Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard

Imani N. Sherman, Daniel Delgado, Juan E. Gilbert, Jaime Ruiz, Patrick G. Traynor
University of Florida

Abstract

The Federal Communication Commission (FCC) has taken action against the increasing number of spam calls by mandating service providers implement STIR/SHAKEN, a framework for authenticating Caller ID. Specifically, STIR/SHAKEN provides users with a series of alerts representing the various potential states of authentication of an incoming call. While these states have a clear definition in the standards, it is unclear whether end users can interpret these states and whether they will ultimately help users defend themselves against robocalls. In this paper, we perform the first survey of consumer preferences (n=806) for how carriers should react to specific authentication types. We then evaluate user interpretation of warning designs representing various STIR/SHAKEN authentication states. Finally, we explore how users interpret and plan to react to these different states through interviews (n=20). The results suggest that users have difficulty fully understanding the output from STIR/SHAKEN due to personal preference, understanding of authentication states, and the impact of design. This misunderstanding leads to unintended interpretations and behavior. In so doing, we show that significant design challenges must be overcome for STIR/SHAKEN to reach its full potential as a means of mitigating robocalls.

1 Introduction

The increase in spam calls has become a point of concern for both consumers and government officials. American consumers reported losing more than $667 million in 2019 from spam calls [63]. Unfortunately, until call authentication becomes available in telecommunications systems, spam calls will likely continue to be a low-risk and high reward crime. To add some form of authentication to incoming calls, researchers and practitioners have developed solutions to authenticate spam calls through various means. Solutions such as block and allow listing [38, 62], chatbots [48], call back verification [36], CAPTCHA [59], content and audio analysis [7, 34], provider-based solutions [4, 52, 60], and end-to-end authentication [41, 42]. Among these suggestions is STIR/SHAKEN, a provider-based framework for authenticating voice-over internet protocol (VoIP) calls [4]. This solution includes notifying users of various potential authentication states, which are formally referred to as *levels of attestation*. Although the FCC mandated that STIR/SHAKEN be implemented by telephone carriers in the future [16], the ruling did not include guidelines on how and when carriers should communicate levels of attestation to consumers. This could be problematic if carriers decide to communicate information differently, thus causing confusion and distrust in the new technology.

In this paper, we identify the usability challenges that would likely occur if the FCC mandate is deployed in its current form. First, we conduct a survey (n=806) with both visually impaired and sighted users to determine what levels of attestation consumers want and if they want carriers to notify them about these levels. We understand that users often want and need different information, which is why we solicited responses from both groups of users. Then, we test user reactions to and interpretations of STIR/SHAKEN output in warning form. Finally, we interview 20 individuals to determine further how consumers make sense of STIR/SHAKEN levels of attestation. Our findings suggest that consumers want and expect Caller ID information to be accurate regardless of the attestation level. Due to their current understanding of Caller ID, consumers did not use warning information when the carrier was unable to verify all of the Caller ID information. Instead, they referred to the caller's number and name to determine how to respond. We make the following contributions:

1. **Identify User Preferences:** We evaluate the results of a survey distributed to Mturk crowdsource workers and members of the National Federation of the Blind to establish user expectations of call authentication. We show that both sighted and visually impaired users prefer all Caller ID information be verified.

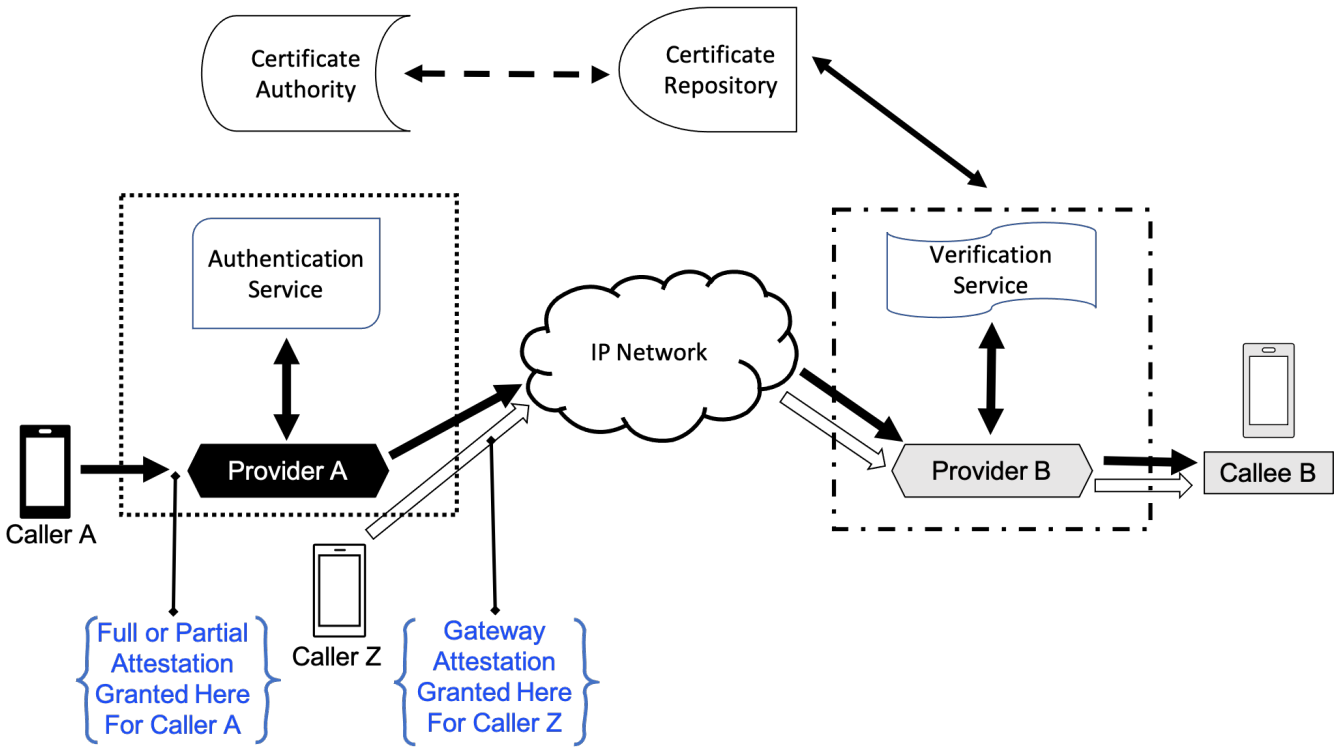


Figure 1: This figure displays how STIR/SHAKEN works in the telephone network. When a call is made, the caller's provider will grant full or partial attestation. However, the provider will grant Gateway Attestation when it can authenticate where it received the call from but not the call source.

2. **User Understanding of Authentication States:** We analyze user responses and feedback on design representations of authentication states. While 57% of survey participants were able to interpret that something was verified or unverified, they (63%) still selected unintended interpretations about the amount of verified information, call safety, expected reactions, and provider actions.

3. **Future Guidelines:** Our results identify three challenges with communicating STIR/SHAKEN results and provide a starting point for design guideline development and testing towards usable STIR/SHAKEN implementation.

The remainder of this paper is organized as follows: Section 2 provide background information about STIR/SHAKEN; Section 3 discuss the user study methodologies used ; Sections 4, 5, and 6 present the results of the three user studies ; Section 7 provides the limitations of the work; Section 8 discusses the results found and suggestions for improvement of usability; Section 9 details related work; and Section 10 provides concluding remarks.

2 Background

Traditionally, calls are made using the Public Switch Telephone Network (PSTN). These circuit-switched networks rely on older technology (i.e., dedicated lines), require extensive infrastructure, and are limited in the type of data they can transmit from one caller to another. As technology advanced, the Voice over Internet Protocol (VoIP) was created to remove the limitations of PSTN. VoIP networks are packet-switched, which requires fewer resources than PSTN and allows users to do more over their network. However, VoIP's introduction has led to an increase in robocalls since VoIP calls cost less to make and are easier to manipulate. STIR/SHAKEN, shown in Figure 1, was developed to provide authentication for VoIP.

STIR/SHAKEN is made up of two mechanisms -STIR and SHAKEN. The STIR protocols support the creation of digital signatures for a call. These signatures indicate that the caller's provider has authenticated some or all information regarding the call. The SHAKEN standards detail the implementation of STIR by service providers. These protocols work together to certify call origination information, similar to how Domain Key Identified Mail (DKIM) works for email [18].

During this process, the originating service provider is tasked with determining how to certify or attest to the call source's validity and calling number. There are three levels

of attestation [**?**]:

Full Attestation (A) — The service provider of the caller has authenticated the caller's identity, confirmed they (the caller's service provider) are responsible for call origination, and verified the number.

Partial Attestation (B) — The service provider of the caller can confirm the identity of the caller, that they (the caller's service provider) are responsible for the origination of the call, but they can not confirm the phone number used is associated with the caller.

Gateway Attestation (C) — A service provider can confirm that the call originated from their VoIP network.

The various levels of attestations allow the originating service provider to attest for calls made from international gateways and business numbers. They might be unable to certify the caller, confirm the caller's number, service provider and the network where the call originated. However, we hypothesize that if the "attestation" is not carefully explained and presented to consumers, the various levels might be difficult to understand. Thus, we sought to identify challenges carriers may encounter when communicating this information. Our investigations focus on the following research questions:

1. What information do consumers want to be verified?
2. When do consumers want to be notified about verified or unverified information?
3. How do consumers interpret various levels of attestation?
4. How do consumers respond to various levels of attestation?

3 Methodology

We conducted both surveys and interviews with visually impaired and sighted participants to help answer our research questions. We included those with and without visual impairements becuase we recognize that users have varying needs and communicating information includes thinking about those who are unable to recieve visual cues. In this process, we created accessibe warnings to introduce participants to attestation levels in a less complicated way. Our institution's Internal Review Board approved all studies discussed in this paper.

3.1 Surveys

We conducted a series of online surveys using Amazon's Mechanical Turk (MTurk) crowdsourcing service in 2020. In order to participate, MTurk workers had to be 18 or older, a resident of the United States of America, and have a 95% or higher approval rating [39]. Additionally, to prevent workers from completing more than one survey, participants were only able to complete one of the surveys. Participants were paid $.30 for completing the 2-minute survey. We also invited members of the National Federation of the Blind (NFB) to take a similar survey. They had to be 18 or older and a resident of the United States of America to participate. There was no general compensation due to the large number of participants. However, every 25th participant received a $25 gift card.

Participants: In total, 806 participants completed one of the surveys. The majority of the participants were from MTurk (n=606). Additionally, most participants identified as white (73%), male (53%), and had a Bachelor's degree (50%), as shown in Table 7 in the Appendix. We recognize that MTurk workers are usually younger and more technically advanced than the general population. However, research shows that MTurk surveys can provide a more diverse sample than universities [10, 13, 27], and they are representative of the U.S population for privacy and security related user studies [43].

Survey Design: MTurk and NFB participants were asked to respond to two of six incoming call screenshots, as shown in Figure 2. 36% of MTurk participants were asked to respond to one mock call and three questions about how they prefer service providers react to unverified call information. Both versions of the survey displayed questions in a random order but ended with a demographic questionnaire. The survey sent to NFB participants included descriptions for each design that would read precisely what was written on the warnings for those who used a screen reader.

Data Analysis: The survey results were analyzed using descriptive statistics to determine which survey options were preferred. Additionally, a chi-squared test of homogeneity analysis without correction was used to compare proportions [6].

3.2 Interviews

Following the surveys, we then conducted user interviews to understand user response to the incoming call screenshots. Participants were paid $10 for completing the 35-minute interview.

Participants: We interviewed 20 individuals, where three participants identified as experts in user experience, design, and accessibility. Ten participants identified as blind, and ten were sighted. Half (50%) of the participants were male, and most were white (60%) and had a college degree (80%), as shown in Table 7.

Interview Procedure: Each semi-structured interview started with the participant detailing their recent experience with incoming calls and describing their ideal incoming call alert to the researcher. The interviewer then showed or played a series of warnings to get the user's reaction and interpretation. Each interview ended with the interviewer recapping what they heard and providing space for the participant to correct or add to what was recorded. The experts were interviewed following those of the non-expert participants. We spoke with them to get their perspective on accessible and usable warnings for various call types based on their experi-

Table 1: Percent of Particpants that Prefer Specific Types of Informaiton Be Verified.

I would like my telephone provider to verify...	**% of Participants (n=411)**
Name of the caller	77%
Number of the caller	81%
Location of the caller	60%
Service provider of the caller	24%
If the call was allowed by the caller's service provider	6%
other	2%

Table 2: Percent of Particpants that Prefer to be Notified About the Authentication Status of Information.

When I receive a call I want to be notified when...	% of **Participants**		
Options	**Verified (n=212)**	**Unverified (n=199)**	**Both (n=411)**
The name of the caller shown is unverified	71%	70%	71%
The location of the caller is unverified	59%	54%	56%
The number of the caller is unverified	73%	70%	72%
The service provider of the caller is unverified	19%	29%	24%
The call was allowed by the caller's service provider without Caller ID verification	11%	25%	18%
Other	2%	2%	2%

ence.

Qualitative Analysis: All interview transcripts were analyzed using thematic-analysis and open coding [14]. Two researchers independently coded four transcripts and discussed disagreements until a consensus was reached [35]. Then, the remaining transcripts were coded by one researcher similar to previous research [33].

3.3 Warnings

We created warnings to help introduce participants to various levels of attestation. These warnings were inspired by previous work related to robocall warnings [20, 53] and the explanations of attestation levels in the STIR/SHAKEN standards [**?**].

Full attestation, where the caller's service provider authenticates the caller, number and call origin, is expressed through the Authenticated Caller (Auth) and Number Verified (#Verf) warnings, shown in Figure 2a and 3a.

Partial attestation, where the caller's service provider authenticates the caller, call origin, and not the number, is expressed through the Unverified (UNverf) and +Icons[1] warning, shown in Figure 2b and 3b.

The *Gateway attestation*, where a service provider confirms that the call is coming from their network, is expressed through the Unverified + (Unver+) and Not Verified (Not Verf) warning, shown in Figure 2c and 3c.

4 Consumer Incoming Call Preferences

We asked participants (n=411) how they would like their service provider to handle incoming call information. We asked them to indicate the type(s) of information they would like to be verified, notified of, or calls they want to be blocked based on the verification results. The options provided for each question were derived from the levels of attestation. These questions were asked in a random order to each participant to prevent bias. The survey results are presented in this section.

4.1 User Preferences for Verified Information

Participants were asked to select the type of information they would like to be verified for a call. They had the following multiselect options:

1. Name of the caller
2. Number of the caller
3. Location of the caller
4. Service provider of the caller
5. If the call was allowed by the caller's service provider [2]
6. Other

[1] The inverse of the warning, where there was a checkmark near the name and X mark for the number and location was also shown.

[2] we recognize that this option is not necessarily related to levels of attestation. However, we acknowledge that

Table 3: Percent of Participants that Prefer Calls with Certain Information Unverified to be Blocked.

Please indicate which type of calls you would like your provider to block and not notify you about	% of Participants		
Options	**Block & Don't Notify (n=212)**	**Block & Notify (n=199)**	**Total (n=411)**
The name of the caller shown is unverified	45%	55%	50%
The number of the caller is unverified	45%	47%	64%
The location of the caller is unverified	62%	67%	46%
The service provider of the caller is unverified	27%	29%	28%
The call was allowed by the caller's service provider without caller id verification	20%	28%	24%
Other	6%	4%	5%

We found that the verification of names and numbers was important to most participants. The majority of participants indicated that they wanted the number (81%), name (77%), or both (65%) verified for incoming calls. This is not surprising as prior work has shown that users rely heavily on Caller ID and look at the number and name of incoming calls to determine how to respond [53, 61]. Full descriptive statistics are shown in Table 1.

4.2 User Notification Preferences

Participants were also asked to select their preference for verification notifications. Fifty-two percent of participants (n=212) were shown the word *unverified* in the multiple-choice options while the other 48% (n=199) were shown the word *verified*. They had the following multiselect options:

1. The name of the caller shown is (un)verified
2. The location of the caller is (un)verified
3. The number of the caller is (un)verified
4. The service provider of the caller is (un)verified
5. The call was allowed by the caller's service provider without Caller ID verification
6. Other

Significantly more participants (X^2 =13.36 , df = 1, p < .001, N=212,199, 95% CI[-.22, -.06]) indicated that they wanted to be notified when "The call was allowed by the caller's service provider without Caller ID verification" when shown alongside the unverified options (25%) compared to when it was shown alongside the verified options (11%). Overall, the response trends are similar for both groups, which suggests that asking users about unverified information may have encouraged them to read the options more carefully. There were no other significant differences between the remaining options for the verified and unverified questionnaire (see Figure 2). Overall, most participants wanted to be notified about the verification status of the number (72%), name (71%), or both (65%) of a caller.

4.3 User Preferences Regarding Blocked Calls

Participants were also asked about telephone carriers blocking calls for them. Fifty-two percent of participants (n=212) were asked to select the type of calls they wanted to be blocked and notified about while 48% (n=199) were asked to indicate the type of calls they wanted blocked without notification. Both groups had the following options:

1. The name of the caller shown is unverified
2. The location of the caller is unverified
3. The number of the caller is unverified
4. The service provider of the caller is unverified
5. The call was allowed by the caller's service provider without Caller ID verification
6. Other

There were no significant differences between the two groups (see Table 3), so we report descriptive statistics for the combined data. Overall, most participants wanted their provider to block calls from unverified numbers (64%) and names (50%).

5 Survey Participants' Reaction and Interpretation of Warnings

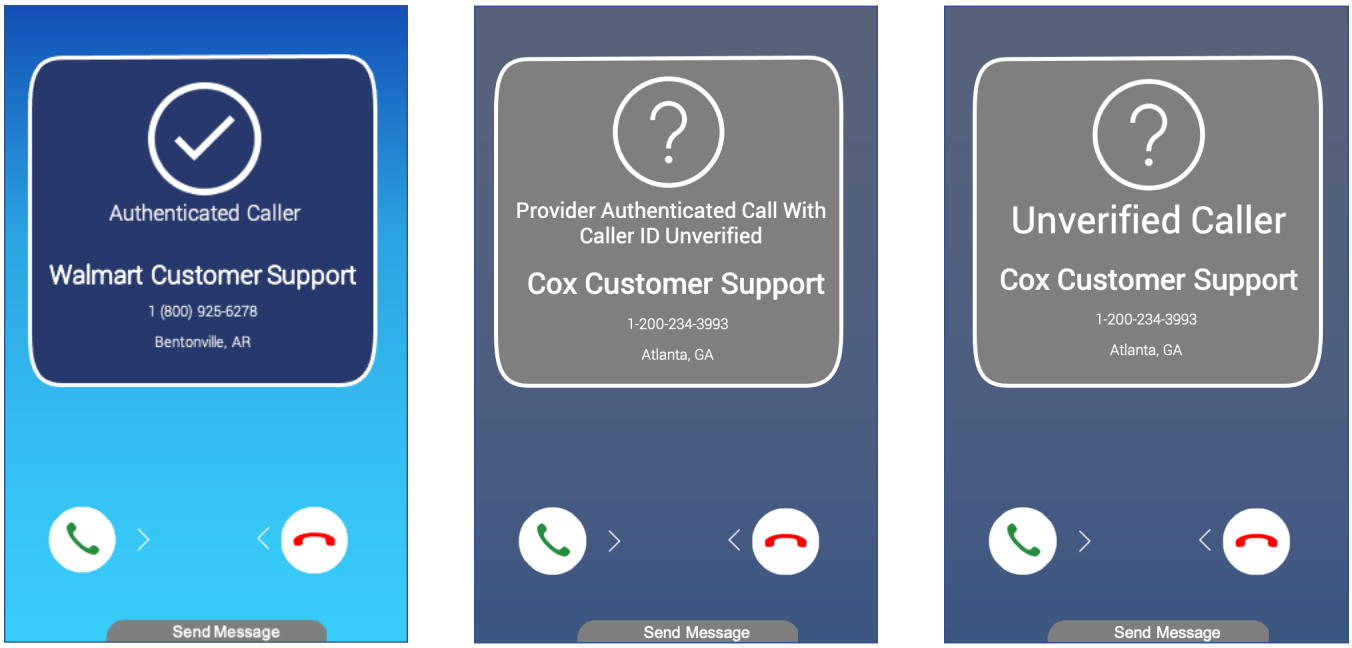
We also evaluated how users might react and interpret warnings that encompassed the survey options. We showed six warnings in the survey process, to expose participants to other possible incoming call scenarios, but will focus this section on the warnings that directly correlate to attestation levels, see Figure 2. Participants were asked to select the options they believed best matched their warning interpretation. They

Table 4: Participant Interpretation of and Response to the Unverified Warning

	% of Participants		
Interpretation of UNverf	**All (n=314)**	**Sighted (n=212)**	**Visually Impaired (n=102)**
All of the Caller ID information is unverified*^{o}	29%	24%	33%
Some of the Caller ID information is unverified*^{o}	42%	44%	31%
I should not answer this call^{x}	46%	39%	55%
It is not safe to answer this call^{x}	34%	31%	35%
The call was allowed but the Caller ID was not checked^{x}	10%	7%	17%
I don't know how to interpret this	13%	15%	7%
Other	4%	1%	9%
*Intended Response	62%	63%	61%
^{o}(All or Some) Information Unverified	62%	63%	61%
^{x}Unintended Meaning	63%	58%	73%
Response			
Answer	23%	29%	8%
Ignore	40%	33%	47%
Decline	42%	37%	45%

Table 5: Participant Interpretation of and Response to the Unverified+ Warning

	% of Participants		
Interpretation of Unverf+	**All (n=297)**	**Sighted (n=199)**	**Visually Impaired (n=98)**
All of the Caller ID information is unverified*^{o}	24%	25%	23%
Some of the Caller ID information is unverified^{o}	37%	38%	36%
I should not answer this call^{x}	44%	39%	56%
It is not safe to answer this call^{x}	26%	26%	27%
The call was allowed but the Caller ID was not checked*	21%	19%	24%
I don't know how to interpret this	13%	19%	1%
Other	3%	1%	7%
*Intended Response	40%	39%	43%
^{o}(All or Some) Information Unverified	57%	57%	57%
^{x}Unintended Meaning	77%	76%	78%
Response			
Answer	24%	26%	19%
Ignore	35%	32%	40%
Decline	41%	42%	41%



(a) Auth (b) Unverf+ (c) UNverf

Figure 2: This figure displays the three warnings shown in the user surveys. The FCC has not provided guidance on how carriers should alert users. Therefore, these are derived from previous research on spam call warnings [20, 53]. Figure 2a uses the phrase "Authenticated Caller", has a blue background color and has a check mark at the top. Figure 2b uses the phrase "Provider Authenticated Call With Caller ID Unverified" and includes a question mark icon. Figure 2c uses the phrase "Unverified Caller" and has a check mark icon at the top of the screen.

were also asked how they would respond to each type of call. These questions we asked in random order to avoid bias.

Participants from MTurk and NFB were shown or listened to the Auth (n=299), UNverf (n=297) and Unverf+ (n=314) warning, seen in Figure 2. For each warning, we asked the participants to select the options that best reflected their interpretation of the warning and asked them if they would answer the call. The purpose of this survey is to see how consumers might react to and interpret warnings related to various levels of attestation.

5.1 UNverf vs Unverf+

Within the two UNverf warnings, sighted and visually impaired participants responded to the warnings in significantly different ways (see Table 4 and 5). First, significantly more sighted participants said they should not answer the UNverf (X^2 =6.71 , df = 1, $p < .05$, N=102,212, 95% CI[.03,.29]) and Unverf+(X^2 =66.94 , df = 1, $p < .001$, N=98,199, 95% CI[.4,.62]) warning call (55%, 56%) compared to the visually impaired participants (39%, 39%). Second, significantly more sighted participants (X^2 =16.9 , df = 1, $p < .001$, N=102,212, 95% CI[-.3,-.13]) said they would answer the UNverf warning call (29%) compared to the visually impaired participants (8%). Lastly, significantly less (X^2 =16.63 , df = 1, $p < .001$, N=98,199, 95% CI[-.24,-.11]) visually impaired participants (1%) choose "I don't know how to interpret this" when interpreting Unverf+ compared to the MTuk workers (19%). This suggests that visually impaired consumers may be more likely to misinterpret unverified information to mean that they should not answer a call and thus not answer a call. Researchers should consider the impact of the word unverified on interpretation when heard versus when it is seen among other visual elements. We leave design choices to other work and instead point out the importance of considering universal design in creating these types of notifications. We also found that overall significantly more participants (X^2 =13.48 , df = 1, $p < .001$, N=297,314, 95% CI[.05,.17]) believed that *the Caller ID information was not checked* for Unverf+ (21%) than UNverf (10%). This was expected as the Unverif+ warning includes a longer phrase to communicate this information. However, most participants did not interpret the information as intended.

5.2 Auth vs Unverf+

Each warning included a label to inform the user about the information being shown. Auth included the phrase *Authenticated Caller*, whereas Unverf+ explicitly states that the *Caller ID [is] unverified*. However, significantly more participants

Table 6: Participant Interpretation of and Response to the Authenticated Call Warning

Interpretation of Auth	% of Participants		
	All (n=293)	**Sighted (n=195)**	**Visually Impaired (n=98)**
All of the Caller ID information is verified* [o]	68%	72%	61%
Some of the Caller ID information is true/verified[o] [x]	27%	31%	20%
I should answer this call [x]	50%	50%	50%
It is safe to answer this call [x]	25%	26%	24%
I don't know how to interpret this	2%	3%	0%
Other	5%	0%	15%
*Intended Response	78%	86%	63%
[o](All or Some) Information is Verified	85%	88%	80%
[x]Unintended Meaning	68 %	70%	64%
Response			
Answer	74%	79%	65%
Ignore	18%	16%	23%
Decline	6%	5%	9%

(X^2 =33.26 , df = 1, $p < .001$, N=293,297, 95% CI[.16,.32]) selected the answer that correlates to the label when shown Auth (68%) than Unverf+ (24%). This suggests that if carriers want to communicate Gateway Attestation to consumers, they need to be careful about the words and design elements they use. In this case, explicitly saying that the Caller ID information was unverified did not clearly correlate to how much information was not verified. This is likely due to Caller ID still being present, users understanding of unverified, and the use of conflicting words which we further discuss in Section 6.

5.3 Auth

Most participants interpreted Auth (see Figure 2a and Table 6) to mean that all the Caller ID information was verified (68%) and that they would answer such calls (74%). There was also a significantly larger (X^2 =28.39 , df = 1, $p < .001$, N=98,195, 95% CI[.07,.23]) proportion of visually impaired participants (15%) that wrote in their interpretation of the warning, compared to the sighted participants. Most of the participants that selected *other* (93% or 14 of the 15) used the space to mention that call appearing to be from Walmart would play into their interpretation and response.[3]. These written responses highlight the impact of Caller ID on user reaction to calls. For example, participants stated:

> "Thus far, I may or may not answer the calls but having Caller ID prepares me for how I want to handle them. No call scares or intimidates me."

> "If I had a reason to expect a call from customer service then I would answer it if I didn't expect a call from customer service I would not answer it"

> "If I wasn't expecting a call from Walmart support, I wouldn't answer it. I would assume that it was either a mistake or a spoofed number which had circumvented the authorization process. I wouldn't think (in this case) that an out of state call was automa[tic]"

6 Reaction and Interpretation of Warnings from the Interview Participants

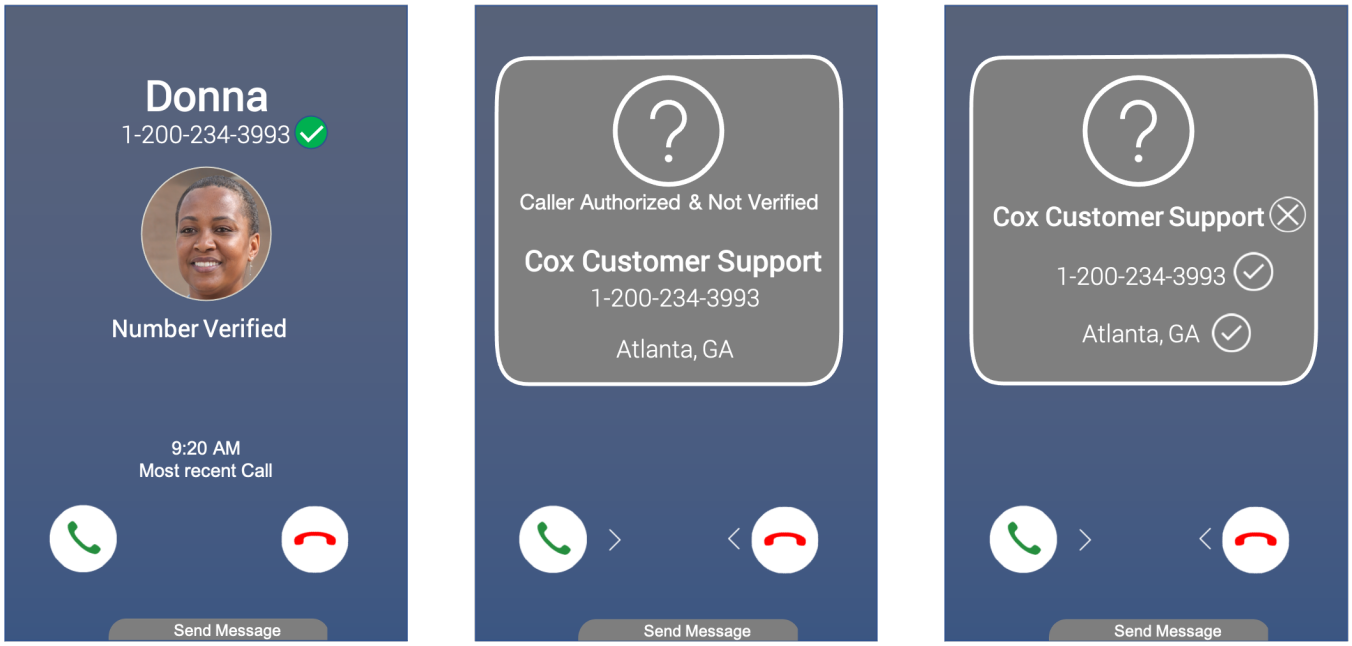
As a follow-up to the survey, we interviewed new participants about the warnings previously shown in the survey (Auth, UNverf, Unverf+), and a few additional designs (#Verf, Not Verf, +Icons). Participants were shown ten warnings during the interview process. However, we will only discuss how participants reacted to and interpreted those directly related to attestation levels, see Figure 2 and 3.

6.1 Interview Participants' Warning Interpretations

Auth. When asked how they would interpret the Auth warning (see Figure 2a), most participants indicated that the information present was likely accurate and that the call was not a spam call. For example, P4 stated the following:

> "I like the checkmark, and I like that it includes the name of the person calling. This is clear. I'd be happy if I saw this." -P4 (Sighted, Female, 60s)

[3]The other person used the space to say they didn't know how to react because they could not clearly see the warning and their screen reader was unable to read our description



(a) #Verf (b) Not Verf (c) + Icons

Figure 3: This figure displays the three additional warnings shown in the user interviews. The FCC has not provided guidance on how carriers should alert users. Therefore, these are derived from previous research on spam call warnings [20, 53]. Figure 3a uses the phrase "Number Verified" and has a checkmark near the number. Figure 3b uses the phrase "Caller Authorized & Not Verified" and includes a question mark icon. Figure 3c uses X marks and checkmarks to show that the phone number and name used may not be associated with one another.

However, some participants mentioned that the word verified was preferred over the word authenticated due to interpretation difficulties. For example, while participant P4 liked this design, they also said the following:

> "For me, the term that I prefer is verified... When I look at these other terms, authenticated, authorized, I think there's confusion. " -P4 (Sighted, Female, 60s)

Most participants preferred the word verified over authenticated due to interpretation difficulties and the simplicity of the word verified. This was a consistent pattern between both sighted and blind participants. Many participants understood both words but believed the word *verified* was simpler, easier to interpret at a glance, or a less confusing word. Some blind participants requested the change of words since the shorter word is easier to interpret when listening to the warning. For example, P10, P15 stated the following:

> "Yes [I prefer verified]...Verified has the implication of [something] being checked..Unauthenticated is too long of a word...Potential spam is good [and my preferred phrase]. Unverified, it seems like I would say no [to answering that call] immediately." -P10 (Blind, Female, 40s)

> "I don't know if it [screen reader] really needs to say authenticated call, you know what I mean. Just seems like a long word... I don't know I think it's , I think it's kind of long. " -P15 (Blind, Male, 60s)

#Verf. As shown in Figure 3a, we also showed or played a warning that used the phrase *Number Verified*. Similar to Auth, participants interpreted this to mean the Caller ID information was correct and the call was not spam. For example, participant P13 and P20 stated the following:

> "I like that... I like that because one it tells you that it's it's a person and if you know a Donna Jones or even if you don't at least you know who's going to be on the other end of the call." -P13 (Blind, Male, 60s)

> " I glanced at that and I'd say okay that's my friend Donna. It's been verified that it's Donna and so I [would] definitely take that call you know to the extent that I could or wanted to. " -P3 (Sighted, Male, 50s)

UNverf. Most participants understood this design (see Figure 2c) to mean that the carrier was unable to determine if

this call was spam or a legitimate call. When we asked participants to explain what they thought the warning was trying to convey, some participants replied as follows:

> " I guess if you don't know what Cox customer support is then they don't really have no business calling you. but also because it says like unverified that also makes me think that maybe it's not even cox customer support." -P6 (Sighted, Female, 20s)

> "Ok now that one I wouldn't answer. unverified caller. I like the verbage. In other words they haven't provide their Caller ID or their phone number. " -P7 (Sighted, Male, 70s)

> "Like the cell phone provider is a real company but they don't know where the call or who to call is coming from... it makes me think of like a call center when it's... all one company but several different lines like several different extensions so they don't. I don't know like it's like maybe that extension isn't associated with a particular name or something " -P14 (Sighted, Female, 30s)

Not Verf & Unverf+ While most participants appreciated the warning's visual aspect, they did not like the phrases selected. They had difficulty determining why this would matter and why a carrier would authenticate or authorize a call without verifying the Caller ID information. Additionally, blind participants believed that the phrases used were too long and that a simpler phrase would suffice. Some participants stated the following when shown warnings with the long-phrase:

> " i'm very confused i'm not sure what that means...who authorized what, what is authorized for what..[and it's] not verified. It just tells me that it's.. they cannot verify that it's actually Cox, maybe?" -P16 (Sighted, Male, 20s)

> " So they're authorized to call me but they're not verified. I would take that mean that is a spam call and but it's okay they're authorized? That's cool but they're not verified so they're probably not real and again I still don't know who Cox is...But that's a rather long thing for it to say. Spam risk is two words, but all those words is a lot of words." -P11 (Blind, Female, 60s)

We also showed +Icons, a warning of unverified information that used icons instead of a phrases, to express that the name and number might not be associated with one another. Even though participants understood what was being conveyed, participants did not like the additional work required of them. For example, one participant stated the following:

> " I think it's kind of too much going on because like when you're going to answer a phone call, I don't really think you're trying to read that much information or decipher that much. Like okay is it really this place, is it really this number. Okay but that's not who it is. It's kind of like when you answer the phone call you're just looking at it and kind of making a quick decision." -P6 (Sighted, Female, 20s)

6.2 Interview Participants' Reactions to Warnings

When asked how they might react, all responses were based on the Caller ID information present. Although most participants stated that they would be more likely to answer calls that were confirmed as legitimate, all responses were dependent on the Caller ID information present. For example, a few of the responses are as follows:

> " I mean again this is a call that I would not take. I would not accept, probably would not even return this call because again I have no interest in the merchandise of the alleged merchant. " -P1 (Blind, Female, 60s)

> " I wouldn't, I wouldn't answer it because we don't have Cox in our area. " -P9 (Blind, Female, 60s)

> " I would be skeptical you know. If... I had reached out to Cox for something maybe [I wouldn't be skeptical]... But if ...they're just calling to say "hey how are things going", which they don't [usually] do, again I'd be skeptical " -P4 (Sighted, Female, 20s)

7 Limitations

We used MTurk as a way to get a larger number of responses to the incoming call warnings. We recognize that there are limitations in sample demographics for MTurk. However, as previous work has found, using crowd worker platforms is sufficient for security-related research [43].

This study is also limited by the number of warnings tested in both the survey and interviews. Interviewing participants about some warnings where there are no survey results could make it challenging to correlate user feedback to survey responses. However, this study aims to identify the challenges of communicating STIR/SHAKEN and how consumers comprehend various levels of attestation. It is not necessary to make direct comparisons for every warning shown. The warnings are used as a conduit to display concepts to users. Thus, we can make comparisons for concepts. We encourage future work to investigate using warnings for this context and how those warnings should appear to users.

8 Discussion

This research aimed to identify the communication challenges with STIR/SHAKEN implementation and encourage design or communication guidelines to assist carriers in this process. This section discusses the results of our user studies and reveals challenges for future work.

8.1 Consumers Preferences without VoIP

Our results suggest that consumers prefer that Caller ID information (name and number) be verified. Not only do consumers rely on Caller ID to determine if they will answer a call, but our work also suggests they would like to be notified about the verification status of information and prefer calls be blocked based on verification. Providing users with this information is beneficial as it encourages answering legitimate calls from unfamiliar numbers [53]. Additionally, providing users with additional accurate information about the Caller ID can increase their trust in the technology [20]. However, since STIR/SHAKEN will only work over VoIP, and carriers will be unable to fully attest for all calls, consumer preferences will not be met for all legitimate calls. **Therefore, the first challenge is to determine how to communicate information to users about VoIP calls without negatively impacting incoming calls from non-VoIP networks.**

8.2 Communicating Facts

Similar to prior work [20], we used definitive and unbiased phrases in this study to prevent influencing user assumptions about a caller's intent. Our results suggest that definitive phrases may not impact what users believe the intent of a verified or unverified call might be, but the Caller ID information might. When discussing the various warnings in the interviews, our participants did not mention a call's intent except when talking about the name and number presented. For example, when users saw an unverified call from Cox Communications, they assumed a particular intent if they did not have business with Cox. Therefore, they would not answer the calls. In the surveys, most participants (>65% in every case) did not use the warning to determine if answering the call would be a safe choice. For example, when shown Auth, 50% of the participants believed that they should answer the call, and only 25% believed it was safe to answer the call. Still, 74% said that they would answer the call. Most participants did not believe the call from Walmart was safe to answer, yet most participants thought they should answer the call and indicated that they would answer the call. **Therefore, the second challenge is to determine how to inform users about verified or unverified information without encouraging them to make choices despite believed intent.** STIR/SHAKEN is not foolproof, and spammers can still use legitimate numbers to make spam calls that appear legitimate. The information communicated to users should provide facts but not encourage users to override their instincts.

8.3 The Use of Warnings

In an attempt to test how consumers might make sense of partial and gateway attestation, we display various phrases in the survey (see Table 1, 2, and 3) and in the interviews (see Figure 2 and 3). We understand that these phrases may not be the best phrases to describe these levels. However, we tested multiple variations to understand better how various visual and audible representations of the same concepts might impact user understanding of STIR/SHAKEN attestations. We found that users were confused by the longer phrases and, in some cases, were unsure of how to proceed due to conflicting words being used. The survey responses also highlight that longer phrases may not work for more complicated attestations, primarily since they do not provide the user with the information they see as useful. This is evidenced by most participants discussing that they would respond to these warnings based on the Caller ID information displayed. **Therefore, the third challenge is to determine which levels of attestation carriers should alert users about and how those warnings should be designed.**

We bring forth these challenges and encourage research to determine best practices for communicating call information before STIR/SHAKEN is implemented worldwide. Since user adoption of wireless technology is influenced by their perceived usefulness and ease of use [19, 66], carriers would benefit from acknowledging and solving these challenges to provide users with useful information and easier transition to STIR/SHAKEN.

9 Related Work

When consumers' experiences are sought and considered, researchers or practitioners can use them to improve and inform technology standards and policy [8]. The continuous usability evaluation of technology has provided improvements in accessibility and security.

The World Wide Web Consortium has provided accessibility guidelines developed by various researchers over time for online content. These guidelines are used internationally to evaluate the accessibility of various websites [3, 24, 26, 28, 64] and mobile applications [15, 47, 51] to encourage companies to make their content accessible. These guidelines are also used to help organizations become compliant with Section 508 of the Rehabilitation Act, which requires federal agencies to use, create or produce accessible technology and content.

Additionally, the 2000 U.S presidential election put voting usability and accessibility challenges under the spotlight after the close election results became dependent on counting confusing ballots. In response, the U.S Congress passed the Help America Vote Act in 2002 to combat these issues.

Since then, researchers have continued to investigate the accessibility [50, 54, 56] and usability [9, 29, 40, 57] of voting processes independently and with voting, officials to inform future elections.

Researchers have also investigated the accessibility and usability of mechanisms used to communicate information about privacy or security to the end-user. For example, prior work shows that users have difficulty understanding privacy policies [30] and may not read it in its entirety [37]. In response, researchers have suggested various ways to improve how privacy policy information is presented [1, 17, 32, 49]— ultimately helping to inform how organizations present privacy policy information to users. Additionally, researchers have worked to improve communication of security threats through extensive work on warning designs for web browsers [2, 21–23, 44–46, 58, 65], software [12], malware [5], app warnings [53, 55] and warning fatigue [11], which ultimately help to encourage users to make safe decisions while online.

Similar to other researchers [8, 25, 31], the authors of this work encourage others to participate in policy development, technology standards, or related activities.

10 Conclusion

The FCC has mandated call authentication mechanisms and not the communication of verification results [16]. This is understandable as it will take time for some service providers to upgrade their infrastructure to support STIR/SHAKEN. However, when usability is an afterthought, consumers often suffer. Technology can be ineffective if consumers do not know how to use it. Research has shown that there may be trade-offs when making security technology usable. However, warning design and communication standards are crucial and should be a part of the mandate. We identify the challenges that might arise with communication STIR/SHAKEN results to users in this work. We find that users prefer that information be verified due to previous experience with Caller ID. Due to this, users have difficulty determining how to apply partial and gateway attestation in their decision-making and ultimately ignore it. Thus, how should carriers inform their consumers, if at all, about various attestation levels? Additionally, since STIR/SHAKEN is for VoIP calls only, we encourage more research on applying this without negatively impacting non-VoIP calls. We encourage the ongoing development of design guidelines to assist carriers in implementing STIR/SHAKEN communication due to these challenges.

References

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017.

[2] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium*, pages 257–272, 2013.

[3] Hend S Al-Khalifa, Ibtehal Baazeem, and Reem Alamer. Revisiting the accessibility of saudi arabia government websites. *Universal Access in the Information Society*, 16(4):1027–1039, 2017.

[4] Alliance for Telecommunications Industry Solutions. Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, 2017.

[5] Hazim Almuhimedi, Adrienne Porter Felt, Robert W Reeder, and Sunny Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *Symposium on Usable Privacy and Security*, 2014.

[6] Richard A Armstrong. When to use the bonferroni correction. *Ophthalmic and Physiological Optics*, 34(5):502–508, 2014.

[7] Vijay A Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael T Hunter, and Patrick Traynor. Pindr0p: using single-ended audio features to determine call provenance. In *ACM SIGCSAC CCS*, pages 109–120, 2010.

[8] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. Is your inseam a biometric? A Case Study on the Role of Usability Studies in Developing Public Policy. *Proc. USEC*, 14, 2014.

[9] Benjamin B Bederson, Bongshin Lee, Robert M Sherman, Paul S Herrnson, and Richard G Niemi. Electronic voting system usability issues. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 145–152, 2003.

[10] Adam J Berinsky, Gregory A Huber, and Gabriel S Lenz. Using mechanical turk as a subject recruitment tool for experimental research. *Political Analysis*, pages 351––68, 2011.

[11] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Harder to ignore, revisiting pop-up fatigue and approaches to prevent it. *USENIX Association*, pages 105–111, 2014.

[12] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Symposium on Usable Privacy and Security*, page 6. ACM, 2013.

[13] Michael Buhrmester, Tracy Kwang, and Samuel D Gosling. Amazon's mechanical turk: A new source of inexpensive, yet high-quality data? *American Psychological Association*, 2016.

[14] Philip Burnard. A method of analysing interview transcripts in qualitative research. *Nurse education today*, 11(6):461–466, 1991.

[15] Lucas Pedroso Carvalho, Bruno Piovesan Melchiori Peruzza, Flávia Santos, Lucas Pereira Ferreira, and André Pimenta Freire. Accessible Smart Cities? Inspecting the accessibility of Brazilian municipalities' mobile applications. In *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems*, pages 1–10, 2016.

[16] Federal Communications Commission. FCC Mandates STIR/SHAKEN to Combat Spoofed Robocalls. 2020.

[17] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 10:273, 2012.

[18] Dave Crocker, Tony Hansen, and Murray Kucherawy. Domain Keys Identified Mail (DKIM) Signatures. *ser. RFC6376*, 2011.

[19] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management science*, 35(8):982–1003, 1989.

[20] Gregory W Edwards, Michael J Gonzales, and Marc A Sullivan. Robocalling: STIRRED AND SHAKEN!-An Investigation of Calling Displays on Trust and Answer Rates. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[21] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074, 2008.

[22] Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving ssl warnings: Comprehension and adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2893–2902. ACM, 2015.

[23] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security*, pages 1–14, 2016.

[24] Nádia Fernandes, Daniel Costa, Carlos Duarte, and Luís Carriço. Evaluating the accessibility of web applications. *Procedia Computer Science*, 14:28–35, 2012.

[25] Harry Hochheiser and Jonathan Lazar. Hci and societal issues: A framework for engagement. *International Journal of Human Computer Interaction*, 23(3):339–374, 2007.

[26] Jiayi Hu, Meng Zhen, Cristina Olteanu, and Ronen Avram. An evaluation of accessibility and content of microsurgery fellowship websites. *Plastic Surgery*, 24(3):187–190, 2016.

[27] Panagiotis G Ipeirotis. Demographics of mechanical turk. *NYU working Paper No. CEDER-10-01*, 2010.

[28] Arvinder Kaur, Diksha Dani, and Gaurav Agrawal. Evaluating the accessibility, usability and security of hospitals websites: An exploratory study. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pages 674–680. IEEE, 2017.

[29] Bridgett A King and Norman E Youngblood. E-government in alabama: An analysis of county voting and election website content, usability, accessibility, and mobile readiness. *Government Information Quarterly*, 33(4):715–726, 2016.

[30] Alan Levy and Manoj Hastak. Consumer comprehension of financial privacy notices. *Interagency Notice Project*.

[31] Clayton Lewis and Jutta Treviranus. Public policy and the global public inclusive infrastructure project. *Interactions*, 20(5):62–66, 2013.

[32] Bin Liu, Jialiu Lin, and Norman Sadeh. Reconciling Mobile App Privacy and Usability on Smartphones: Could user privacy profiles help? In *Proceedings of the 23rd International Conference on World Wide Web*, pages 201–212, 2014.

[33] Matthew Lombard, Jennifer Snyder-Duch, and Cheryl Campanella Bracken. Content Analysis in Mass Communication: Assessment and Reporting of Intercoder Reliability. *Human communication research*, 28(4):587–604, 2002.

[34] Federico Maggi. Are the con artists back? a preliminary analysis of modern phone frauds. In *10th IEEE CIT*, pages 824–831, 2010.

[35] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[36] H. Mustafa, W. Xu, A. R. Sadeghi, and S. Schulz. You can call but you can't hide: Detecting caller id spoofing attacks. In *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 168–179, June 2014.

[37] Jonathan A Obar and Anne Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, 2020.

[38] Sharbani Pandit, Roberto Perdisci, Mustaque Ahamad, and Payas Gupta. Towards measuring the effectiveness of telephony blacklists. In *NDSS*, 2018.

[39] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. Reputation as a sufficient condition for data quality on amazon mechanical turk. *Behavior research methods*, 46(4):1023–1031, 2014.

[40] Gillian E Piner and Michael D Byrne. Baseline usability data for a non-electronic approach to accessible voting. In *EVT/WOTE*, 2010.

[41] Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *26th USENIX Security Symposium* , pages 575–592, Vancouver, BC, 2017.

[42] Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016.

[43] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How well do my results generalize? Comparing Security and Privacy Survey Results from Mturk, Web, and Telephone Samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1326–1343. IEEE, 2019.

[44] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. You want me to do what? a design study of two-factor authentication messages. In *Symposium on Usable Privacy and Security*, 2017.

[45] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the CHI conference on human factors in computing systems*, pages 1–13, 2018.

[46] Richard Roberts, Yaelle Goldschlag, Rachel Walter, Taejoong Chung, Alan Mislove, and Dave Levin. You are who you appear to be: a longitudinal study of domain impersonation in tls certificates. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2489–2504, 2019.

[47] Anne Spencer Ross, Xiaoyi Zhang, James Fogarty, and Jacob O Wobbrock. Examining image-based button labeling for accessibility in android apps through large-scale analysis. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 119–130, 2018.

[48] Merve Sahin, Marc Relieu, and Aurélien Francillon. Using chatbots against voice spam: Analyzing lenny's effectiveness. In *Symposium on Usable Privacy and Security*, pages 319–337, 2017.

[49] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security*, pages 1–17, 2015.

[50] Lisa Schur, Meera Adya, and Mason Ameri. Accessible Democracy: Reducing Voting Obstacles for People with Disabilities. *Election Law Journal*, 14(1):60–65, 2015.

[51] Leandro Coelho Serra, Lucas Pedroso Carvalho, Lucas Pereira Ferreira, Jorge Belimar Silva Vaz, and André Pimenta Freire. Accessibility evaluation of e-government mobile applications in brazil. *Procedia Computer Science*, 67:348–357, 2015.

[52] Amit Sheoran, Sonia Fahmy, Chunyi Peng, and Navin Modi. Nascent: Tackling caller-id spoofing in 4g networks via efficient network-assisted validation. In *IEEE INFOCOM*, pages 676–684, 2019.

[53] Imani N Sherman, Jasmine D Bowers, Keith McNamara Jr, Juan E Gilbert, Jaime Ruiz, and Patrick Traynor. Are you going to answer that? measuring user responses to anti-robocall application indicators.

[54] Simone A Smarr, Imani N Sherman, Brianna Posadas, and Juan E Gilbert. Prime III: Voting for a More Accessible Future. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 335–336, 2017.

[55] Vlasta Stavova, Lenka Dedkova, Vashek Matyas, Mike Just, David Smahel, and Martin Ukrop. Experimental large-scale review of attractors for detection of potentially unwanted applications. *Computers & Security*, 76:92–100, 2018.

[56] Kathryn Summers, Dana Chisnell, Drew Davies, Noel Alton, and Megan McKeever. Making Voting Accessible: Designing Digital Ballot Marking for People with Low Literacy and Mild Cognitive Disabilities. In *2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14)*, 2014.

[57] Kathryn Summers and Jonathan Langford. The impact of literacy on usable and accessible electronic voting. In *International Conference on Universal Access in Human-Computer Interaction*, pages 248–257. Springer, 2015.

[58] J Sunshine, S Egelman, H Almuhimedi, N Atri, and LF Cranor. Usenix security symposium. *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*, pages 399–416, 2009.

[59] Aimilia Tasidou, Pavlos S Efraimidis, Yannis Soupionis, Lilian Mitrou, and Vasilios Katos. Privacy-preserving, user-centric VoIP CAPTCHA challenges. *Information & Computer Security*, 2016.

[60] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Toward authenticated caller id transmission: The need for a standardized authentication scheme in q. 731.3 calling line identification presentation. In *ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT)*, pages 1–8. IEEE, 2016.

[61] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Users really do answer telephone scams. In *28th {USENIX} Security Symposium*, pages 1327–1340, 2019.

[62] Daniele Ucci, Roberto Perdisci, Jaewoo Lee, and Mustaque Ahamad. Towards a Practical Differentially Private Collaborative Phone Blacklisting System. In *Annual Computer Security Applications Conference*, pages 100–115, 2020.

[63] Monica Vaca. The top frauds of 2019. *FTC.gov*, 2020.

[64] Silas Formunyuy Verkijika and Lizette De Wet. Accessibility of south african university websites. *Universal Access in the Information Society*, 19(1):201–210, 2020.

[65] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In *Proceedings of the 2018 World Wide Web Conference*, pages 217–226, 2018.

[66] David C Yen, Chin-Shan Wu, Fei-Fei Cheng, and Yu-Wen Huang. Determinants of users' intention to adopt wireless technology: An empirical study by integrating ttf with tam. *Computers in Human Behavior*, 26(5):906–915, 2010.

A Demographics

Table 7: Survey and Interview Demographics Data

Demographics	Survey (n=806)	Interview (n=20)
Gender		
Female	46%	50%
Male	53%	50%
Non-binary	1%	0%
Prefer not to answer	0%	0%
Age		
18-22	2%	5%
22-30	27%	10%
31-40	32%	20%
41-50	19%	5%
51-60	11%	20%
Over 60	8%	35%
Prefer not to answer	0%	5%
Race/Ethnicity		
White	79%	60%
Hispanic or Latino	6%	5%
Black or African American	8%	25%
Native American or American Indian	2%	5%
Asian	6%	15%
Native Hawaiian or Pacific Islander	0%	0%
Other	1%	0%
Prefer not to answer	2%	5%
Education		
Some high school credit, no diploma or equivalent	1%	0%
High school graduate (high school diploma or equivalent including GED)	9%	5%
Some college but no degree	14%	11%
Associate's degree	7%	16%
Bachelor's degree	50%	32%
Advanced degree (e.g., Master's, doctorate)	18%	32%
Prefer not to answer	2%	5%