Exploring Website Location as a Security Indicator

Der-Yeuan Yu, Elizabeth Stobert, David Basin, Srdjan Capkun
Department of Computer Science, ETH Zurich
{dyu,elizabeth.stobert,basin,srdjan.capkun}@inf.ethz.ch

ABSTRACT
Authenticating websites is an ongoing problem for users. Recent proposals have suggested strengthening current server authentication methods by incorporating website location as an additional authentication factor. In this work, we explore how location information affects users’ decision-making for security and privacy. We conducted a series of qualitative interviews to learn how location can be integrated into users’ decision-making for security, and we designed a security indicator to alert the user to changes in website locations. We evaluated our tool in a 44-participant user study and found that users were less likely to perform security-sensitive tasks when alerted to location changes. Our results suggest that website location can be used as an effective indicator for users’ security assessment.

1. INTRODUCTION
The Internet has become a central medium for global information exchange. Users’ reliance on the Internet for critical services, such as banking, data storage and communication, highlights the importance of data security. However, users currently can do little to ascertain whether their security is ensured and their privacy is respected by online services. For example, it is often unclear whether online firms reveal users’ profiles to third parties, such as advertising firms or government agencies. The risk of personal data leakage requires users to determine, consciously or subconsciously, whether a website is trustworthy enough. This places an extra burden on users since security is not usually their primary goal.

Users’ trust in websites is also strongly tied with the problem of server authentication, currently achieved using public key certificates under the CA/browser model. Browsers typically display a green lock icon to indicate successful authentication or a warning otherwise. Unfortunately, research has found that users frequently ignore or bypass related warnings, making themselves vulnerable to online threats. Users also often fail to notice or comprehend certificate information, which has been addressed with improved interface design. As website impersonation attacks increase, novel mechanisms to strengthen server authentication are being explored. One recent research direction proposes using the server’s geographic location as an additional trust factor. However, the usefulness of website location information depends critically on how it is presented to users and how they in turn perceive and evaluate it. Until now, these questions have been unexplored.

In this paper, we explore users’ decision-making processes regarding their security and how website locations can play a role. Using a user-centered design approach, we gathered requirements, designed a location indicator, and evaluated its usability and effect on user behavior. We conducted semi-structured interviews with 15 participants and applied thematic analysis to identify issues relevant to online trust. Based on our themes, we developed a model to describe the factors in users’ trust and analyzed the role of website locations in their decisions. We found that users’ perception of online security and web authenticity are often intermixed with their concerns about privacy. The participants often assessed their security on a conceptual level by gauging their risks in terms of financial security and personal privacy. We also found that participants, while describing various trust concerns in their online security, expressed preferences for particular locations when dealing with sensitive information or transactions. These findings suggest that the knowledge of website locations plays a potential role when users make security decisions.

Based on the results of the qualitative thematic analysis, we derived requirements for a location tool to inform users of website locations. We designed and implemented LocationWatch, a Chrome extension that makes website locations available to the users and alerts them to changes in server locations. Using LocationWatch, we conducted a user study with 44 participants to analyze how website locations affect their decision-making processes. Our statistical analysis showed that participants’ decisions were significantly affected by website locations, with fewer users completing sensitive tasks when the website location had changed. The participants’ decisions also varied depending on the sensitivity of data in different scenarios.

The effects of website location knowledge on users’ decision-making processes have not been investigated until now. With recent proposals for strengthening authentication using website locations, it is important to evaluate how this information is perceived by users and how it can be best leveraged.
in their decision-making processes. Our results show that users are sensitive to website locations when informed in a non-intrusive way. This shows the promise of using location information as an additional security factor.

2. BACKGROUND

Current research on location-based website authentication raises the question of how users might leverage such location information in decision-making. Compared to digital certificates, the tangibility of location and its clear relationship to the real world suggests that location can play a role in users’ security and privacy awareness.

2.1 Location-based Decision-Making

Psychological research on decision-making has found that people tend to underestimate risk. Since safety and security are abstract concepts, users are unmotivated to pay attention to these risks. Research examining how users make decisions about computer security has found that users reason inconsistently about their gains and losses, and are likely to overprioritize the cost of losses [48]. For security, because the gains are abstract and the consequences seem random, users often focus on costs, which are immediate and tangible [15]. Hardee, West, and Mayhorn [24] found that users consider gains, such as protecting information, money, or property, but that they are unaware of risks relating to money and property loss online. Users are also concerned about personal inconvenience in using online services.

Users’ security decisions often serve to protect their personal privacy. Research has found that users’ privacy preferences are context-dependent and can be easily influenced [3]. Users also experience high uncertainty about whether and to what extent they should be concerned about data privacy. Human decision-making can appear inconsistent, but it is governed by a complex calculus of decision-making [32] that factors in additional information such as social norms and emotional responses.

Although other researchers have explored location and privacy for users [9, 14, 25], most existing research has been in the context of having the user share their own location with online services or other parties. Fisher et al. [19] studied iPhone users and found that they used permissions-based access control to limit their location-sharing to certain applications. Patil et al. [30] found that while users were motivated to share their locations for social purposes and in-app rewards, they overwhelmingly desired location-sharing to be explicit. While our work addresses an opposing issue, this research emphasizes the importance of location as a relevant factor in security and privacy decisions.

Little research to date has analyzed users’ perceptions of where their data is stored or to what locations it is transmitted over the Internet. Kang et al. [40] conducted a qualitative study investigating users’ mental models of the Internet and found that users had only a vague understanding of where data is stored online. They also found that factors such as reputation and appearance were likely to influence users’ perceptions of what was happening to their data. Ion et al. [26] interviewed users about their data privacy awareness and their attitudes about where their online data should be kept. They found that users generally preferred sensitive data to be stored locally than uploaded to cloud storage. They also identified cultural differences that affect users’ understanding and preference for their online privacy. A large-scale study of website credibility [29] found that websites were more believable when they communicated the “real world” aspect of the organization, were professional and easy to use, and included indicators of trustworthiness.

It remains unexplored how users might integrate information about the website’s location into their evaluation of these environmental cues.

2.2 Website Location and Authentication

Web authentication is currently achieved using TLS, which requires the server to have a valid X.509 public-key certificate. The client’s browser must validate this certificate upon connection to the server by checking a certificate authority’s (CA) signature and other fields. However, recent incidents have demonstrated the weaknesses of the public key infrastructure against a strong adversary [35]. More specifically, attackers have been able to compromise CAs to obtain a fraudulent certificate of an arbitrary website to impersonate it. Such attacks have been addressed by a wide range of enhancements to TLS authentication, such as Certificate Transparency [31], pinning [12], etc. We refer the reader to a more thorough treatment on TLS authentication by Clark and van Oorschot [13]. Despite the improvement to certificate validation, a strong attacker may still be able to compromise a web server and obtain the private key associated with the public key used in its certificate, e.g., by exploiting TLS implementation bugs [4] or zero-day vulnerabilities. In these scenarios, server impersonation attacks can subsequently be performed remotely by the adversary that controls the network.

As one of the approaches to strengthen server authentication, recent work has proposed using website location as an additional authentication factor. Conceptually, verifying a website’s location during authentication detects remote server impersonation attacks resulting from the compromise of CAs or websites’ private keys. Yu et al. explored the use of location in addition to digital certificates to authenticate servers in TLS handshakes [50]. This approach requires a trusted party to estimate the location of a website server and issue a signed statement binding the server location to a particular connection with the client. The browser can either perform automatic verification (e.g., during the TLS handshake) of the location information or directly display it to the end user. Abdou and van Oorschot proposed similar methods of augmenting TLS by actively estimating website locations using delay-based measurements from multiple locations [2]. Both works propose the concept of integrating website location into server authentication and detect location changes. These approaches essentially leverage the uniqueness and verifiability of private web server locations to supplement certificate-based server authentication.

The use of location as an authentication factor is increasingly possible due to the availability of pervasive location information, IP geolocation services, and general localization techniques. A non-technical approach to website localization is the use of public ledgers to record and make available the location of data centers. Online services often host their web servers in data centers, whose locations are known in public. For example, online resources such as Data Center Knowledge [37] provide a public listing of data center deployment and news about web hosting companies. Com-
panies are also increasingly disclosing their server locations to the public \(^6\)\(^{22}\), and using on-site security to protect critical online services from physical intrusion by malicious parties \(^{23}\)\(^{16}\). In addition to out-of-band channels, CAs can also verify the locations of online firms and store them in Extended Validation (EV) certificates \(^{12}\) as part of the Subject field, which can be extracted by the browser.

Commercial IP geolocation solutions (e.g., MaxMind \(^{23}\), GeoBytes \(^{21}\), IP2Location \(^{27}\), IPigence \(^{28}\), etc.) allow users to query for accurate website locations using IP addresses. These services use public WHOIS databases maintained by regional Internet registrars (such as ARIN \(^{8}\), RIPE \(^{35}\), and APNIC \(^{7}\)). The accuracy of IP geolocation is far from perfect, and each provider uses a different technique. However, the capacity of IP geolocation solutions is limited by the local ISP. Currently, IP geolocation is the most common source of website location data. There also already exist software solutions showing IP geolocation data to users, such as Flagfox \(^{15}\) and IP Whois & Flags \(^{44}\). However, they do not guarantee that the web servers really are at these locations upon client connection. Moreover, while some solutions support other features such as website safety checks and ratings, their impact on users’ security awareness and decisions has not been explored in depth.

3. RESEARCH OVERVIEW

Given the increasing availability of server location information, our goal was to explore how it can be leveraged as part of users’ trust in websites and online services.

Since we aim at evaluating the effect of location verification when presented to users, we adopted the same attacker model proposed in related work on TLS \(^{13}\) and website location authentication \(^{2}\)\(^{50}\). More specifically, we assume that the attacker is able to impersonate the server by compromising its public key certificate. This can be achieved by taking control of a CA to issue a fraudulent certificate or learning the private key associated with a website’s public-key certificate. Since location is used as a unique factor in previous work, we also make the same assumption that the remote attacker is unable to physically co-locate with the victim’s website but resides in a separate location. The attacker’s goals may consist of stealing user credentials (e.g., login information), providing false information (e.g., fake news), or collecting sensitive data (e.g., credit card numbers or private documents). Concerning the use of website location as an authenticating factor, we specifically aimed to answer the following research questions about user behavior.

**RQ1** How do users currently make online security decisions and how could location play a role?

**RQ2** Does having information about website locations affect users’ behavior?

We explored these problems using a user-centered design approach \(^{29}\). To answer **RQ1**, we conducted a series of qualitative interviews and applied thematic analysis to understand users’ decision-making processes for online security. The themes we identified allowed us to develop a model of users’ trust assessment and derive design requirements for a website location tool for a broad range of web users. To answer **RQ2**, we designed a location tool that displays the web server’s location, which we implemented as a Chrome browser extension. Finally, we conducted a user study to evaluate the usability of our location tool and analyze the impact of location knowledge on users’ decisions in real-world application settings. All studies involving human subjects were approved by our institution’s ethics committee.

4. STUDY 1: QUALITATIVE INTERVIEWS

In our first study, we interviewed users about how they currently determine websites’ trustworthiness. Our goal was to understand how location information could fit into users’ current decision-making practices and to identify design requirements for a location indicator.

4.1 Study Design

We chose a semi-structured interview approach to ensure that we covered topics of interest while giving participants the freedom to discuss their decision-making processes and concerns. Our interview covered three areas: Internet use, security awareness, and location-related preferences. We carefully selected topics that might have associated security or privacy concerns for different Internet usage scenarios: online file storage, emails and calendars, online financial transactions (banking and shopping), and social media. For each topic, we asked about how participants used these services, the kinds of data they stored or obtained through those services, and what kinds of security and privacy concerns they had around these activities. Regarding security awareness, we asked participants about their general security and privacy precautions and where they thought Internet data was stored and served from. Because we were interested in the development of a security indicator, we asked about how they currently determine that websites are legitimate or trustworthy. In the final part of our interview, we explained the concept of location as a security indicator, and asked participants how they might use website location information if it were available\(^1\). Our interview script can be found in Appendix A.

Because using location as an website security indicator is a novel concept, we did not expect participants to explicitly identify it during the interviews. We therefore framed our interview broadly and encouraged discussion on a wide range of topics with relevant security and privacy concerns. By eliciting detailed feedback about users’ current decision making strategies, we sought to understand how location is currently perceived and how it can be used in users’ security decisions. Rather than specifically introducing technical concepts of location-based authentication, we introduced topics that naturally led to the subject of location. If participants did not bring up the subject of location on their own, we attempted to steer the conversation in that direction.

We audio-recorded the interviews to facilitate subsequent note-taking and transcription for analysis. Participants also completed a brief demographics questionnaire before the interview. Each interview lasted between 30 and 60 minutes.

4.2 Participants

We wished to represent a diverse array of perspectives in our interviews, so we recruited people of different genders, ages, education levels, occupations, and diverse nationalities. We

\(^1\)To make it easier for the user study participants to understand, we used the term “website locations” in our user studies. We use the terms “website locations” and “server locations” interchangeably throughout the rest of the paper.
4.3 Thematic Analysis

Following completion of the interviews, we reviewed the audio recordings and transcribed each interview. This produced a qualitative dataset that we analyzed using thematic analysis [1], a flexible qualitative analysis methodology that allowed us to identify themes and relationships in the data. We began our analysis with open coding. We traversed and reviewed the transcriptions line by line and assigned codes to recurring ideas. To ensure consistency, each interview was coded by two researchers, and codes were cross-checked to improve reliability.

An example of our open coding process can be seen in the following quote, where a participant was asked about how she verifies website authenticity:

“...I didn’t think of [authenticating websites] before. I think every website will give us some legal documents to read before we give information to them. I will scan the documents.” – P5

We assigned the code lack of awareness to highlight the participant’s lack of concern. Because she mentioned her attention to legal documents, we assigned the code legal concern. We identified 46 open codes in our data, and a complete list can be found in Appendix B. Following the process of open coding, we refined the codes and classified them into themes, described in the subsequent sections. These themes highlight patterns of typical behaviors we observed, rather than representing categories of users.

4.3.1 Trusting by Default

When asked about their online decision-making, many participants described taking the security of websites for granted without much investigation.

“Well, I mean, [website authentication] is not something I think about. You just go to the webpage, it looks familiar, and then it never crosses your mind that it may have been forged.” – P12

We also noticed users’ default approach to trust in the way they described their automatic use of various online services, such as synchronization of data (e.g., contacts and files) across different devices linked to the same platform.

“I think I do use sometimes iCloud. I think it just come automatically with my iPhone. Each two weeks, asking me if I want to store it [...] I think mainly I, I just let it.” – P1

Most participants embraced the convenience of automated functions, such as allowing web email servers to automatically store email addresses of frequent contacts, and took their trustworthiness for granted.

Most participants’ initial approach toward online security was to trust that the default configurations are secure. Few participants mentioned looking out for browser security indicators, such as the lock icon or website certificates. When asked about decision-making, participants did not frequently engage in discussions of security and privacy until potential online risks were specifically brought up. Most participants reported using the Internet by simply trusting the way it is.

“One keeps hearing about Internet security and all this, but unless something happens, you don’t pay a lot of attention to it.” – P12

4.3.2 Having Diverse Areas of Concern

Although their default approach was to view the Internet as secure, most participants were able to elaborate areas of specific concern regarding the security and privacy of their data. Among these areas were concerns about personal privacy, financial safety, and freedom of speech.

Personal privacy was a major concern that was brought up repeatedly during the interviews. Participants discussed privacy concerns about sharing information with both online services and other users of those services (and often conflated these two threats).

“I just kind of like the idea of not being very traceable, not because I’m hiding something specifically but because it’s my own business kind of, where I am, what people I’m seeing. I don’t make my life very public...” – P14

Some participants were aware of data collection by companies, but had decided to ignore the implications, or did not perceive this as a threat.

“As a user, I don’t really see the problem. I mean, okay, [online services] are going to have my numbers, and other numbers, but it doesn’t really affect me.” – P2

However, other participants acknowledged the necessity of disclosing personal information. For example, P5 stated that “sometimes we have to be checked by other people” (referring to public security). Others seemed to regard the purpose of the Internet as being to share information, and said that curtailing this sharing would render their online presence less meaningful.
“If someone knows where I worked, that’s not a problem because it actually helps me connect with other people because they know where I worked.” – P15

Another area of concern that was repeatedly mentioned was financial security. Many participants discussed security concerns around online banking and shopping. For example, many participants declined to allow websites to store their credit card information.

“Never, especially after some information in mass media […] about a risk of misuse” – P11

Regarding freedom of speech, a few participants were concerned about the future consequences of sharing information and opinions online.

“I don’t really trust that [my words] might not one day be used against me… I think a lot of this information is stored and it’s just uncomfortable.” – P14

Some participants take precautionary measures before making online purchases.

“I never trust the information even if the website says that it’s safe to buy there. I always try to think or to ask friends if they have ever bought something in that website.” – P10

4.3.3 Relying on Multiple Trust Factors

When discussing how they decided to trust websites, participants mentioned a variety of factors. Most participants associated website trustworthiness with subjective impressions, such as familiarity of brand presentation, the website interface, and the past experiences of themselves and friends. Even knowledgeable participants admitted to relying on such non-technical cues.

“The first [thing I notice] would be the brand, the logo itself […] does it look the same?” – P2

One major trust factor was the company’s reputation. For example, when asked about why they trust particular storage services, some participants relied on the brand name: “I think having the Apple’s name behind it, it’s quite safe.” (P3) Participants also listed firms like Google and Amazon as their trusted service providers. Many preferred to avoid unknown third-party shopping websites and rely on payment services with buyer protection policies (e.g., PayPal).

In addition to their own previous experiences, participants also relied on experience from friends or website reviews to judge whether websites were trustworthy. These social cues were used to help discern trustworthiness.

“[How do you choose where to shop online?] Um I usually, usually based on the community. I usually read some forums because I never trust the information even if the website says that it’s safe to buy there. I always try to think or to ask friends if they have ever bought something in that website.” – P10

4.3.4 Taking Risks for Practicality

Most participants described clear heuristics for online decision making based on their trust factors and concerns. These included using pseudonyms, providing fake profile information, avoiding saving credit card information on websites, and only buying from familiar vendors.

However, participants often admitted to bending their rules or making exceptions for practical reasons. They often justified decisions by discussing the acceptability or manageability of the potential risks, e.g., a small financial risk when ordering from an untrustworthy merchant. Participants also frequently indicated that their decisions depended on the urgency of the matter at hand.

“If I’m doing stuff on the Internet, I just want it done as fast as possible so I can do something else.” – P14

Compromises were thus often made in the presence of security warnings. Users put themselves in insecure situations (such as by ignoring the website certificate warnings) to ensure convenience and access to online services. In such situations, participants often described a tradeoff between personal security and service accessibility when making their decisions. Though security compromises were made, participants mentioned various secondary measures to reinforce their decisions, such as obtaining tangible proofs of their transactions (“I want to have photocopy or paper as proof” – P1) or contacting customer service.

4.3.5 Helplessness and Learning from Consequences

When discussing their decision-making processes and concerns, participants often expressed frustration over missing information or knowledge that prevented them from behaving securely. Many expressed a kind of learned helplessness relating to their inability to understand security measures.

“[How do you know you are visiting the real website?] I don’t think too much on these things because I don’t know exactly how it works.” – P1

Another aspect of this helplessness originated from users’ inability to affect corporate policy and their lack of control over where sensitive data is stored.

“Yeah like it’s 2016 now. You don’t really have power over [where data is stored] anymore.” – P9

Another participant stated that “a company could say one thing and do another thing” (P2), suggesting their lack of control and distrust in the honesty of companies.

However, though participants expressed a lack of contentment about not being able to control the security of their information, they also mentioned that having that control could be a burden to them.

“If location would be available for me, I would have a feeling that from that time I am the one who has to be responsible for that.” – P7
4.4 The Process of Decision-Making

There was considerable variation in how individual participants made trust decisions in online and real-life scenarios. However, we were still able to identify themes and patterns in how users approached the process of making security-related decisions online. Having identified the themes in how people make these decisions, we identified a model of how they combine them in the decision-making process.

During our conversations, we observe that however many elements for decision-making our participants described, they were still left to combine these elements into each single decision. This tension was often explicit – when participants described rejecting security for pragmatic reasons, or when trying to find an “acceptable” level of risk to assume in a dubious transaction. To describe these tensions, we chose to use the metaphor of a funnel, where users are trying to force different aspects of assessment into the funnel of decision-making, but are ultimately limited by the bottleneck where only a single decision can be made.

Figure 1 shows our funnel model for how users combine different elements into making each decision. The user’s decision-making process begins by incorporating the materials used by the user to determine the trustworthiness of a website: their default trust, their varying concerns about security and privacy, the list of factors that give them confidence, their past experiences in similar situations, and the demands of the primary task. In the top of the funnel, the user’s decision elements are assembled: their default attitude, the primary task that they have to accomplish, the result of their previous decisions, the amount of risk they are willing to assume, their particular areas of concern, and the trust factors that they habitually rely on.

The narrow stem of the funnel represents the bottleneck, where certain elements outweigh others, and the user must obtain a single decision that combines all of their priorities, concerns, and trust. In our interviews, participants seemed unable to give clear descriptions of exactly how they weighted these varying considerations, and it was clear that there was a complex personal calculus that formed each decision. However, users did often describe the tensions of having to make a single decision from an overload of information (and sometimes, a lack of relevant information).

Following this decision, its consequences (e.g., improved security, identify theft) may impact not only a single user but also their friends and family as other users look for information to feed into their own decision-making processes. If the user chose not to trust a website, they might have a primary task that remains incomplete, and still be looking for ways to accomplish that task. If they did trust the website, and no security problems result, they may relate that positive experience in user reviews or feedback to other users. In other situations, it may be unclear what the exact consequences of the decision are, but the experience of having to make that decision may feed into feelings of a lack of a control or learned helplessness.

4.5 The Role of Website Locations

In the final segment of our interviews, we briefly explained the concept of location-based website authentication to participants, and asked them for some feedback about how they thought it could (or could not) be useful to them. Users were heavily primed to discuss security in this part of the interview, but because our goal was to design a tool for users, we wanted to understand what users might desire from this kind of tool.

Unsurprisingly, participants had not typically related website locations to Internet security. Similar to previous findings, they were also mostly unaware of the geographic locations of websites and where their data was stored. Several participants speculated that data must be stored in the same countries where the parent companies were based. These responses were sensible and expected since the infrastructure of the Internet abstracts away the physical locations of website content and data storage.

Although we explained location in the context of a security indicator, participants nearly always conflated security (the authenticity of the website) with privacy (where, how, and whether users’ data is stored or collected).

When asked about the presentation of location information, most participants discussed the idea of location on the country level (as opposed to the city or continent level). Participants often brought up the legal implications to do with having data stored in different countries (mainly in the context of financial information). They also occasionally referred to public disclosures of nation level surveillance programs (e.g., mass surveillance in the USA) and other data-gathering concerns when discussing where they avoided sharing or storing personal data.
“I would say it is important to be sure they are stored in countries with high security levels... I would say in the first place legal regulations: who is allowed to have access and under what conditions someone could have access to such data. And in Europe, I would say such [legal institutions] are on a high standard.” – P11

Participants often suggested that location information could be most helpful for sensitive applications such as banking, but One participant also identified the potential for location to be incorporated into security mechanisms.

“But I think in the end it will be used everywhere because it would be like a, like an adapted protocol. I think for me it would be useful into banking.” – P4

Participants often related website location to the implication of disclosing their information to the corresponding governments. In addition to a concern related to our assumed server impersonation attacks, the participants prominently cared about how foreign governments could harm their privacy when websites are hosted abroad.

Regarding trust factors, we noticed that participants were more receptive to discussions of website locations as opposed to traditional security solutions, such as public key certificates or authentication. Users had opinions about locations, and were willing to discuss how they might relate website locations to other information about countries or services. One participant discussed the utility of location information in relation to logistical concerns such as shipping and postage when shopping online. Another participant wanted to be able to consider environmental implications of web server locations, and discussed her concerns about the damage inflicted by large heat-generating data centers. Another participant mentioned a similar concern, but related her desire to know that her data was being stored in a location where workers were being treated and paid fairly.

5. DESIGN OF LOCATIONWATCH

Based on our qualitative analysis and funnel model, we developed a set of design requirements for our location tool, LocationWatch. LocationWatch is intended to act as a visual indicator to inform users about the result of server location verification, envisioned to use recently-proposed methods. We implemented LocationWatch as a Chrome extension featuring: a flag indicator, a location tip, and a warning message. Since website location verification methods are still under development, LocationWatch currently uses IP geolocation databases as a reference.

LocationWatch’s main features include a flag indicator, a location tip, and a warning message. The flag indicator (Figure 2a) is an icon near the address bar showing the flag of the server’s residing country. It also shows more information in a popup window when clicked by the user. The location tip (Figure 2b) is a small window on the upper-right corner of the web content that appears on the first visit to a website. The warning message (Figure 2c) appears when a website’s location has changed since the user’s previous visit and allows the user to decide whether to continue visiting it. In the event of a server impersonation attack (i.e., using a fraudulent certificate or a compromised server’s private key), this tool would display information about the location of the attacker’s server.

5.1 Design Rationale

We aimed to implement LocationWatch as an unobtrusive and effective tool to assist users in assessing the inputs to their decision. We developed LocationWatch as a separate browser indicator so that location can later be independently evaluated without users being explicitly aware of its purpose.
for security. We save our discussions on its integration with existing security indicators for Section 7.

5.1.1 Default Trust
Since users often trust websites by default and without understanding security indicators, security information should be made intuitive for them. Some may even prefer not to be bothered with location details since website security is not their primary task. We therefore designed LocationWatch to be non-intrusive by showing only the flag icon by default.

5.1.2 Diverse Concerns
We found that participants were generally concerned about how their private data was used or misused by governing nations in which the web servers reside. Since legal protection laws differ across countries, the location of where data is stored or sent may prompt different user concerns and influence subsequent decision-making. We therefore designed a popup (Figure 2a) that appears when the user clicks on the flag icon. This popup shows the server’s governing country, and information on that country’s data protection laws for the user’s reference.

5.1.3 Trust Factors
While recent work has shown the potential of location as a trust factor, most participants did not initially think of it when being interviewed. To strengthen users’ attention to location, the location tip appears on the user’s initial visit to a website (Figure 2b). While slightly obtrusive, this tip provides an attentive user a first impression of where this website is originally located and it is designed to only appear once by default. We also use the popup window (Figure 2a) to show more detailed information for interested users.

5.1.4 Past Experience
Past experience plays an important role since many participants considered the visual familiarity of websites as a primary factor for trust. Therefore, we chose to show a visual cue to inform the user when the website location has changed. This is realized using a warning message (Figure 2c) showing the current and previous website locations, thereby increasing the users’ security awareness.

5.1.5 Practicality
As discussed, participants admitted to ignoring security warnings for practical reasons such as convenience or an acceptable level of risk. Our location indicator does not prohibit such choices, as is also available with certificate warnings. In the warning message, we provided two buttons: “leave the website” and “proceed carefully” (Figure 2c). The phrasing of these buttons were aimed to hint that users should reconsider the security of their decisions.

6. STUDY 2: USER EVALUATION
To evaluate the impact of the information provided by LocationWatch on users’ decision-making processes, we conducted a user study. First, we aimed to evaluate the usability of our location interface to see if it satisfied our design concepts and requirements. Positive user feedback would suggest the potential of location as useful added information for users. Second, we aimed to evaluate how users’ security awareness in online services changes when website locations are provided. In the qualitative analysis, we found that many users relied on past experiences and impressions of the website. We therefore hypothesized that website location changes between subsequent visits would alarm users and could be used as an indicator of their security awareness.

6.1 Study Design
To evaluate LocationWatch and users’ response to website locations, we designed an experiment where participants used three web services (file storage, social networking, and online banking) and performed routine but potentially sensitive tasks. We chose these services to prompt typical concerns from the qualitative analysis: personal privacy, identity safety, and financial security. We aimed to measure how online behavior varied when participants were given website location information using LocationWatch.

Our study had a mixed design, where group was a between-subjects factor and stage was a within-subjects factor. There were two groups: control and experiment. In the control condition, the location interface was configured to show only the flag icon and the popup window (making it similar to existing tools [15][34]). In the experiment condition, participants used the fully-featured version of LocationWatch, including the location tip and the location change warning. The study had three stages and in each stage the participant was asked to perform three tasks, as shown in Table 1. We used a Latin square design to shuffle the task order across different participants in each stage to avoid order effects.

| Stage | Tasks | Website location | Available indicators |
|-------|-------|------------------|----------------------|
| 1 Initial visit | Dropbox: upload passport scan | United States | Flag |
| | Facebook: update status | Sweden | Flag |
| | Banking: check 1st account balance | Switzerland | Flag |
| 2 Re-visit without change | Dropbox: upload password list | United States | Flag |
| | Facebook: update status | Sweden | Flag |
| | Banking: check 2nd account balance | Switzerland | Flag |
| 3 Re-visit with change | Dropbox: upload credit card | China | Flag |
| | Facebook: upload party photo | United States | Flag |
| | Banking: check 3rd account balance | Japan | Flag |

Table 1: Study 2 tasks and location configuration for the control and experiment groups.
Each participant was given a brief introduction to the study’s purpose as a usability evaluation of a software tool. All participants received the same tutorial on LocationWatch, introducing the concept of geographic locations of websites, the flag icon, and the popup features. To avoid priming users to expect location changes, we did not introduce the location tip and warning (these features were only available to the experiment group). Participants were then given login information for the accounts and files created for the studies, and instructed to treat these accounts as if they were their own. LocationWatch was pre-installed in the participants’ browser to prevent its installation process from becoming a confounding factor to user response.

6.2 Selecting Test Locations

We chose to have our tool show three types of locations: neutral countries typically associated with good privacy impressions (Sweden, Switzerland, Japan), and a developing country with known Internet censorship (China). We also chose plausible locations for the services used in the study. For the last stage of the study, we programmed LocationWatch to show location changes: Dropbox to China, Facebook to the USA, and the online bank to Japan. For the control group, this resulted in a change of the country flag and contents in the popup. For the experiment group, the location change warnings were additionally shown.

Any choice of countries would naturally subject our study to various user-side cultural biases, and we therefore fixed the country assignments across different participants rather than randomizing them to minimize experiment variation. Since we were focused on observing whether location plays a role at all in this study, we leave the design of a more large-scale and ecologically valid study as future work.

Each session lasted between 30 and 60 minutes, and the study was conducted in our lab to facilitate observation and discussion. In addition to instrumented data collection about their interaction with the tool, participants also completed three questionnaires during the study: demographics, a pre-test questionnaire about their online decision-making habits, and a post-test questionnaire about their impressions of the usability and security of LocationWatch.

6.3 Participants

We recruited users who were aged 18 years or above, spoke English, and had experience with the Internet, including experience with online banking, file storage, and email. 44 participants completed the study (23 female and 21 male), most of whom were students (32). They ranged in age from 20 to 59, with most (34) being between 20 and 29 years old. Participants’ nationalities spanned 17 countries. They were studying in a variety of areas, including social sciences, humanities, natural sciences, and engineering. They had visited a median of 15 countries. Each study lasted between 25 and 40 minutes.

6.4 Results

We evaluated performance in our study with two main measures: the number of tasks that were completed, and the time that users took in the decision-making process.

6.4.1 Task Completion

We recorded how often users completed the tasks in each stage and each condition of the experiment, and used task completion as a measure of how location affected participants’ behavior. We defined task completion as having logged into the web service and completed the given task. We encoded completed tasks as 1, and uncompleted tasks as 0. For each stage we summed the scores from the three websites to produce an aggregate score between 0 and 3.

Figure 3 shows the distributions of completion scores. While most control group participants completed all tasks in all stages, fewer experiment group participants completed the task when the location changed, as also evidenced in the statistics in Table 2.

We first looked for differences in task completion between the control and experiment groups. Since task completion was based on counts, we performed a between-subjects Chi-squared test on the sum of completion scores across all stages and found a significant difference between the two conditions ($\chi^2(1) = 9.44, p = 0.002$). Post-hoc pairwise Chi-squared tests using a Bonferroni correction showed that this differ-

![Figure 3: Box plots of task completion scores across different stages for all websites.](image)

Table 2: Descriptive statistics of task completion across different stages.

| Stages | Control | Experiment |
|--------|---------|------------|
|        | Mean    | Mdn        | SD   | Mean    | Mdn        | SD   |
| 1      | 2.82    | 3          | 0.50 | 2.73    | 3          | 0.63 |
| 2      | 2.55    | 3          | 0.60 | 2.32    | 2          | 0.65 |
| 3      | 2.32    | 3          | 0.84 | 1.45    | 2          | 0.96 |

Table 3: Chi-squared tests of task completion across different stages using the Bonferroni correction. We did not perform pairwise tests on the control condition since we found no significant differences between all the stages.

| Stages | $\chi^2$ | df | $p$ | $\chi^2$ | df | $p$ |
|--------|----------|----|-----|----------|----|-----|
|        |          |    |     |          |    |     |
| All    | 7.35     | 2  | 0.228 | 30.86    | 2  | < 0.001 |
| S1 vs. S2 | –      | –  | –     | 3.62     | 1  | 0.513 |
| S1 vs. S3 | –      | –  | –     | 26.15    | 1  | < 0.001 |
| S2 vs. S3 | –      | –  | –     | 10.52    | 1  | 0.011 |

2The notches in the box plots represent the 95% confidence intervals around the median. When the intervals fall outside the 1st or 3rd quartiles, the notches extend beyond the box.
ence occurred in Stage 3 ($\chi^2(1) = 10.52, p = 0.011$), where the warning made participants in the experiment group less likely to complete the task.

In the absence of an omnibus test for categorical data, we conducted Chi-squared tests to look for differences between the stages in each condition. We found a significant effect of stages in the experiment group ($\chi^2(2) = 30.86, p < 0.001$), but no effect in the control group ($\chi^2(2) = 7.35, p = 0.228$). Table 5 shows the results of post-hoc pairwise Chi-squared tests. We found significant differences in task completion between Stage 1 and Stage 3, and between Stage 2 and Stage 3 for the experiment group, showing that the warning for location changes significantly affected whether participants completed critical tasks.

### 6.4.2 Decision-Making Times

As an indication of how much attention participants paid to making decisions about location, we recorded the time taken in the login process. We measured the time between when the webpage loaded and when the user clicked the login button (in seconds). This measurement included the time that the user spent deliberating about whether to login. We aggregated the times for each participant in each stage by taking the mean of the times for the three websites. Figure 4 shows the distribution of times across the three stages.

Table 4 shows descriptive statistics of the times that participants took to make decisions and login by group and stage. The times in Stages 1 and 2 were similar across the two groups, the times decreased in Stage 2 (from ∼30 seconds to ∼17 seconds). In Stage 3, the experiment group spent more time considering their login decision (54 seconds).

We conducted a mixed two-way ANOVA to analyze the differences in login times between the two conditions and between the stages. There were significant effects of both condition ($F(1,41) = 12.73, p < 0.001$) and stage ($F(2,82) = 9.92, p < 0.001$) and a significant interaction between condition and stage ($F(2,82) = 10.65, p < 0.001$). We then used post-hoc pairwise t-tests to observe differences between the two groups. There were significant differences only in Stage 3 ($t(21) = -3.08, p = 0.051$), implying that the warning made the experiment group spend more time than the control group. We further conducted post-hoc pairwise t-tests with a Bonferroni correction to look for differences within each group (Table 5). There were significant differences between Stages 1 and 2 for both conditions, possibly since participants became accustomed to the login process. The experiment group had significantly different login times between Stages 2 and 3, implying that the location change warning affected the time spent deciding to log in.

### 6.4.3 Task Completion on Different Websites

To examine whether LocationWatch had an effect on participants’ willingness to complete security-sensitive tasks, we aggregated completion scores within the same stage in our initial task completion analysis. However, we were also interested in how users reacted to different location changes on different websites. The scale of our study prevented us from exhaustively testing different websites and locations. However, in our study design we attempted to pick security-sensitive websites, and to choose location changes that might represent different attacks. We included location changes to countries that were neutral but implausible (Switzerland to Japan, banking), locations with well-publicized privacy issues (USA to China, Dropbox), and changes from plausible locations to other plausible locations (Sweden to USA, Facebook). As an exploratory analysis, we analyzed whether there was an effect of website (and the corresponding country change) on task completion.

Using the same definition for task completion as previously, we defined a participant’s task completion score for each website, ranging between 0 (no tasks completed) and 3 (tasks completed in all three stages). The distributions of website task completion scores for the control and the experiment groups are shown in Figure 5. In both conditions, participants completed fewer tasks on Dropbox (Table 6).

A Chi-squared test using a Bonferroni correction showed a significant effect of website in both the control condition ($\chi^2(2) = 29.17, p < 0.001$) and the experiment condition ($\chi^2(2) = 32.07, p < 0.001$). Post-hoc pairwise tests revealed that in both conditions, significantly fewer participants completed the tasks on Dropbox than on Facebook or banking, as shown in Table 7.
6.4.4 Usability
We used the System Usability Scale [11] to evaluate the usability of our location interface (detailed SUS results are presented in Appendix [9]). Both variants of our interface were ranked as ‘excellent’ (scores greater than 80) [39]. The average scores were 81.61 for the control group and 82.2 for the experiment group. Using a Mann-Whitney test, we found no significant difference in usability between the two versions of LocationWatch (U = 254.5, p = 0.78).

6.5 Summary
We found that participants’ decisions were indeed affected by their knowledge and perception of the websites’ locations. In particular, there were statistically significant behavior changes in task completion when the locations changed in the experiment condition, as participants completed fewer tasks than before. This suggested that they were alarmed by the location changes and some responded by avoiding performing sensitive tasks online. Participants who did complete the tasks when the locations changed mainly cited the website’s reputation as the main reason for them to proceed. They sometimes used extra steps to validate the authenticity of the websites. For example, when the location changed, some participants tried connecting to the designated website by searching for it using multiple search engines.

Additionally, we also noticed that when warned of website location changes, two users in the experiment group still chose to sign in and further inspect the website before refusing to perform the given task. This suggests that for some users, the critical decision point for personal security or privacy sometimes lies past the sign-in process. This supports previous work on designing browser warnings [41] that prevent users from leaking personal credentials to websites before ascertaining their trustworthiness, but suggests that part of the problem with browser indicators is that they appear at the wrong time.

LocationWatch did not interrupt users in non-critical cases since both groups took similar times in the login process in Stages 1 and 2. We found that there was a significant difference in Stage 3, in which warnings were shown in the experiment condition. In this stage, the experiment group took significantly longer, because they were deciding how to proceed or looking up reference information. Together with the task completion, this showed that the tool managed to attract users’ attention with the warning message.

Although not one of our original goals, we found preliminary evidence that location information may have increased significance in certain tasks that users perceive as sensitive. In our study, significantly fewer participants completed the Dropbox tasks, citing that they would not feel comfortable uploading personal information in such situations. However, many participants still logged in despite warnings in the banking task, which the interview results suggested would be most sensitive. It is difficult to know exactly why this effect occurred, but it suggests that participants interpret location information differently in different contexts.

In addition to identifying location’s role in users’ decision making, our evaluation also showed that LocationWatch was usable. SUS scores were good and similar for both groups. This showed that the version with the location change warning was as usable as existing solutions which primarily show the country flag (control group). The warning was also a desired feature since similar notifications were suggested by many participants in the control group (8 out of 22) during the post-study discussion.

7. DISCUSSION
The results of our studies suggest that website location is a promising research direction for helping users authenticate websites. Location is a comprehensible, approachable factor that users are able to relate to privacy and security, and incorporate when making security-related decisions online. In our qualitative analysis, we found that users lean on multiple factors to evaluate whether to make security decisions. We designed LocationWatch to let users incorporate location into this decision, and found that having location information available does affect how users make decisions about security and privacy.

7.1 Adoption and Deployment
We envision that in the future, location verification could become an important consideration for data center deployment, which is presently concerned with infrastructure and sustainability [17]. Online companies often contract their web hosting to content delivery networks (CDNs), which distribute data from the “origin” to servers closer to the clients (often to the same city or region), and we imagine that mar-
Co-location and third-party resources are fundamental limitations to users to explore the web server origins of multiple content pages and do not directly visit individual webpage elements. To avoid confusing users, as they typically view complete web content are not displayed. This is a design choice made to focus on the top-level web server, while the locations of embedded resources (e.g., CSS, JavaScript) in modern websites, which might consist of multiple locations served by other CDNs from other locations. Therefore, users are often bypassed or ignored. It remains a challenge to balance catching users’ attention with relevant warnings before their privacy or security are compromised, while not overwhelming them with notices.

In terms of real-world deployment and adoption, website owners would opt in to provide verifiable and fresh location information upon client connection as a service to users for added security assurance. We envision that LocationWatch would store a public list of legitimate server locations for each supported website, which might consist of multiple locations of the hosting CDN. Detailed information including precise website locations would be available to interested users. If the tool detects that the website is being served from an unlisted location, a warning similar to that in LocationWatch would be shown to the user. Given the findings of our study, we expect that users’ security awareness could be raised by such warnings, allowing them to take further caution with their private data.

In our study, we implemented LocationWatch as a separate tool because we wanted participants to be aware of its existence while minimizing the influence of their preconceptions of TLS warnings. However, we envision its functions to be integrated with existing security indicators, such as the TLS lock icon and its corresponding detailed information. This would allow the additional security messages provided by LocationWatch to be consumed by the user with other security information in a consolidated manner.

7.2 Future Challenges

There are challenges that currently limit the use of website locations as a trust factor due to the nature of the underlying infrastructure of the Internet. First, given the wide adoption of CDNs, it is likely that many websites are physically hosted from the same CDN server. This allows an attacker that compromises one website to gain access to that CDN, thereby effectively opening the opportunity to serve malicious web content from the same location. Such an attack is not detectable in the currently proposed location-verification protocols [24] since the location ceases to be a unique factor of the website that can be used as verification. However, major websites are still resilient to such attacks since they often host their login web pages on privately owned data centers. In terms of our location indicator, the warnings are effective only if the TLS endpoint of website is served from unique locations that are not shared by others.

Another limitation of related work on location-based security approaches stems from the use of numerous third-party resources (e.g., CSS, JavaScript) in modern websites, which can be served by other CDNs from other locations. Like current security indicators, LocationWatch shows the location of the top-level web server, while the locations of embedded content are not displayed. This is a design choice made to avoid confusing users, as they typically view complete web pages and do not directly visit individual webpage elements. An open design challenge is to create a design that allows users to explore the web server origins of multiple content sources on a single page. In general, the issues of adversarial co-location and third-party resources are fundamental limitations inherited from recent location-based authentication mechanisms. Although our exploration of location as a security indicator inherits such limitations, our focus was on understanding whether there was any potential for location information as a comprehensible security indicator.

Finally, a challenge with any added security mechanism is that it may distract or overwhelm users. While security warnings aim to protect watchful users from online threats, they are often bypassed or ignored. It remains a challenge to balance catching users’ attention with relevant warnings before their privacy or security are compromised, while not overwhelming them with notices.

7.3 Limitations

An unavoidable issue in this type of work is the subjectivity of participants’ views. We chose to conduct our studies in the lab in order to obtain richer data about participants’ interactions with LocationWatch. This allowed us to obtain detailed information about how location warnings are perceived by users through an interactive process. However, it also limited the diversity of perspectives that we were able to capture (both in terms of participants and the number of websites and locations we could present). In future work, it would be interesting to conduct a larger scale study using crowdsourcing platforms to evaluate theories about location’s influence and capture a more global perspective.

Our study was also affected by the aforementioned challenges of location-based authentication. More specifically, CDNs serve web content of different websites from multiple and non-unique locations. Therefore, participants that are aware of CDNs are less likely to be concerned when the websites’ locations changed during our experiment. Our in-person experiment allowed us to observe users in an interactive way and observe the large space of different contingent actions (e.g., retroactively deleting files or reasoning about warning messages). Overall, despite these limitations, our study is the first to explore how users reason with location information and integrate it into their decision-making.

8. CONCLUSION

Authenticating websites is an important problem that affects users because they must make decisions about whether or not a website is trustworthy. The current certificate model forces users to interpret dense and unfamiliar technical information, which results in users expressing confusion about warnings or ignoring them in favor of non-technical cues [16]. Recent proposals suggest the addition of web server location authentication [24, 50] to strengthen TLS. Our work is the first to explore the usability aspects of these proposals. We investigated how location information can fit into users’ decision-making processes, and whether location information affects the decisions that users make about security-sensitive tasks.

We designed LocationWatch, a browser extension to notify users of website locations and their changes. We conducted a user study and found that when alerted to a location change, users understood the change and interpreted it in light of their current task. As a result, they were less likely to complete security-sensitive tasks when warned about location changes. Our findings suggest that website location indication has the potential to be a usable approach to helping users make informed decisions about privacy and security.
9. REFERENCES

[1] CVE-2014-0160. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160 2014.

[2] A. Abdou and P. van Oorschot. Server location verification and server location pinning: Augmenting tls authentication. arXiv preprint arXiv:1608.03939, 2016.

[3] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. Science, 347(6211):p509–514, Jan. 2015.

[4] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13), pages 257–272, 2013.

[5] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo. Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning. In SOUPS, pages 113–128, 2014.

[6] Amazon Web Services. AWS Global Infrastructure. https://aws.amazon.com/about-aws/global-infrastructure/ 2016.

[7] APNIC. Asia-Pacific Network Information Centre. https://www.apnic.net/ 2016.

[8] ARIN. American Registry for Internet Numbers. https://www.arin.net/ 2016.

[9] L. Barkhuus and A. K. Dey. Location-Based Services for Mobile Telephony: a Study of Users’ Privacy Concerns. In INTERACT for Mobile Telephony: a Study of Users’ Privacy and human behavior in the age of information. Science, 347(6211):p509–514, Jan. 2015.

[10] V. Braun and V. Clarke. Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2):p77–101, Jan. 2006.

[11] J. Brooke. SUS-A quick and dirty usability scale. Usability evaluation in industry, 189(194):p4–7, 1996.

[12] CAB Forum. EV SSL Certificate Guidelines. https://cabforum.org/extended-validation/ 2016.

[13] J. Clark and P. C. van Oorschot. SoK: SSL and HTTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In IEEE Symposium on Security and Privacy (S&P), 2013.

[14] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages p81–90. ACM, 2005.

[15] Dave G. Flagfox. https://flagfox.net/ 2016.

[16] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL warnings: comprehension and adherence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI), pages p2893–2902. ACM, 2015.

[17] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acar, E. Morant, and S. Consolvo. Rethinking Connection Security Indicators. In Twelfth Symposium on Usable Privacy and Security (SOPUS), 2016.

[18] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo. Experimenting at scale with google chrome’s SSL warning. In Proceedings of the 32nd annual ACM conference on Human factors in computing systems, pages 2667–2670. ACM, 2014.

[19] D. Fisher, L. Dorner, and D. Wagner. Short paper: Location privacy: User behavior in the field. In Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pages p51–56. ACM, 2012.

[20] B. J. Fogg, P. Swani, M. Treinen, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, and J. Shon. What makes Web sites credible? In Proceedings of the International Conference on Human Factors in Computing Systems (CHI), pages p61–68. ACM, 2001.

[21] Geobytes. Geobytes IP Address Locator. http://geobytes.iplocator/ 2016.

[22] Google. Google Data Center Locations. http://www.google.com/about/datacenters/inside/locations/index.html 2016.

[23] Google. Google for Work Security and Compliance Whitepaper. https://static.googleusercontent.com/media/www.google.com/en/US/work/apps/business/files/google-apps-security-and-compliance-whitepaper.pdf 2016.

[24] J. B. Hardee, R. West, and C. B. Mayhorn. To download or not to download: An Examination of Computer Security Decision Making. ACM SIGCSE Bulletin, 13(3):32–37, May 2006.

[25] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Abowd. Developing privacy guidelines for social location disclosure applications and services. In Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS), pages p65–76. ACM, 2005.

[26] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOPUS). ACM, 2011.

[27] IP2Location.com. IP2Location. http://www.ip2location.com/ 2016.

[28] IPligence. IPligence Geolocation Solutions. http://www.ipligence.com/ 2016.

[29] Ergonomics of human-system interaction – Part 210: Standard, International Organization for Standardization. March 2010.

[30] R. Kang, L. Dabbish, N. Frucher, and S. Kiesler. “My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security. In Eleventh Symposium On Usable Privacy and Security (SOUPS), pages p39–52, 2015.

[31] A. Langley, E. Kasper, and B. Laurie. Certificate Transparency. https://tools.ietf.org/html/rfc6962 2013.

[32] R. S. Laufer and M. Wolfe. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues, 33(3), 1977.

[33] MaxMind. IP Geolocation and Online Fraud Prevention. https://www.maxmind.com/ 2016.

[34] myip.ms. IP Whois and Flags Chrome and Websites Rating. http://chrome.myip.ms/ 2016.
APPENDIX

A. USER INTERVIEW SCRIPT

We attach our semi-structured interview script here. We prepared the following interview questions to ask participants about their Internet use, location and security awareness, and preferences on location.

Online Storage
1. Do you use online file storage services (e.g., Dropbox, Apple iCloud, Google Drive)? Could you mention some examples of how you use it?
2. What kinds of data do you store online? Are there types of data that you typically try not to put on the Internet?
3. Is there any information about yourself that you specifically try not to store on the Internet?

Email, Calendars, Contacts
4. Do you use online calendars like the Google Calendar, or the iCloud calendar? Can you elaborate on the types of events you mark on your calendar that you store online?
5. Do you use a web-based email service? What do you use it for?
6. Do you store your contact information online? What kinds of information do you store?

Finance and Shopping
7. Do you use online banking? Could you mention some examples of how you use it? E.g., just checking your balance, transferring funds, stocks investment or financial planning.
8. Do you use your credit card to shop online?
9. How do you choose where to shop online? What kind of considerations are likely to make you trust an online store?
10. When you are shopping online, how would you feel if store’s domain indicates a foreign country?
11. What kind of precautions do you take around handling financial transactions online (whether with credit cards or online banking)? Do you store your credit card information online?
12. Are there any aspects of financial management that you would not feel comfortable performing online?

Social Networking
13. Do you use social networking or messenger services, such as Facebook, Google Plus, Twitter, Instagram, etc.? This may also include messaging services like WhatsApp.
14. Is there a difference in the kind of information you share to different platforms? What kind of considerations do you make before putting your information on different types of social media?
15. What are your concerns regarding your privacy on social networking websites, such as Facebook, Twitter, or Instagram?

Knowledge of Locations
16. When you store your files (photos, videos, documents) online, where do you think these files are stored?

[35] Netcraft. Fake SSL certificates deployed across the internet. http://news.netcraft.com/archives/2014/02/12/fake-ssl-certificates-deployed-across-the-internet.html 2014.
[36] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In Proceedings of the 5th Symposium on Usable Privacy and Security, 2012.
[37] Penton. Data Center Knowledge.
[38] RIPE. Regional Internet Registry for Europe, the Middle East and parts of Central Asia.
[39] S. Ruoti and K. Seamons. Standard metrics and scenarios for usable authentication. In Symposium on Usable Privacy and Security (SOUPS), 2016.
[40] N. Security. IRS reports 400-month increase in phishing malware.
[41] D. Shin and R. Lopes. An empirical study of visual security cues to prevent the SSLstripping attack. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 287–296. ACM, 2011.
[42] R. Sleevi, C. Evans, and C. Palmer. Public Key Pinning Extension for HTTP.
[43] J. Sobey, R. Biddle, P. C. van Oorschot, and A. S. Patrick. Exploring user reactions to new browser cues for extended validation certificates. In European Symposium on Research in Computer Security, pages 411–427. Springer, 2008.
[44] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In Proceedings of the Seventh Symposium on Usable Privacy and Security, page 3. ACM, 2011.
[45] J. Sunshine, S. Egelman, H. Almuhiomed, N. Atri, and L. F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In USENIX Security Symposium, pages 399–416, 2009.
[46] USA Today. Top secret Visa data center banks on security, even has moat.
[47] Verne Global. Data Centre Risk Index.
[48] R. West. The Psychology of Security. Communications of the ACM, 51(4):p34–40, Apr. 2008.
[49] A. Whitten and J. D. Tygar. Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security, volume 1999, 1999.
[50] D.-Y. Yu, A. Ranganathan, R. J. Masti, C. Soriente, and S. Capkun. SALVE: Server Authentication with Location VErification. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom), 2016.
17. When you visit a website, such as Wikipedia, Google Maps, or Yahoo News, where do you think the web content is stored?

18. When you visit a website, such as online banking or online storage, how do you know you are actually visiting the real website, as opposed to a forged website to steal your personal information? Are there particular indicators that you pay attention to?

**Internet Service Location Preferences**

Interviewer: We’ve so far talked about a lot of things you can do using the Internet. A lot of these services store your data in data centers located somewhere in the world. Companies also use these data centers to store information that you consume, such as news articles. Let’s talk about your trust or various preferences regarding these data centers.

1. What are your privacy concerns about your data online? This might include files stored online, personal information, or credit cards?

2. Do you have any concerns about where your data are being stored? What kind of concerns? For example, where would you like your data to be stored?

3. Does your preference of where your data is stored depend on the type of data? Specifically, consider the following types of data: your banking account data, online shopping history, chats, emails, social networking data, hotel or flight bookings, etc.

4. Imagine that you are provided with information regarding the location of where your online services are. How would such information influence your trust in these services?

5. What kind of location information do you have in mind? How detailed would you prefer such information to be presented?

6. Imagine that the location information can be presented to you when you visit a website. How do you think this location information should be displayed?

7. If you had location information available to you, in what kind of services do you think it would be useful?

**B. THEMATIC ANALYSIS**

We obtained the themes from our observations in the open coding process. The identified codes are organized by theme and shown in Table 8.

**C. SUS OF LOCATIONWATCH**

We present the SUS results of LocationWatch in Figure 6.

Figure 6: SUS results of LocationWatch using the Likert scale. Both variants were considered useful by the participants and no statistically significant differences between them were found.
Table 8: Complete list of all the open codes used in the analysis, organized by theme.

| Code                      | Description                                                                 |
|---------------------------|-----------------------------------------------------------------------------|
| **Theme: Trusting by Default** |                                                                             |
| Lack of awareness         | The user lacks awareness in online security and privacy.                    |
| Misconceptions            | The user exhibits incorrect perceptions of online services.                 |
| Automatic use             | The user allows automatic mechanisms to transfer data.                      |
| **Theme: Having Diverse Areas of Concern** |                                                                             |
| Security concern          | The user is concerned with online security.                                |
| Privacy concern           | The user is concerned with privacy.                                         |
| Financial concern         | The user is concerned with financial safety.                                |
| Credential concern        | The user is concerned with identity safety.                                 |
| Political concern         | The user is concerned with the political stance.                            |
| Legal concern             | The user is concerned with legal regulations that govern online services.  |
| Third-party concern       | The user is concerned with non-official sources of service                  |
| Indifference              | The user is indifferent to security and privacy issues                      |
| Fear                      | The user worries about online security and privacy.                         |
| **Theme: Relying on Multiple Trust Factors** |                                                                             |
| Looks for personal impact | The user decides by weighing the potential risks of insecurity.            |
| User interface cues       | The user observes website content to identify suspicious websites.          |
| Security indicators       | The user pays attention to existing browser certificate indicators          |
| Familiarity               | The user feels more secure interacting with familiar online services.       |
| Reputation                | The user feels more secure interacting with well-known online services.     |
| First-party trust         | The user trusts the origin manufacturer when shopping online.               |
| Escrow reliance           | The user relies on escrow services in online shopping.                     |
| Previous experience       | The user uses past experience to evaluate website trustworthiness.          |
| Social reassurance        | The user trusts a service because friends also use it.                     |
| Geopolitical oversight    | The user prefers countries with good legal frameworks.                     |
| **Theme: Practicality**   |                                                                             |
| Research                  | The user uses online resources like website reviews                         |
| Convenience               | The user makes trust decisions driven by convenience.                       |
| Privacy unconcern         | The user is not concerned with online privacy.                              |
| Out-of-band communication | The user contacts customer service.                                         |
| Safe fallbacks            | The user resorts to other means of achieving their application goals.       |
| Limited online presence   | The user limits personal exposure when storing data online.                 |
| Fake profiles/pseudonyms  | The user submits false profile information to online services.             |
| Pragmatic approach        | The user chooses practical solutions.                                       |
| Leap of faith             | The user uses an online service by asserting that it is secure.             |
| Compromise                | The user compromises security indicators to use service.                   |
| Security/usability tradeoff | The user considers the tradeoff between security and usability.           |
| Tangibility               | The user maintains tangible proofs (e.g., paper) of online transactions.    |
| Social pressure           | The user uses online services driven by social pressure.                    |
| **Theme: Helplessness and Learning from Consequences** |                                                                             |
| Security as personal responsibility | The user understands that online security is a personal responsibility.   |
| Lack of control           | The user lacks means of controlling online presence and exposure.          |
| Lack of knowledge         | The user lacks technical knowledge.                                         |
| Confusion                 | The user is unsure of the implications of online behaviors.                |
| Acknowledgment of inability | The user acknowledges imperfect abilities and decisions.                  |
| Frustration               | The user feels helpless due to repetitive frustration.                     |
| **The Role of Website Locations** |                                                                             |
| Locality                  | The user thinks that a firm’s website is located in the firm’s country.    |
| Cultural factors          | The user’s trust is based on cultural factors or biases.                   |
| Ecological concern        | The user is concerned with environment impact of online services.          |
| Conspiracy theory         | The user is informed of conspiracy theories such as public surveillance.   |
| Sensitivity               | The user is sensitive to the topic website location.                       |