they felt best represented the various viewpoints expressed by participants.

In total, there were seven coders that analyzed the data. We validated the consistency of the coders using Fleiss' Kappa [5]. Coders' agreement ranged from "substantial agreement" to "almost perfect agreement" (with kappa values ranging from .687 to 1, mean of .865 and median of .833).

Quality Control

To ensure participants provided valid data, we accepted only participants that had previously completed 1,000 tasks on MTurk with an overall task approval rate of 95% or higher. Second, the seven coders examined participants' responses to open-ended questions in order to ensure that participants had both understood the description of TLS proxies and remained on topic. We validated the consistency of the coders' choice to exclude participants' responses using Fleiss' Kappa [5] and found that coders were in perfect agreement (kappa value of 1). A participant's responses were discarded if their answers were clearly spam, such as copying the text of a Wikipedia page, or they did not understand the questions being asked. In total, we excluded 153 participants' responses (12.1%) from the first category and 60 participants (4.8%) from the second. The remaining 1,049 participants' responses constitute the results of our first survey.

Second Survey

We collected data for our second survey on Tuesday, February 24, 2015 between 11:02 AM and 1:06 PM (PST). Each participant could take the survey once and received $1 USD as compensation upon completing the survey. The survey begins exactly as the first survey by gathering demographic information and then instructing participants about TLS proxies and their uses, both benevolent and malicious. Participants are then asked their opinions regarding the use of TLS proxies by various organizations. In total 1,005 people completed the online survey.

Study Description

The first portion of the second survey includes the same description of TLS proxies as the first one. It then asks several questions repeated from the first survey: whether TLS proxies are an invasion of privacy and whether there are acceptable uses for TLS proxies.

The main portion of this survey asks participants their opinion regarding different situations where TLS proxies may be used, such as by an employer, at a school, or a café with free WiFi. The full list of scenarios is listed in Figure 4. For each situation, participants are asked whether the organization should be allowed to run a TLS proxy, with responses taken from (1) *No*, (2) *Only if I*

	Survey 1	Survey 2
Country		
United States	86.9%	94.3%
India	11.5%	5.7%
Other	0.3%	N/A
Gender		
Male	61.1%	60.6%
Female	38.6%	38.9%
Prefer not to answer	0.3%	0.4%
Age		
18–24 years old	18.7%	17.8%
25–34 years old	47.0%	45.8%
35–44 years old	19.6%	21.8%
45–54 years old	8.6%	7.9%
55+ years old	5.8%	6.3%
Prefer not to answer	0.3%	0.4%
Relationship		
Single	59.5%	60.9%
Married	35.5%	35.6%
Other	4.7%	2.7%
Prefer not to answer	0.6%	0.8%
Children		
Yes	36.6%	32.5%
No	62.3%	67.2%
Prefer not to answer	0.9%	0.3%
Education		
No diploma	1.0%	0.6%
High school	12.4%	11.0%
Some college or university credit	28.9%	29.3%
College or university degree	49.9%	50.5%
Post-Secondary Education	7.6%	8.4%
Prefer Not To Answer	0.2%	0.1%
Knowledge		
No Knowledge	4.6%	2.6%
Somewhat Knowledgeable	35.7%	32.4%
Mildly Knowledgeable	42.4%	47.8%
Highly Knowledgeable	14.4%	15.2%
Expert	2.4%	1.8%
Prefer Not To Answer	0.2%	0.2%

Table 1. Participant demographics

consent, (3) *Only if I am notified (consent not required)*, (4) *Yes (neither notification nor consent required)*, or (5) *Unsure*. To choose the situations, we used responses from open-ended questions in the first survey, along with suggestions from our research team to fill out the list.

Quality Control

To ensure participants provided valid data, we accepted only participants that had previously completed 1,000 tasks on MTurk with an overall task approval rate of 95% or higher. Second, the seven coders examined participants' responses to open-ended questions in order to ensure that participants had both understood the description of TLS proxies and remained on topic. We discarded participants whose responses were clearly spam or who incorrectly answered a validation question. We used a validation question in the second survey because there were not enough open responses to always distinguish spam entries. In total, we excluded 78 participant's responses (7.8%). The remaining 927 participant's responses constitute the results of our second survey.

Demographics

The demographics for the participants in both surveys are shown in Table 1. Most participants were from the United States (87% and 94%), with the rest primarily from India. Note that the first survey was open to anyone in the world, with 1.5% participation from other countries, while the second survey was open only to residents of the United States or India. Although results from a previous paper suggested that MTurk participants from India are less concerned with privacy [10], the results from our first survey found that they were more likely to report privacy concerns in our first survey than their counterparts from the United States of America ($\chi^2[2, N = 1049] = 12.35, p < 0.01$).

Participants in both surveys were skewed towards males (61% in both), and ages were centered around 25–32 (46% and 47%). Most participants were single (60% and 61%) and had no children (62% and 67%). Nearly all participants had completed high school, with the majority having completed some level of higher education (57% and 59%).

Participants were asked to self-report their level of knowledge of Internet security, with most rating somewhere between somewhat knowledgeable and mildly knowledgeable (78% and 80%).

After reading the description of TLS proxies, participants were asked whether they had prior knowledge of TLS proxies. In the first survey, most participants reported having little to no awareness of TLS proxies before the survey: unaware (66.5%), unsure (8.1%), aware (25.4%). In the second survey, more participants reported being aware of proxies beforehand (the difference is statistically significant, $\chi^2[4, N = 1976] = 60.003, p < 0.001$), though over half still reported having little to no awareness of TLS proxies before the survey: unaware (50.5%), unsure (13.2%), aware (36.3%). In both cases, we speculate that, due to the effects of illusory superiority, the number of participants that were unaware of TLS proxies before the survey was even higher than reported [7, 8]. Additionally, participants may have conflated knowledge of traditional web proxies with knowledge of TLS proxies.

RESULTS

In this section we discuss the results of our surveys in four areas: acceptable uses for TLS proxies, acceptance of TLS proxies in specific scenarios, general concerns toward their use, and the reaction participants would have if they discovered a network they use employed a TLS proxy. The full survey data is available at [redacted].

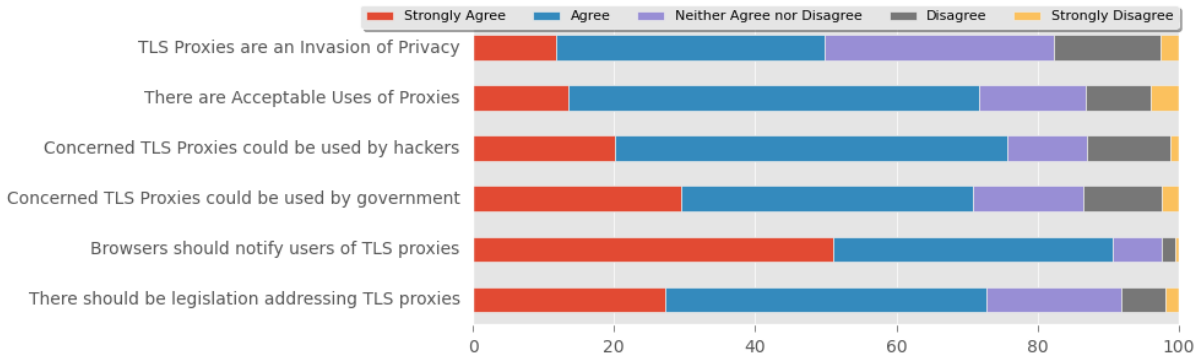

Figure 3. Participant attitudes toward TLS proxies, first survey (N=1,049)

Opinion	Participants
Acceptable Uses	
Protect organizations	51.4% (n=539)
Protect individuals	34.8% (n=365)
Law enforcement and surveillance	8.9% (n=93)
Censor content	7.1% (n=75)
Never censor content	3.1% (n=32)
Acceptable at work, not at home	2.9% (n=30)
Concerns	
Hackers and spying	60.5% (n=635)
Privacy and identity theft	55.4% (n=581)
Done without knowledge or consent	13.2% (n=138)
Reactions	
Negative	60.8% (n=638)
Positive	5.0% (n=52)
Depends	34.2% (n=359)
Suspicious	25.8% (n=271)
Discontinue use	17.2% (n=180)
Change behavior (besides discontinue)	6.2% (n=65)

Table 2. Qualitative response categorization, first survey (N=1,049)

Acceptable Uses of TLS Proxies

Figure 3 shows participant attitudes toward proxies from the first survey. A somewhat surprising result is that participants largely (752; 71.7%) felt that there were acceptable uses for TLS proxies This feeling prevailed even though nearly half of the participants (522; 49.8%) indicated that TLS proxies are an invasion of privacy, and only one-eighth of participants (185; 17.6%) felt they presented no invasion of privacy. There is a strong correlation between thinking TLS proxies were an invasion of privacy and believing that there were not acceptable uses for them ($\chi^2[4, N = 1049] = 141.50, p < 0.001$). Nevertheless, over a quarter of participants (297; 28.0%) felt that TLS proxies were an invasion of privacy, but still had acceptable uses.

To better understand what uses might be acceptable, we asked participants who felt there were acceptable uses to enumerate those uses in an open-ended question. The results from our coded responses are shown in the top part of Table 2. The acceptable uses are largely concentrated on three use cases:

1. **Protecting organizations (493; 65.6%).** Many participants felt that organizations (e.g., businesses, government agencies, schools, libraries) had a right to protect their own intellectual property and security. This included protecting the company from viruses, hackers, filtering inappropriate or potentially malicious websites, and preventing the leak of sensitive information. Participants mentioned that since these organizations provide the Internet for their employees or constituents they had a right to use TLS proxies on their own networks.

2. **Protecting individuals (339; 45.1%).** Participants saw value in businesses using TLS proxies to protect their customers. This protection came in one of two forms:

   - **Direct.** Antivirus applications and firewalls could use TLS proxies to filter malware and viruses. Similarly ISPs, could use TLS proxies to detect and prevent phishing attackers and block other inappropriate or malicious websites.
   - **Indirect.** Participants recognized that they have a significant amount of private information stored externally on the web (e.g., at Amazon or Google). In order to protect this data, participants hoped that the companies storing their private data would employ TLS proxies internally to ensure the safety of the customer's data.

Note that the second of these cases may result from some misunderstanding of the purposes and uses of TLS proxies. Companies often do use intrusion detection systems to protect sensitive customer data, but this is not a typical use case for a TLS proxy. Our second survey better clarifies user attitudes toward particular uses of TLS proxies.

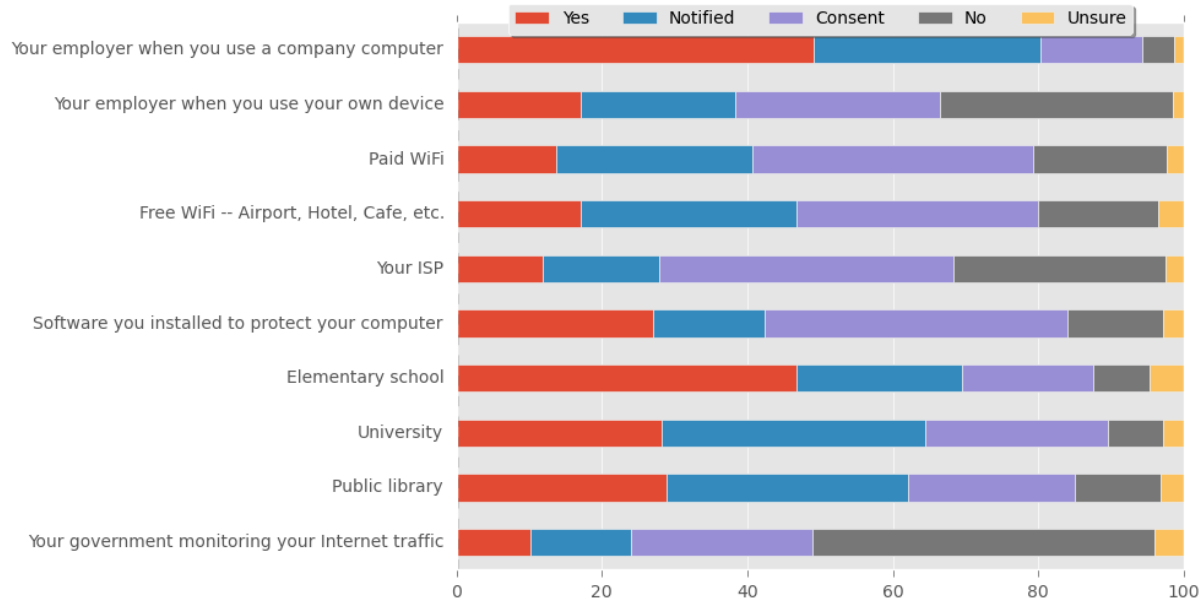

Figure 4. Participant responses toward TLS proxy scenarios, second survey (N=927)

3. **Law enforcement and surveillance (65; 8.6%).** Nearly a tenth of participants expressed that law enforcement agencies should also be allowed to use TLS proxies. This includes use by local or federal agencies to track criminal or terrorist activity. Several participants also expressed that while this was a legitimate use it should only be done with a valid warrant or if there was an imminent threat to national security.

Scenarios

Because these responses were taken from an open-ended question, they represent a conservative measurement of these acceptable uses. To better clarify user feelings in this area, we formulated the second survey to ask users about a series of specific scenarios where a TLS proxy could be used. For each situation, participants are asked whether the organization should be allowed to run a TLS proxy, with responses taken from *No*, *Only if I consent*, *Only if I am notified (consent not required)*, *Yes (neither notification nor consent required)*, or *Unsure*. Figure 4 shows these results.

Users are generally willing to accept the use of TLS proxies in most situations, with acceptance ranging from 65% to 90% of participants, when summing together those who accept it, those who desire notification, and those who desire both notification and consent. For both employers (when you use your own computer) and elementary schools, the support for using TLS proxies without notification or consent from users is surprisingly strong (455; 49.1% and 434; 46.8%). This may be due to a belief in employer rights in the first case and a desire to protect children in the second case. In both cases there is still strong support for either notification or consent (419; 45.2% and 377; 40.7%).

The strongest objections to any kind of TLS proxy are for government monitoring (437; 47.1%), using your own device at work (297; 32.0%), or using your own ISP (271; 29.2%). Note these latter two map to situations where the user has paid for the device or for network access. Users have stronger objections to TLS proxies when they pay for network access through a home ISP than when they pay for WiFi when they are away from home.

When examining the differences among opinions for notification versus consent, we see that the preference for consent is higher for personal firewalls (software you installed to protect your computer), your ISP, free WiFi, paid WiFi, and using your own device at work. The preference is higher for notification for a public library, university, elementary school, and using a company computer at work. This seems to be a clear split that favors consent in cases where the user feels in control versus notification when an organization is in control. The strongest support for consent is with a personal firewall (385; 41.5%), your ISP (375; 40.5%), and paid WiFi (358; 38.6%).

Concerns

Even though many participants in the first survey saw acceptable uses for TLS proxies, they were not without concerns or reservations. Based on our coding, we grouped these concerns into the categories shown in the middle part of Table 2. Three-quarters of the participants (795; 75.8%) mentioned they worried about hackers and nearly as many were concerned about the possibility for governmental spying (743; 70.9%). There was also a strong correlation between the concern that hackers could use TLS proxies and that the government could use them ($\chi^2[4, N = 1049] = 194.57, p < 0.001$).

The most visceral concerns were related to the breach of privacy. One of the open response questions asked participants to list what possible concerns they had regarding the use of TLS proxies. Over half of participants (581; 55.4%) mentioned they were concerned with a loss of privacy and personal information. Nearly a tenth of participants (104; 9.91%) mentioned having their identity stolen, and even more participants had answers that addressed the issue of identity theft generally. A non-negligible number of the participants freely shared that either they, a family member, or other acquaintance had been the victim of account compromise. Similar to the finding of Shay et al. [18] this was a traumatic experience and it left participants especially concerned that TLS proxies could be used to perpetuate identity theft. R208 shared,

> *"A major concern that I would have would be the security of my personal and financial information. I have many friends who have been victims of identity theft and fraud, and would hate to have to go through what they did."*

Participants were also concerned that TLS proxies could be used without their knowledge. One-eighth of participants (138; 13.2%) mentioned in the open response question that they were concerned with privacy. Furthermore, when directly asked about notification, an overwhelming majority of participants (951; 90.7%) asserted they wanted to be notified by their browsers of the presence of TLS proxies. Similarly, participants largely (942; 89.8%) felt that there should be legislation concerning TLS proxies. Most (782; 74.5%) wanted legislation to require notification, and nearly as many (701; 66.8%) wanted legislation to require consent.

Reactions

Participants in the first survey had varied responses on how they would react to learning that they currently use a network that employs TLS proxies. Based on our coding, we grouped these concerns into the categories shown in the bottom part of Table 2. Over half of participants (638; 60.8%) mentioned that it would negatively affect their opinion of the owner of that network. For example, R77 stated,

> *"I would be angry and would feel that organization violated my trust. I would wonder what information that organization had been collecting on me and what they planned to do with it. If it was my employer, I also would think that organization did not trust me and would consider working somewhere else."*

Still, a third of participants (359; 34.2%) said that their reaction would depend on who the owner of the network was and how they were using the proxy. For example, if the owner of the network was their employee they would not have a negative reaction, but if it was their ISP or government they would be very unhappy. Participants also mentioned that their approval would rest on whether or not any personal information was collected and/or sold and whether their consent had first been obtained. R960 explained,

> *"It would be on a case by case basis. I can see some instances where it would be understandable, but if it was going on without my consent, I would be wary of dealing with them in the future."*

Participants also mentioned ways in which their behavior would change if they learned a network was employing a TLS proxy. A quarter of participants (271; 25.8%) said that it would make them suspicious of the owner of that network. A quarter of participants (245; 23.4%) also mentioned that they would change their behavior on that network. For some participants (180; 17.2%) this included discontinuing use of the network and its services, while others (65; 6.2%) mentioned they would change the content they looked at on the Internet or be more careful about entering personal information, including but not limited to e-commerce transactions. At the extreme, some participants mentioned they would quit their job if they found that their employer's network used a TLS proxy. For example, R127 expressed,

> *"If my employers were secretly spying on my private data, I would sue them if legally possible, and quit the job regardless."*

PERSONAS

As our research group discussed the answers to open response questions in the first survey, it became clear that the participants could be classified into one of four personas: *pragmatic majority*, *privacy fundamentalist*, *jaded*, and *unconcerned*. One of the coders classified each of the participants into one of the four personas based on the responses to the open-ended questions, and the percentages of participants in each category are shown in Table 3.[1] A second coder was used to verify the first coder's work, and in the test set (70 participants) they had perfect agreement with a Kappa value of 1. It was only after creating these classifications and categorizing each participant that we realized they bore some similarity to the personas that Westin formulated in a series of studies [21]. Westin classified roughly 57% of participants as being part of the pragmatic majority, 25% as privacy fundamentalists, and 18% as unconcerned. The jaded persona we identify is not present in Westin's studies.

Pragmatic Majority, N=802

The pragmatic majority weighed consumer benefits and protections of public safety against costs of intrusive practices, believed that organizations should earn the public's trust, and wanted to have the opportunity to opt-out of intrusive practices. This group was strongly correlated with being more likely to feel there were

[1]There were ten participants whose answers were vague enough that we did not feel comfortable classifying them as any of the personas.

Persona	Number	Percent
Pragmatic majority	802	76.5%
Privacy fundamentalist	178	17.0%
Jaded	48	4.6%
Unconcerned	11	1.0%
Unclassified	10	1.0%

Table 3. Participant persona categorization (N=1,049)

acceptable uses for TLS proxies ($\chi^2[4, N = 1028] = 230.48, p < 0.001$). As expressed by R93,

> *"I think it is perfectly acceptable for organizations (companies, schools, libraries, etc.) to use TLS proxies because it protects their computers. It keeps hackers from getting to sensitive or confidential information of the organization. In addition, it blocks harmful viruses that can cause a lot of damage and expense in repair. It can also keep individuals from accessing websites (employees from playing online games or minors from accessing pornography). It is perfectly reasonable for companies to employee this device for these purposes when an individual is using their computer. We should not expect privacy when we are using someone else's computer."*

Though the pragmatic majority all weighed consumer benefits versus intrusive practices, they were not uniform in their conclusions about where and how TLS proxies should be used. Some recognized the right of employers to use them, while others believed they should only be allowed in narrow cases such as with a warrant.

Privacy Fundamentalist, N=178

The privacy fundamentalist was generally distrustful of organizations that ask for personal information, in favor of legislation enhancing privacy, and chose privacy controls over consumer benefits when a trade-off existed between the two. Participants classified in this group were strongly correlated with being more likely to feel TLS proxies were an invasion of privacy ($\chi^2[4, N = 1028] = 114.81, p < 0.001$). These participants were also more likely to support legislation addressing TLS proxies ($\chi^2[2, N = 1028] = 14.40, p < 0.001$).

The defining feature of the privacy fundamentalists was that they viewed privacy as so important that it could not be traded for any benefit, no matter how great. As emphatically stated by R1119,

> *"I believe privacy is sacrosanct and one could argue that it's a Constitutional right."*

They were also likely to relate the use of TLS proxies to more traditional methods of surveillance such as wiretapping and intercepting mail.

Jaded, N=48

Jaded individuals were aware that violations of privacy happen regularly, believed that governments conduct surveillance on the general public, and had lost hope that they can have privacy online. These participants felt that "the system" was rigged to remove any real chance of them having privacy. For example, R713 expressed,

> *"I know that it is my choice to use the internet; however, since I live in a remote area with no transportation to the nearest city (30 miles away) I am 'stuck' working and banking and doing business on the internet. I feel it is unfair to be made to choose between being 'safe' and having privacy freedom. I am especially disgusted by our government's spying behaviors and the rhetoric about it being necessary for national defense."*

Likewise, when asked about concerns regarding the use of TLS proxies, R831 shared,

> *"None. The government (via the NSA) is already reading everything we do and share online. So no surprises there."*

Other jaded participants felt they had no choice in the matter because in the United States Internet service providers often have a monopoly.

Unconcerned, N=11

Unconcerned participants were generally trustful of organizations that ask for personal information, willing to sacrifice personal privacy to obtain consumer benefits, and not in favor of legislation to protect or enhance privacy. In our study, we found very few unconcerned participants (1%). It is possible that the recent news regarding widespread government surveillance caused participants to be more privacy aware and sensitive. In addition, our use of qualitative data to classify participants allowed us to recognize that participants were part of the pragmatic majority even when their Likert responses might seem to indicate otherwise.

DISCUSSION

A number of interesting themes emerged as we read the participant responses to open-ended questions.

Informed Participants

Most of the participants showed a high level of engagement in the survey. At the end of the survey when asked if they had any additional comments, a large number of participants mentioned that they were thankful that we had informed them of this information. Some even asked where they could get more information on the topic of TLS proxies. We were impressed with the in-depth analysis of trade-offs that many users shared.

Recognition of Trade-offs

Participants clearly understood that there were trade-offs involved with the use of TLS proxies, weighing the benevolent uses for schools or workplaces and the danger of misuse by insiders or by hackers. As they struggled with this trade-off, participant responses indicated confusion, doubt, worry, equivocation, and reasoned conclusions. Confusion regarding how to resolve the conflict

was evident when participants labeled it a "grey area." R988 considered both good and bad uses and worried

> *"How are you supposed to know which is happening?"*

Fear of identity theft was widespread. Some participants weighed the trade-offs and resolved the dilemma by deciding that proxies should only be used by consent. For example, R827 expressed,

> *"I believe that TLS proxies are an invasion of privacy, as is anything that monitors my internet usage without my permission. However if you are using someone else's (like a company's) network, they have every right to make the rules of use... This is one of those doubled-edged swords – it can be used for your good and security and it can be used to harm and spy on you. Because of the distinct possibility of lost privacy, this type of proxy should [not be] used, except by your agreement, not by anyone else."*

Others wanted companies or schools to be able to use TLS proxies for security purposes, but also wanted to prevent them from being used for government surveillance or by hackers. Still others felt TLS proxies should *only* be used by the government to catch terrorists or criminals.

Notification and Consent

Numerous participants expressed a desire for notification and consent when TLS proxies were being used on a network. A typical response as given by R413 was,

> *"Well for some things it would be understandable, I'd just like to be informed so I know the risk I'm taking."*

R313 expressed,

> *"If I encrypt something no one has the right to unencrypt it unless I give them the right to - simple as that."*

Participants expressed extreme distrust for those who would use TLS proxies without informing users, going so far as to say they *"would hate them," "would wonder what they are looking for,"* and *"would assume they were up to no good."*

Others stated they would change their behavior if notified about a proxy, such as avoiding commercial transactions, using a VPN to circumvent a proxy, or self-sensoring their Google searches and other online communication.

Jaded Participants

We were surprised to find that 4.5% of participants were jaded towards the current state of affairs. They felt that using the Internet today involved giving up any security or privacy in the face of anybody determined enough to conduct surveillance. Many felt that the government was already spying on everything, and that even if TLS proxies did not exist the government would just find another way to gain access to their private information. Others felt that they have no recourse if they discover a TLS proxy because their access to the Internet is controlled by a monopoly.

We find this group concerning, as this is not a group of individuals unconcerned with security and privacy. Rather they are a group that once cared about these issues but has lost all hope and has largely given up on ever achieving a secure world. Developing security solutions that help people trust that their privacy is being safeguarded is a major challenge to the usable security community.

LIMITATIONS

MTurk has known biases, but is still a mostly reliable platform for rapidly obtaining results related to user sentiment [20, 11, 3]. Participant demographics were slightly skewed towards a younger male population and nearly all participants were from the US and India. Surveys of participants from other countries would be useful, but would need to be conducted by researchers intimately aware of cultural perceptions in those areas.

Our two surveys used different populations and the second survey occurred one year after the first. In the second survey, more participants reported being aware of TLS proxies before taking the survey. It is unclear how this difference might have affected the second results, and care should be taken when trying to directly compare trends in the first and second surveys.

All of our data is self-reported, and as such carries with it inherent participant bias. The continuing news coverage of leaked NSA documents may have influenced user answers.

CONCLUSION

This paper presents the first survey of user attitudes toward TLS proxies. Responses indicate that participants hold nuanced opinions on security and privacy trade-offs, with most recognizing legitimate uses for the proxies, but concerned about threats from hackers or government surveillance. A significant concern about malicious uses of TLS inspection is identity theft, and many would react negatively and some would change their behavior if they discovered inspection occurring without their knowledge. We also find that there are a small but significant number of participants who are jaded by the current state of affairs and have no expectation of privacy.

There is strong support for notification and consent when a TLS proxy is intercepting their traffic. This represents a challenge for the usable security community to design user interfaces that help users make choices that align with their security preferences. One participant (R226) expressed hope for technology meeting these concerns, stating *"I certainly hope smart people are working on this."*

REFERENCES

1. Annie I Antón, Julia B Earp, and Jessica D Young. 2010. How Internet users' privacy concerns have evolved since 2002. *Security & Privacy, IEEE* 8, 1 (2010), 21–27.
2. Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, Saranga Komanduri, and Manya Sleeper. 2011. Improving computer security dialogs. In *Human-Computer Interaction–INTERACT 2011*. Springer, 18–35.
3. Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 6.
4. Michael Buhrmester, Tracy Kwang, and Samuel D Gosling. 2011. Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science* 6, 1 (2011), 3–5.
5. Joseph L Fleiss. 1971. Measuring nominal scale agreement among many raters. *Psychological bulletin* 76, 5 (1971), 378.
6. Eva Galperin, Seth Schoen, and Peter Eckersley. 2015. A Post Mortem on the Iranian DigiNotar Attack. `https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack`. (2015).
7. Arthur M Glenberg, Alex Cherry Wilkinson, and William Epstein. 1982. The illusion of knowing: Failure in the self-assessment of comprehension. *Memory & Cognition* 10, 6 (1982), 597–602.
8. Vera Hoorens. 1995. Self-Favoring Biases, Self-Presentation, and the Self-Other Asymmetry in Social Comparison. *Journal of Personality* 63, 4 (1995), 793–817.
9. Lin-Shung Huang, Alex Rice, Erling Ellingsen, and Collin Jackson. 2014. Analyzing Forged SSL Certificates in the Wild. In *IEEE Symposium on Security and Privacy*.
10. Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the US Public. In *Symposium on Usable Privacy and Security (SOUPS)*.
11. Patrick G Kelley. 2010. Conducting usable privacy & security studies with Amazon's Mechanical Turk. In *Symposium on Usable Privacy and Security (SOUPS)*. Citeseer.
12. Aniket Kittur, Ed H Chi, and Bongwon Suh. 2008. Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 453–456.
13. P. Kumaraguru and L. Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies, ISRI Technical Report CMU-ISRI-05-138*. Technical Report. CMU. `http://reports-archive.adm.cs.cmu.edu/anon/isri2005/abstracts/05-138.html`
14. Moxie Marlinspike. 2011. SSL and the future of authenticity. *Black Hat USA* (2011).
15. David Meyer. 2013. Nokia: Yes, we decrypt your HTTPS data, but don't worry about it. `http://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/`. (2013).
16. Mark O'Neill, Scott Ruoti, Kent Seamons, and Daniel Zappala. 2014. TLS Proxies: Friend or Foe? *arXiv preprint arXiv:1407.7146* (2014).
17. Timothy J. Seppala. 2015. New Lenovo PCs shipped with factory-installed adware. `http://www.engadget.com/2015/02/19/lenovo-superfish-adware-preinstalled/?ncid=rss_truncated`. (2015).
18. Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. 2014. My religious aunt asked why I was trying to sell her Viagra: experiences with account hijacking. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2657–2666.
19. Christopher Soghoian and Sid Stamm. 2012. Certified lies: Detecting and defeating government interception attacks against SSL (short paper). In *Financial Cryptography and Data Security*. Springer, 250–259.
20. Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, and others. 2012. How does your password measure up? The effect of strength meters on password creation. In *Proc. USENIX Security*.
21. Alan F Westin. 1991. Harris-Equifax consumer privacy survey. *Atlanta, GA: Equifax Inc* (1991).
22. Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Symposium on Usable Privacy and Security (SOUPS)*.