A Survey of the Privacy Preferences and Practices of Iranian Users of Telegram

Elham Vaziripour
Brigham Young University
elhamvaziripour@byu.edu

Reza Farahbakhsh
Institut Mines Télécom, Telecom SudParis
reza.farahbakhsh@it-sudparis.eu

Mark O'Neill
Brigham Young University
mto@byu.edu

Justin Wu
Brigham Young University
justinwu@byu.edu

Kent Seamons
Brigham Young University
seamons@cs.byu.edu

Daniel Zappala
Brigham Young University
zappala@cs.byu.edu

***Abstract*—Telegram is a secure messaging application that offers a wide variety of privacy and security features, but these features must be activated or chosen by users, rather than being turned on by default. At the same time, Telegram has a large number of users in Iran, who may potentially have a high need for privacy and security. In this paper, we present a survey of about 400 Iranian users of Telegram, living both inside and outside of Iran, exploring their privacy preferences and their use of Telegram's available privacy and security features. We find that the overwhelming majority of respondents feel it is important that messaging applications protect the privacy of their messages, yet their adoption of the available privacy and security features is mixed. We discuss in detail these varying practices and how the design of Telegram influences adoption of various features. We finish by discussing recommendations for improving the design of Telegram and similar secure messaging applications so that they place a greater priority on protecting privacy.**

I. Introduction

Recent disclosures of government surveillance in the United States and other countries, as well as fears over cybersecurity attacks, have increased interest in secure and private communication. In response to this demand, numerous secure messaging apps have been developed in recent years. Applications such as WhatsApp, Signal, and Viber encrypt all messages by default, using end-to-end encryption between the devices of communicating partners, so that the service provider is unable to view the content of messages and passive monitoring by a government or hacker is not possible. Other applications use plaintext messaging, with encrypted chat as an optional feature, including Facebook Messenger and Telegram.

An important question is whether secure messaging applications are meeting the security and privacy needs of their users. Of particular concern are those countries that practice censorship and restrict civil liberties, including blocking access to social media and communications applications, blocking access to content, and arresting journalists and bloggers [17]. Are citizens of these countries, in those cases where secure messaging apps are not blocked, able to effectively use the privacy and security features at their disposal?

One of the few studies in this area, by Rashidi et al., examined the privacy practices of WhatsApp users in the Kingdom of Saudi Arabia [27]. This study found that many users had changed their privacy settings and had blocked unwanted contact, but also wanted more control over their privacy. They did not examine the use of security features in WhatsApp. Other work has studied users of Telegram, but only in interviews within a lab setting [1], [2].

Telegram is a particularly interesting subject for study because of its widespread usage among the Iranian populace. One study estimates that Telegram is used by approximately 40 million users in Iran [16], with many residents using it daily, primarily to chat with friends and family [7]. From a technical perspective, Telegram is interesting because, in contrast to WhatsApp, Telegram's encrypted chat functionality is optional, a decision that has been criticized by privacy advocates [33]. Similarly, Telegram provides users a wide array of privacy and security features that they must opt into using. Privacy features include the ability to control who can see the last time they were active, who can call them or add them to a group, and who can send them messages. Security features include adding a passcode lock to the app, enabling two-step verification, and using end-to-end encrypted chat. Understanding how these features are used can help improve messaging application design. Given the sensitivity of information that can be discussed online, it is important to understand whether these features are being used. For example, Telegram has been used for sharing political views, resulting in the closure of some channels and the arrest of the users who managed them [16], [13].

Accordingly, we have conducted the first large-scale survey of Iranian users of the Telegram secure messaging application to seek insight into how they use the privacy and security features it offers. Specifically, we are interested in understanding (1) how participants perceive the importance of secure messaging; (2) why participants use Telegram; (3) whether they use Telegram to send sensitive information, why or why not, and the general

Workshop on Usable Security (USEC) 2018
18 February 2018, San Diego, CA, USA
ISBN 1-891562-53-3
https://dx.doi.org/10.14722/usec.2018.23033
www.ndss-symposium.org

strategies they use to protect their privacy; (4) how participants use the privacy features of Telegram; and (5) how participants use the security features of Telegram, including whether they use the authentication ceremonies in encrypted chat and phone calls. We used snowball sampling and some advertising on Twitter to distribute our survey, and, after filtering for unfinished responses, our final data set totals 392 responses.

An important aspect of our work is in analyzing the differences between participants living in Iran versus those living outside Iran. Do the differences in environment translate into differences in perceived threat models, and do these, in turn, translate into differences in adopted attitudes and behaviors? Because our sample population is largely homogeneous while including members both inside and outside Iran, it has the potential to offer great insight into these questions, and this is one focal point of our analysis.

Our results indicate that privacy is important to the vast majority of participants, yet half have shared sensitive information on Telegram, and a primary factor is trust in the security of Telegram. Use of privacy and security features is mixed, with high usage for blocking and editing or deleting messages, but low usage of security features. There is a significant lack of understanding of what encrypted chat does and the security guarantees it provides for users. Participants living in Iran were more likely to rate privacy as extremely important to them, more likely to use Telegram daily, and yet are also more likely to share sensitive information while using Telegram. Based on these findings we make several recommendations for improving the privacy and security of Telegram and similar secure messaging applications.

Artifacts: We have created a companion website at `https://telegram.internet.byu.edu` that provides the survey questions, anonymous participant responses, coded data for open response questions, and a script that calculates relevant summary tables and statistics. For convenience we also include the survey questions and summary tables of the responses in the Appendix.

II. Related Work

Two papers have examined questions relating to use of security and privacy features in secure messaging applications in particular countries. Rashidi et al. conducted a study of the privacy practices of 626 WhatsApp users in the Kingdom of Saudi Arabia [27]. They found that majority (59%) had changed at least one privacy setting, with about 45% changing who could see their *last seen* status, while about 25% changed who could see their profile photo or status. They also found that 2/3 had been contacted by strangers and 75% had used the blocking feature. Church et al. previously studied a very early version of WhatsApp and used a survey of 131 residents of Spain to show that users were concerned about showing their *last seen* status and the delivery status of their messages [8].

Other work that studies Telegram includes a paper by Abu-Salma et al. that conducted a user study of Telegram's security features [1] with 22 participants. They found at most partial adoption of Telegram for its security features, and those who had used the tool previously often abandoned it for a more popular app. Participants tended to use other methods, such as phone calls or meeting in person, to exchange sensitive information, rather than using Telegram. They also found some confusion about the functionality of *secret chat* and the self destruct timer. Another paper by Abu-Salma et al., while focused primarily on adoption of secure messaging, touches on use of Telegram [2]. They found that all of the participants who used Telegram did not use *secret chat*, due to the overhead of switching between the default and secure mode, or because they forget to use it. Only one participant was able to explain the key fingerprints used in the authentication ceremony, most participants did not setup a passcode, and most felt calls and SMS were more secure than secure messaging apps.

Part of our work concerns how users adopt the security features available to them. Renaud et al. [28] found that lack of usability was not the primary reason for users not adopting end-to-end encrypted emails; rather, incomplete threat models, misaligned incentives and general absence of understanding of email security are the main obstacles. Abu-Salma et al. studied the adoption of secure messaging and found that fragmentation of users among a variety of applications and lack of interoperability are the primary obstacles to adoption; users feel that secure messaging applications cannot provide protection against strong adversaries [2]. Work by De Luca et al. also showed that people use secure messaging applications because of peer influence, not due to security concerns [10].

We are also interested in users' privacy preferences. The Android permission system is intended to inform users about the sensitive data an application will access and give them the ability to cancel installation if they do not approve. One study examined the effectiveness of this system and found low attention rates and extremely low comprehension [14]. Subsequent work has proposed a personalized privacy assistant application that could motivate users to review and modify their privacy settings with the aid of privacy nudges [23]. MacNamara et al. [25] showed that those who have a more independent decision-making style tend to be more conservative in sharing personal information. Dupree et al. [12] have clustered users based on their attitudes and practices toward security practices. Acquisti and Grossklags [3] suggested that users are likely to trade off their long-term privacy for short-term benefits in making privacy-sensitive decisions.

We note that Telegram uses a custom protocol, known as MTProto, to provide end-to-end encryption. This is considered poor practice by cryptographers [33], since it is difficult to create a secure protocol on your own, and there is an alternative protocol, Signal, that is well accepted by cryptographers and has been audited extensively [9]. A variety of flaws in MTProto have been found [20], [19], [21], [29].

III. Telegram

Telegram is a free instant messaging application, launched in 2013, that enables users to send messages of any type to each other, including photos, videos, audio messages, or other files. Messages can be sent to individuals, with optional end-to-end encryption, or to groups (200 members maximum), supergroups (20,000 members maximum), and channels (unlimited, public). Messages can be synchronized across mobile, desktop, and web platforms. Telegram has a wide range of privacy and security features that it promotes, particularly encrypted and self-destructing messages. Telegram announced in February,

2016 that it had 100 million monthly users[1]; it has an estimated 40 million users in Iran [31]. Telegram recently added a new voice calling feature, but this has been blocked in Iran [5].

Telegram offers several different privacy and security settings, shown in Figure 1a. Under the category of privacy settings, users can control who is able to see their *last seen* status (time last active in the application), who can call them, and who can add them to groups. These settings all allow three options: *everybody*, *my contacts*, and *nobody*. Telegram also lets users block each other; blocking someone means they can't message you and can't see your *last seen* status.

Under the category of security settings, Telegram provides two additional options. Users can set a passcode lock that can lock access to all chats in the app, which also allows the option of using fingerprint unlock on compatible phones. Users can also enable two-step verification, which sets an additional password that is required when logging in from a new device, in addition to the code received over SMS. This provides additional security against SMS attacks. There have been recent SMS attacks against Telegram reported in both Iran and Russia [18], [26].

Telegram offers two distinct types of individual (person-to-person) messaging. The default messaging in Telegram, which they call *cloud chat*, encrypts messages between users and the Telegram server, but does not use end-to-end encryption. Telegram also offers end-to-end encrypted chats, which they call *secret chat*, which uses a form of end-to-end encryption. When a user deletes a message in a secret chat, it is deleted for both participants. Secret chat also includes a self-destruct feature, controlled by a user-settable timer. Telegram justifies the use of two different types of chat as providing two different use cases, and claims that cloud chat enables Telegram to be used more broadly, so that activists and dissidents are not singled out as being the only ones using their platform.[2]

To initiate a secret chat, a user can click on *New Secret Chat* in the main menu, shown in Figure 1b, or click on a friend's name in a cloud chat and then click on *Start Secret Chat*. An important part of using secret chat securely is to perform the authentication ceremony, which is a process for verifying the integrity of the exchanged encryption keys. Users have the option of checking whether a graphical representation of the key is identical (which would typically be done in person) or whether a decimal representation of the key is identical (which could be done with a phone call). Interestingly, Telegram provides a different authentication method for voice calls, which use end-to-end encryption by default. In this case, users can compare a representation of the key that uses *emojis*.

IV. Methodology

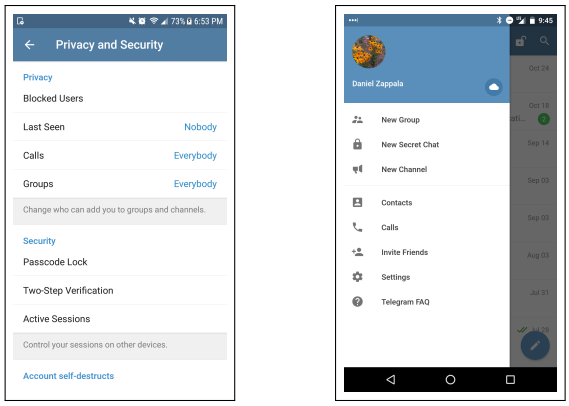
We conducted an IRB-approved, web-based survey to ask Iranian Telegram-users about their perceptions, preferences, and use of this secure messaging application.

A. Survey Development and Distribution

In designing our questionnaire, we began by first exploring the features available in Telegram and drafting questions about

[1]https://telegram.org/blog/100-million

[2]https://telegram.org/faq#q-why-not-just-make-all-chats-secret



(a) Privacy and security settings (b) Initiating a secret chat

Fig. 1: Privacy and security in Telegram

user preference and use of the application. We then reviewed these questions in several rounds of discussion with co-authors and other collaborators. We refined the survey in English, and then one of the authors, a native speaker of Farsi, translated it into Farsi. Before running the survey, a pilot study with 20 participants was conducted in both English and Farsi. Feedback from the pilot study was used to revise the final wording and translations of the questionnaire.

We distributed the survey using the Qualtrics platform and recruited participants via snowball sampling. Two of the authors, native Iranians, asked Iranian friends (living both inside and outside of Iran) who used Telegram to take the survey and share it with their friends. The survey was also publicized on Twitter by tweeting it at approximately 2,000 Farsi speakers over a period of several weeks, in an attempt to mitigate the negative effects of snowball sampling. Overall, we collected 572 responses, most from snowball sampling, removing 172 unfinished responses. We then filtered the remaining results to include only those who had completed at least 60% of the survey and spent at least 2 minutes answering the questions, leaving a total of 392 responses.

B. Potential Risks to Participants

We took a number of precautions to minimize the risk to participants of our survey. First, we avoided asking questions on controversial topics, such as feelings on government censorship or surveillance. Second, we did not ask for any personally identifiable information. Third, the survey was accessed via a TLS connection, to prevent third-parties from observing answers to questions. Fourth, we did not offer any compensation for taking the survey, to avoid inducing respondents to put themselves at risk in return for payment. Finally, we followed guidance from our IRB by placing a clear message for participants at the beginning of the survey. This explained who we were and what the purpose of our survey was. More importantly, it also informed participants that they could skip any questions they were uncomfortable answering as well as end their participation in the survey at any time. The survey questionnaire and all procedures were approved by our IRB.

C. Survey Design

The questionnaire contains 42 questions, the majority of which are multiple-choice and Likert-type questions, with a few open-response questions. At the start of the survey we provided an introduction about the purpose of the study and an implied consent form that follows guidance from our IRB. The survey was divided roughly into the following groups of questions: (a) demographics, (b) privacy preferences, (c) usage of Telegram, (d) usage of privacy features, and (d) usage of security features. At the conclusion of the survey, in lieu of payment, we provided some brief education on the importance of the authentication ceremony when using secure chat, along with a recommendation that for greater security they could use Signal. We then provided some instructions on how to use the authentication ceremony in Telegram. Respondents were given the option to leave an email address for further contact.

D. Data Analysis

In order to analyze the data for open-response questions, three of the authors coded the data together, ensuring agreement on all codes. The coding methodology employed was that of conventional content analysis, which is nearly identical to grounded theory except that it does not attempt to output a theory. In the first phase, we reviewed each response to open-response questions phrase-by-phrase and word-by-word to assign codes that classified users' responses. We translated the Farsi responses so that each of the three coders could work together, and then reviewed the original Farsi and the context of each statement while coding. In the second phase, we used the constant comparative method to group codes into concepts. In the third phase, we organized related categories by merging related codes.

We perform statistical analysis on responses to questions that allow us to do so. We provide basic summary statistics for responses to each question as well as perform statistical tests to identify whether participants living inside Iran answer in a manner distinguishable from those outside. We include a deeper discussion of the statistical analysis performed in the Appendix.

E. Limitations

Snowball sampling is a useful methodology for sampling when it is not possible to use more traditional survey techniques, and it has been employed successfully in previous work [27]. However, this technique does come with a fairly notable downside. Because people tend to associate with those that are similar to themselves, snowball sampling is prone to creating population samples that are highly heterogeneous. Indeed, our sample consists largely of respondents aged 25-34 who are, on average, more educated the general populace as a whole. Because our sample cannot be seen as representative of a larger population, it would be inappropriate to attempt to directly generalize results to the larger population as a whole.

Another limitation of our work is that surveys based on self-reported security practices may be inaccurate due to participants misremembering or misunderstanding how they use security features. Some work has shown that there is not always a correlation between what people say and what they practice [34] in the domain of security behaviors. This work showed that behaviors involving choices and a visible effect, such as installing a popup blocker or using strong passwords, are self-reported with moderate accuracy. There is low accuracy for security behaviors that are more passive, such as the installation of security updates. We believe that the privacy and security practices we survey in this study fall more under the former category and are likely to involve active choices and visible effects, such as blocking users, setting a username, using a passcode, or the use of secret chat. We have further attempted to alleviate misunderstandings about terminology by providing screenshots of the features and settings in question alongside the questions asking about them.

V. Results

A total of 572 participants started the survey online between July 12, 2017 and September 1, 2017. Due to the length of the survey, not all participants completed the entire survey. We include responses only for those participants who completed at least 60% of the survey and spent at least 2 minutes answering the questions. Out of the total, 392 participants meet these criteria and are included in our results.

The full survey is given in the Appendix. Where space permits we include tables in this section showing results from the survey, with additional columns showing results split among those living inside Iran or outside the country. For convenience, we include all summary tables of results in the Appendix.

A. Demographics

Out of the 392 participants, 391 reported their gender. Our sample population skewed toward female (N=234, 59.8%) and younger participants between ages 25–34 (N=239, 60.9%). Most of our participants were educated, with either a four-year degree (N=118, 30%), Master's degree (N=152, 38.7%), or a doctorate (N=88, 22.4%). Most were currently living inside Iran (N=256, 65.3%) with the rest primarily living in the United States of America (N=76, 19.3%). Most participants were born in Iran (N=350, 89.2%). Those who were living outside Iran reported they had lived outside the country for an average of 5 years and 8 months.

B. Privacy preferences

We asked several general questions about privacy preferences. We first asked participants: *How important is it to you that messaging applications protect the privacy of your messages from viewing by other parties?* As shown in Table I, 92.9% of the participants reported that privacy of their conversations is either important or extremely important. More participants living inside Iran reported that the privacy of their conversations is extremely important as compared to those living outside the country (70.3% vs. 54.4%). This difference is statistically significant ($P < 0.0001, \Phi_c = 0.479$, Fisher's exact test).

We next asked participants to rank their agreement with the statement: *I am more likely to trust a secure messaging application to protect my privacy if I pay for it.* Table II shows that nearly half of participants reported either they strongly agreed or somewhat agreed with the statement (N=193, 49.3%). We did not observe a statistically significant difference based on where participants are living ($P = 0.341$, Fisher's exact test).

TABLE I: *How important is it to you that messaging applications protect the privacy of your messages from viewing by other parties?*

Answer	Total	Inside	Outside
Extremely Important	64.8%	70.3%	54.4%
Important	28.1%	22.3%	39%
Neither	5.4%	5.9%	4.4%
Unimportant	1.3%	1.6%	0.7%
Extremely Unimportant	0.5%	0%	1.5%

TABLE II: *I am more likely to trust a secure messaging application to protect my privacy if I pay for it.*

Answer	Total	Inside	Outside
Strongly Agree	14%	11.7%	18.4%
Somewhat Agree	35.2%	37.1%	31.6%
Neither	30.6%	30.9%	30.1%
Somewhat Disagree	10.7%	11.7%	8.8%
Strongly Disagree	9.2%	8.6%	10.3%

C. Using Telegram

The next section of the survey asked about how participants use Telegram. Because Telegram includes both insecure and secure messaging, we are interested in understanding whether participants use Telegram to send sensitive data, and how they conceive of threats against their privacy.

We first asked: *How often do you use Telegram?* The vast majority (90%, N=352) reported that they use Telegram on a daily basis. Those living inside Iran more frequently reported using Telegram daily (93.4% vs 83.7%), and this is statistically significant ($P = 0.011, \Phi_c = 0.162$, Fisher's exact test).

This survey continues by asking: *Why do you use Telegram?*. We gave participants a choice of selecting one or more reasons from a list. As shown in Table III, the most popular responses were using Telegram to stay in touch with friends, being involved within group conversations, and following channels. Only a very small minority reported using Telegram due to its security and privacy features. The differences between those who live inside and outside of Iran are statistically significant ($P = 0.002, \Phi_c = 0.145$, Fisher's exact test). This confirms prior work [11], [15] showing that security and privacy are not the primary reason for users to use secure messaging applications.

TABLE III: *Why do you use Telegram? Check all that apply.*

Options	Total	Inside	Outside
Stay in touch with friends/family	80.9%	81.2%	82.7%
Group conversations	54.3%	58.8%	47.4%
Follow channels	52.6%	64.3%	31.6%
Free international communications	21.9%	19.6%	27.1%
Voice messages	17.9%	16.5%	21.1%
Security/privacy features	11.7%	12.2%	11.3%
Stickers	13.5%	12.9%	15%
Other	7.7%	7.5%	8.3%

1) Sharing sensitive information: We next asked: *Have you ever used Telegram to send private/sensitive information, such as a credit card number?* Just over half (53%, N=207) of participants answered *Yes* to this question. Those living inside Iran are more likely to use Telegram for sharing sensitive information than those living outside the country, 59.8% to 40.3%, and the differences between those who live inside and outside of Iran are statistically significant ($X^2(1, N = 392) = 12.614, P = 0.0004, \Phi_c = 0.185$).

We asked the participants who reported that they used Telegram for sharing sensitive information: *How often do you have conversations on Telegram that include private information?* These responses were split among often (22.2%, N=46), sometimes (36.2%, N=75), and rarely (41.1%, N=85), with one person reporting having never using Telegram for this purpose. The differences between those who live inside and outside of Iran are not statistically significant ($P = 0.752$, Fisher's exact test).

We asked these same participants: *What type of private/sensitive information do you discuss on Telegram?* 151 participants responded to this free-response question. Unfortunately 86 of them mentioned all the types of information they share on Telegram, likely due to a poor Farsi translation of *sensitive/private information* in the questionnaire. For those 65 responses where the question was properly conveyed in English, participants primarily mentioned personal photos, financial information, and personally identifying information.

We also asked these same participants: *Why do you feel comfortable sending private/sensitive information using Telegram?* This was an open response question. We received 154 responses and coded this data. By far the most popular answer was trust in the application, with other responses including convenience, having nothing to hide, or willing to take the risk. Very few responses (6) mentioned the security and privacy features of Telegram, with 2 referring to secret chat and 4 referring to authentication features. Because trust was such a prominent answer, we further separated responses based on the source of user trust. More than half of the responses mentioned explicitly that the participants believe Telegram is secure enough for them to share their sensitive information, while rest use factors such as the popularity of the application, experiences of others, and so forth.

Recall that 47% (N=183) participants reported that they have not used Telegram for sharing sensitive information. We asked this group: *Why don't you send private/sensitive information using Telegram?*. This was an open response question. We received 124 responses, which we coded. Lack of trust in Telegram was the primary reason, with others indicating they feel no need, identify a perceived threat, or prefer alternatives. Our participants mentioned a wide range of potential threats, including hackers, developers, their government, mobile phone eavesdropping, logs, data leakage, and information theft, plus a general unease about the Internet itself. For those cases where participants preferred alternative approaches, many were vague about the alternative, but others mentioned a preference for voice calls, text messaging, and exchanging messages in person.

The Appendix shows the coding results and sample quotes for each of the codes in this section.

TABLE IV: *What strategies do you use to protect your privacy on Telegram?*

Technical strategies	**Percent**	**Count**
End-to-end encryption	13.1%	20
Password authentication	7.8%	12
Enable security features	7.2%	11
Message impermanence	6.5%	10
Two-factor authentication	5.9%	9
Session management	4.6%	7
Selective contacts	4.6%	7
Limit the application permissions	0.6%	1
Non-technical strategies	**Percent**	**Count**
Self filtering	32.2%	49
Preferred alternatives	5.2%	8
Out-of-band communication	2.6%	4
Have nothing to hide	2.6%	4
Use secret phrases (coding)	2.6%	4
Reliance on platform	1.9%	3
Manual content encryption	0.6	1
Credential impermanence	0.6	1
Anonymity	0.6	1

2) Strategies and Threats: We asked participants: *What strategies do you use to protect your privacy on Telegram?*. This was an open response question. For the 233 responses we received for this question, 47% (N=110) of them explicitly mentioned that they have no strategy to protect their conversations within Telegram. We coded the rest of their responses and divided them into technical and non-technical strategies. By technical, we mean using the security features that the application or the phone itself provides. As shown in Table IV, using secret chat was the most popular technical strategy and self-filtering was the most popular non-technical strategy. In a few cases, participants mentioned a combination of technical and non-technical strategies. Of the 18 participants who mentioned end-to-end encryption in their strategy, more than three-fourths (77%, N=14) earlier in the survey reported that they used Telegram for sharing sensitive information.

We asked participants: *Who do you think can read the messages you send on Telegram to your friend, except you and your friend? Check all that apply.* The responses indicate that hackers, Telegram employees, their government are all considered threats by more than half the participants, with other governments and their Internet provider being threats for more than one third of the participants. Those living inside Iran are more concerned about their government than those living outside, 57.4% to 47.8%. The differences between responses of those who live inside and outside of Iran are statistically significant ($X^2(1, N = 392) = 9.802, P = 0.02, \Phi_c = 0.139$).

D. Privacy Features

The next set of survey questions investigates whether people use the privacy features available in Telegram. Users can configure how others can find them and their last seen status. They can block others users and control who can invite them into groups. They can also edit or delete messages. We show overall use of these features in Figure 2. Use of the feature is based on those changing the default setting or reporting using the feature.

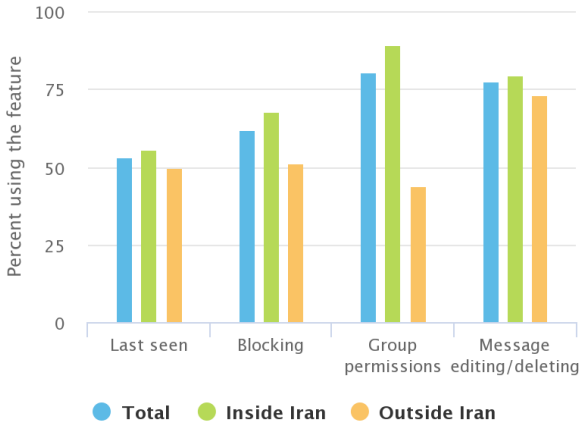


Fig. 2: Participant use of privacy features

We first showed a screenshot of the privacy and security settings screen in Telegram and asked participants: *How often do you change your privacy and security settings in Telegram?* Most users report changing these settings sometimes (64.7%, N=251), while 28.6% (N=111) say they have never changed these settings and 6.7% (N=26) say they frequently change these settings. Those living inside Iran are more likely to change these settings than those living outside Iran, and the overall differences between these groups is statistically significant ($X^2(2, N = 392) = 14.629, P = 0.0007, \Phi_c = 0.194$).

1) Last Seen Status: Regarding the *last seen* status, we asked participants: *How do you currently control this information?* The default settings is for everyone to be able to see this. 55.5% (N=210) of participants changed this setting by limiting it to either *My contacts can see this* (37%, N=140) or *Nobody can see this* (18.5%, N=70). The remainder either chose *Everyone can see this* (27.2%, N=103), the default, or *I don't use this feature* (17.2%, N=65). Those living inside Iran are more likely to let contacts see their status, while those living outside Iran are more likely to allow nobody to see their status or to not use the feature. The differences between those living inside and outside Iran are statistically significant ($X^2(3, N = 392) = 18.51, P = 0.0004, \Phi_c = 0.219$).

2) Blocking: We next asked participants: *Have you ever blocked a person? You may choose multiple answers.* By default, anyone can contact any other user; users are given the option to report another person as spam or block the person. We allowed participants to select from a variety of reasons for blocking, including not knowing the person, not wanting contact with the person, etc. Overall, 62% (N=243) participants use the blocking feature for various reasons. Participants who live inside Iran (67.6%, N=173) use the blocking feature more than those outside the country (51.5%, N=70), and the differences between responses of those who live inside and outside of Iran are statistically significant. ($X^2(1, N = 392) = 10.27, P = 0.001, \Phi_c = 0.162$).

3) Group Permissions: We asked participants: *Do you let other people add you to groups?* Over half of participants (57%,

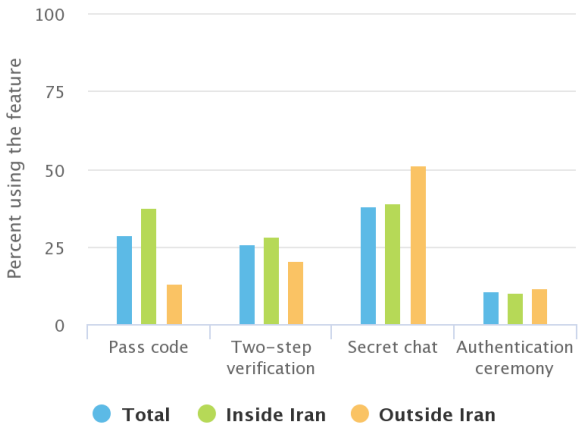


Fig. 3: Participant use of security features

N=220) reported that they leave this option open and let others add them to groups and decide later if they want to leave the group. About a quarter of participants (25.1%, N=97) reported that they blocked anyone outside their contact list from being able to invite them to groups. The rest of the participants (17.9%, N=69) reported never changing their settings in this regard. The default value for this setting is that anyone can invite the user to a group. Thus, only about a quarter of participants have changed this setting. The differences between those living inside and outside Iran are statistically significant ($X^2(2, N = 392) = 36.219, P < 0.0001, \Phi_c = 0.306$).

4) Message Editing or Deleting: We asked participants: *Have you ever used the feature that lets you delete or edit messages you have already sent? You may choose multiple answers.* The majority of participants (66.1%, N=254) reported that they use this functionality in order to delete or edit messages they sent by mistake. About 1 in 5 participants (22.4%, N=86) use this functionality as a strategy to protect their privacy by deleting their messages after they are done with the conversation. About 1 in 5 participants (22.7%, N=87) reported that they never used this feature. The differences between those who live inside and outside Iran are not statistically significant.

E. Security Features

The next set of survey questions investigates whether people use the security features available in Telegram. Telegram includes a variety of security features, including setting a pass code on the application, activating two factor authentication, using secret (end-to-end encrypted) chat, and using the authentication ceremony for secret chat. We show overall use of these features in Figure 3. Use of the pass-code lock and two-step authentication is based on a simple yes/no question. Use of secret chat is based on those who answered *rarely*, *sometimes*, or *often* when asked how often they use it. Use of the authentication ceremony is based on those who answered *sometimes* or *often* when asked if they used the ceremony for secret chat.

1) User authentication: We asked participants: *You can set a pass code lock in Telegram so that you need to enter this code to access your conversations. This could prevent someone from reading your conversations if they find your phone. Have you set up a pass code lock for your conversations?* Most participants (70.8%, N=271) reported that they are not using a pass code in order to protect their conversations in Telegram. Participants inside Iran report using this feature more than those living outside the country, 38.2% compared to 13.6%, and the differences between responses of those who live inside and outside of Iran are statistically significant ($X^2(1, N = 392) = 23.9, P < 0.0001, \Phi_c = 0.256$).

For those who did not setup a pass code, we asked: *Why have you never set up a pass code for your conversations? You may choose multiple answers.* The top answers include not needing it, preferring alternatives, lack of knowledge, or finding the feature inconvenient. The differences between responses of those who live inside and outside of Iran are not statistically significant.

We also asked participants: *Have you set up two-step verification for your Telegram account?* Most participants (72.7%, N=269) reported that they have not used this feature. The differences between responses of those who live inside and outside of Iran are not statistically significant.

For those who did not setup two-step verification, we asked: *Why have you never set up two-step verification for your conversations? You may choose multiple answers.* The top reasons are not needing it, preferring alternatives, lack of knowledge, or finding the feature inconvenient.

2) Secret chat: We asked participants: *How often do you use the Secret Chat feature in Telegram? This is a picture of what it looks like.* The majority (59.1%, N=220) had never used this feature, with some having used it rarely (30.9%, N=115), a few reporting sometimes (9.1%, N=34) and a very small number chose often (0.81%, N=3). There are no significant differences between those living inside Iran and those living outside of Iran using this feature.

We asked participants who responded that they rarely or never use secret chat: *Why have you not used Secret Chat more often? You may choose multiple answers.* The primary reasons indicate no need and lack of knowledge.

We asked all participants: *What do you think the Secret Chat feature does? How is it different from a regular conversation?*, an open response question. Table V shows the categories we coded for the 172 responses we received. Many (40.8%, N=76) indicated they did not know what this feature does. A surprising number mentioned something related to encryption or protection (26.2%, N=45). Only a small number (5.3%, N=10), included in this total, mentioned end-to-end encryption. Some participants (20.4%, N=38) believe that secret chat is similar to self-destructing messages, like Snapchat, since it does include this functionality. Interestingly, 12 participants reported that the secret chat feature has been filtered inside Iran. With further investigation, we realized that this is not the case and they are confused by the fact that two parties need to be on-line to be able to start exchanging messages in secret chat.

We also asked participants: *Who do you think can read your Secret Chat messages with your friend, except you and your friend? Check all that apply.* A large number of participants are concerned about most of the threats listed—hackers, my

TABLE V: *What do you think the Secret Chat feature does? How is it different from a regular conversation?*

Functionality	Percent	Count
Don't know	40.8%	76
Message impermanence	20.4%	38
Encryption	9.6%	18
Protection	9.1%	17
Government filtered	6.9%	13
Restricted sharing	5.9%	11
End-to-end encryption	5.3%	10
Cost saving	1%	2
Safe from third parties	0.5%	1

government, Telegram employees, other governments, my Internet provider—with Telegram employees having the largest concern. The differences between those who live inside and outside of Iran are not statistically significant. Interestingly, concerns are only a little lower than those for normal chat; since most participants have not used it and only know its name, this indicates the name alone does not convey any trust.

We also asked participants: *How much do you trust Telegram to keep your Secret Chat messages private so that only you and your friend can read them?*. Note this came after the previous question asking what they thought secret chat does, to avoid biasing their responses. From the 357 responses, just 5.3% (N=19) trust Telegram a great deal, with 16% (N=57) choosing a lot, 41.7% (N=149) choosing a moderate amount, 26.3% (N=94) a little, and 10.6% (N=38) not at all. The differences between those who live inside and outside of Iran are not statistically significant.

3) Authentication Ceremonies: We asked all those participants who said they had used secret chat: *Telegram has a feature that lets you verify the encryption key for your Secret Chat. How often do you use this feature? This is a picture of what this feature looks like.* The majority (70.4%, N=100) reported that they never used this feature. Some (19.7%, N=28) reported they had rarely used the ceremony, a small number (4.9%, N=7) said sometimes, and another small number (4.9%, N=7) claimed they often used the ceremony. The differences between those who live inside and outside of Iran are not statistically significant.

Telegram also provides end-to-end encrypted voice calls. We asked participants: *Have you ever made a phone call through Telegram?*. A little less than half of participants (47.9%, N=174) reported using this feature before. The rest indicated they had not used this feature (33.3%, N=121) or did not have this feature (18.7%, N=68). Since this feature is blocked inside the country, there is a good chance that some who answered negatively don't have access to calls in Telegram. The differences in usage between those living inside and outside Iran (with those living outside more likely to use phone calls) are statistically significant ($X^2(2, N = 392) = 25.456, P < 0.0001, \Phi_c = 0.265$).

For those who said they had made a phone call, we asked: *How often do you compare emojis when you make a phone call using Telegram? This is a picture of what this feature looks like.* Over half of participants (53.8%, N= 92) claimed they had used the authentication ceremony for voice calls. This may be due to the use of emojis for comparison, rather than a long, numeric key fingerprint. The differences between those who live inside and outside of Iran are not statistically significant.

VI. Discussion

A. Differences Based on Living in Iran

One of the primary research questions this work attempts to answer is whether there are differences in security/privacy behaviors and attitudes between those living in Iran and those living outside. Questions of this nature are often very difficult to answer owing to the numerous confounding socioeconomic factors that are at play. However, because our sample population is so demographically homogeneous—largely sharing culture, language, religion, birthplace, educational attainment, etc.—then resulting differences are much more likely to be a consequence of those factors that are not shared, like the current country of residence. We are thus able to say with much greater confidence that behavioral differences between those participants living inside and outside Iran are likely to be a consequence of differences in their current environment.

Our results indicate that those living inside Iran are more concerned about their privacy, more likely to report daily usage of Telegram, more likely to send sensitive information using Telegram, more likely to change their privacy settings, more likely to change the visibility of their *last seen* status to only their contacts, more likely to block people, more likely to use a passcode lock, and more likely to suspect that Telegram employees can view secret chat messages.

We can speculate about some reasons for why these differences may be influenced by current living environment. The majority of our participants from outside the country are far from the hotly debated issues inside the country and are likely not activists. Their concern about threats to their civil liberties are likely to be lower. On the other hand, people inside the country, in addition to using Telegram for communication with friends and family, are using Telegram for news and discussion by following channels and using groups. The discussed topics inside channels and groups are more likely sensitive and up to date with what is happening in the society. They may feel more worried about inspection of their phone by authorities or shoulder surfing. People inside the country are in contact with others who know their language and it is natural for them to be more cautious to protect their accounts from such attacks.

Overall, these factors could explain some of the differences observed. Participants inside Iran are more likely to send what they consider to be sensitive, but these include items that are personal in nature—photos, financial information, and personally identifiable information—as opposed to information that could lead to arrest. This could simply be due to their more everyday use. Yet people inside Iran are also more likely to use some privacy features, which could be due to differences in perceived threats. They may change their privacy settings more often due to concerns about snooping, and they may be more likely to use a passcode lock if they feel unsafe leave their phone around. People inside the country are more likely to be contacted by others whom they don't like or be added to groups they may not be interested. Thus, it is also normal to

see the majority of this population use features for blocking other even if they are friends, because they are more aware of privacy threats and take them more seriously in comparison to people who live outside.

B. Importance of Privacy and Misplaced Trust

The overwhelming majority of participants (93%) indicated it was either important or extremely important that applications protect the privacy of their messages from viewing by other parties. Yet, despite this strong concern, over half of participants said they used Telegram to send sensitive information. A primary factor in choosing to share sensitive information is trust in the security of Telegram, and nearly half (47%) have no strategy to protect their privacy when using Telegram.

This points to a significant problem for applications like Telegram that do not use end-to-end encryption by default. There is clearly a strong desire for privacy, and significant trust in the application, yet this trust is misplaced when their sensitive information is not being protected. As a result of this misplaced trust, many users make choices that do not align with their stated privacy preferences.

In questions that explore reasons for people not using various privacy and security features, several common themes that participants report include a lack of perceived need, lack of knowledge of the feature, or finding the feature inconvenient. These match closely to work by Renaud et al. in identifying reasons why people do not use secure email [28]. Unlike secure email, there are alternative messaging applications available that do offer strong security and are easy to use (e.g. Signal, WhatsApp), but a primary factor in adoption of secure messaging applications is using a platform that your friends are also using [2], [10].

C. Varying Use of Privacy and Security Features

There is widely varying usage of privacy and security features (12% to 62%). A natural question to ask is why some of these features are used more than others. To explore this question, we compiled the usage of each feature from the survey and then correlated this with how this feature may be prompted in the user interface. None of the features are *explicitly* prompted in the interface, meaning the user is never prompted directly to change their privacy settings or adopt a security feature. Rather, the user experiences *implicit* prompts to protect their privacy when the application does something contrary to their preferences.

The privacy features are all implicitly prompted in the user interface. When chatting with a contact, the last time that contact was seen (active in the application) is shown directly below the contact's name. This could prompt the user to review their own privacy settings once they see how they are able to easily track their contact's activity. Likewise, when chatting with a contact, if a user sends a mistaken or otherwise undesired message to a contact, they could be prompted to tap on it, bringing up the edit and delete options in the contextual menu. The other two privacy features are prompted by experiences in the main screen of the application, when receiving an unwanted message from an individual or a group. These experiences could cause the user to examine their settings to learn how to block a user or prevent others from adding them to a group. For group chats, there is also a menu option in the chat window that allows the user to delete the chat and leave the group. Furthermore, in all of these cases, users may also be prompted to search the Internet for help if they feel their interaction with the application is violating their privacy in any way.

By contrast, users are not prompted, even implicitly, to use the security features of the application. The pass code lock protects and against theft (or other unwanted use) of the device. Two-step verification protects against account hijacking. Secret chat protects against surveillance by Telegram (e.g. for advertising) or the government, or from infiltration of the Telegram server by a hacker. None of these occurrences happen regularly, and violations of privacy are likely to happen silently. The prompts for adopting security practices usually stem from major security breaches reported in the press. For example, in July 2016, more than a dozen accounts of Iranian Telegram users were compromised and the phone numbers of more than 15 million Iranian users were identified by the Roket Kitten Iranian hackers group [26]. It is difficult for users to connect news like this to some action they could take to prevent it in the future. Rather, they are likely to connect this to a security failure by Telegram (similar to a breach of information held by Experion in 2017) and thus expect Telegram to "fix" this problem.

D. Secret Chat and Authentication Ceremonies

Our results indicate a general lack of awareness about secret chat and confusion over the purpose of this feature. The majority (59%) had never used secret chat. Of those who had used it, only 10% of participants reported they use it sometimes or often. Regarding the purpose of secret chat, 95% of participants do not know that secret chat provides end-to-end encryption. At best, 24% know the feature has something to do with protection or encryption, and another 20% recognize that it provides message impermanence. Note that the self-destruct timer, which provides message impermanence, is visible to users, whereas encryption is done automatically and has no visible effect other than a lock icon shown during secret chats.

Of particular concern is a lack of awareness of the security that secret chat offers. The purpose of end-to-end encryption is to ensure that only the sender and recipient can read a message, and no other third party has this ability. However, more than half of participants thought that secret chat messages could be read by Telegram employees, more than 40% thought they could be read by hackers or their government, and over 30% thought they could be read by other governments or their Internet provider. These numbers are only somewhat lower than those for regular chat messages, and *more* people think Telegram can read secret chat messages. It is also possible that participants have a strong sense of distrust in the security of electronic communications.

The infrequent usage of secret chat in Telegram is likely due to Telegram's design choices. Telegram encourages people to use plaintext chatting by integrating more features into this mode, including stickers and group chat. Secret chats must be started with a separate menu option, and by default messages are not encrypted with this functionality. In addition, Telegram's implementation sends an invitation to the other party and requires that they respond before any messages are

sent. This adds additional inconvenience that is not present in other secure messaging applications (e.g. Signal, WhatsApp). Finally, Telegram does not provide support for secret chats to be visible on multiple devices, whereas regular chat messages are viewable on all devices. This lack of equivalent functionality could discourage use of secret chats. Note, there is no technical reason why secret chat can't be made portable; there are a variety of ways to safely transfer encryption keys from one device to another.

We also examined the usage of authentication ceremonies. Of the people who had used secret chat, a strong majority (69%) reported they had never used the authentication ceremony. However, over half of participants reported they had used the authentication ceremony for an encrypted phone call, which consists of comparing emojis. We note that users of Telegram are explicitly prompted to use the authentication ceremony for a phone call—the emojis and brief instructions are shown on the screen when a call is made. In contrast, the authentication ceremony for secret chat is not prompted at all and finding it requires tapping through several menus.

VII. Recommendations

Based on our survey results, we make the following recommendations for improving Telegram. Most of these recommendations generalize to other secure messaging applications, and we use Signal as an illustrative example. Our ideas follow the principles elucidated by Adams and Sasse [4] in *Users are Not the Enemy*: users are security conscious, and they will use security features if they perceive a need for them. Our survey indicates this holds true for privacy-preserving features as well, though adoption could be higher. A related concept is the idea of nudging users toward beneficial behaviors [30], which has been used in several mobile settings [32], [6].

A. Use end-to-end encryption for all chat messages

Secure messaging applications should use end-to-end encryption for all chat messages. Examples of applications that do this include Signal and WhatsApp. The evidence continues to accumulate that when users are given two types of chat, with the default unencrypted, they will use the default chat and send sensitive information over unencrypted exchanges.

Telegram justifies its use of unencrypted chat by claiming that end-to-end encryption of chats do not allow users to easily restore access to their chat history on a new device, for example when replacing a lost phone. It's not clear this is a desired use case, since many users may consider chat messages to be temporary in nature.

B. Use profiles to simplify privacy settings

Although nearly all participants expressed a strong interest in privacy, only some users change their privacy settings. This is similar to a previous study on Facebook, which showed that privacy settings matched user preferences only 37% of the time [24]. Currently, Telegram has defaults that allow anyone to see your *last seen* status, call you, or add you to a group. Changing these defaults requires becoming aware of these settings and finding them in the extensive menu system. Likewise, Signal has privacy settings with defaults that are permissive: contacts can see when you've read a message, you can take screenshots of encrypted messages, and the keyboard can view everything you type to improve its personalized learning algorithm.

When secure messaging applications have numerous privacy settings with multiple options, they can use profiles to help users choose settings that match their privacy preferences. Lin et al. have shown that mobile app users cluster into a small number of privacy profiles [22]. For example, the application could allow users to indicate how concerned they are about privacy, and the application could sort them into one of the groups identified by Lin et al.—conservative, fence-sitters, and unconcerned. These could correspond to default settings that are very conservative (nobody can see your *last seen status*), in the middle (contacts can see your status), and permissive (everybody can see your status). More advanced users could customize each setting individually.

C. Use explicit prompts for privacy and security features

In some cases, user action may be needed to enable a particular feature. For example, even with strong defaults (or if a user relaxes them), a user may still receive an unwanted message from a contact. In Telegram and Signal, this is an implicit prompt for the user to investigate whether they can block someone–they may search Google or look through the application menus. We recommend that applications instead identify cases when a user is contacted for the first time and then explicitly prompt the user, asking if they would like to accept messages from this contact or block them, with a single click required to block the user. To avoid warning fatigue, the application could add a simple "block" button to the chat interface. Likewise, secure messaging applications could prompt users to use the authentication ceremony in an encrypted chat (Telegram's integration of the ceremony into phone calls is a good example), and could explicitly ask users at installation if they want to setup a passcode lock or two-step verification.

VIII. Conclusion

The primary purpose of this study was to determine how well Telegram is meeting the security and privacy needs of their users. The evidence is decidedly mixed. The vast majority of participants say that privacy is important to them, yet only about 10% use end-to-end encrypted chat at least sometimes. Since about half report sending sensitive information while using the application, this indicates that Telegram is not meeting their expressed privacy preferences. Many of those who send sensitive information report trusting Telegram, but that trust is clearly misplaced, especially in light of recent arrests of some who manage Telegram channels. The picture is somewhat better for privacy features, since many report using features that allow them to edit or delete messages, block other users, and change their *last seen status*. However, usage is lower for all security features.

An important point to consider is how our results vary based on whether the participants were living inside or outside of Iran. Participants living in Iran were more likely to rate privacy as extremely important to them, more likely to use Telegram daily, and yet are also more likely to share sensitive information while using Telegram. Given this, there is a strong need to improve the privacy and security of Telegram. Our

recommendations include making end-to-end encryption of chat messages the default, using profiles to simplify privacy settings, and explicitly prompting users when they need to take action to adopt certain security and privacy features. Additional work should be done to study how well these changes would lead to greater use of privacy and security features.

IX. Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1528022.

References

[1] R. Abu-Salma, K. Krol, S. Parkin, V. Koh, K. Kwan, J. Mahboob, Z. Traboulsi, and M. A. Sasse, "The security blanket of the chat world: An analytic evaluation and a user study of telegram," in *European Workshop on Usable Security (EuroUSEC)*, 2017.

[2] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in *IEEE Symposium on Security and Privacy*, 2017.

[3] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Symposium on Security & Privacy*, 2005.

[4] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[5] N. Al Ali and G. Motevalli, "Telegram's new audio messaging feature blocked in Iran," April 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-04-18/telegram-s-new-audio-messaging-feature-blocked-in-iran

[6] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, "Your location has been shared 5,398 times!: A field study on mobile app privacy nudging," in *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 787–796.

[7] M. Azali, "Infographic: Telegram usage statistics in Iran," TechRasa, September 2017. [Online]. Available: http://techrasa.com/2017/09/06/infographic-telegram-usage-statistics-in-iran/

[8] K. Church and R. de Oliveira, "What's up with WhatsApp?: comparing mobile instant messaging behaviors with traditional SMS," in *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2013, pp. 352–361.

[9] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A formal security analysis of the Signal messaging protocol," in *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE, 2017, pp. 451–466.

[10] A. De Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie, "Expert and non-expert attitudes towards (secure) instant messaging," in *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[11] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[12] J. L. Dupree, R. Devries, D. M. Berry, and E. Lank, "Privacy personas: Clustering users via attitudes and behaviors toward security practices," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 5228–5239.

[13] M. Etehad, "Telegram was the app where Iranians talked politics. then the government caught on," LA Times, March 2017. [Online]. Available: http://www.latimes.com/business/la-fi-telegram-iran-20170313-story.html

[14] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2012, p. 3.

[15] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *Proceedings of the 2006 CHI Conference on Human Factors in Computing Systems*. ACM, 2006, pp. 591–600.

[16] A. Ghajar, "A messaging app that can change iran," IranWire, May 2017. [Online]. Available: https://iranwire.com/en/features/4607

[17] F. House, "Freedom on the net 2016," 2016. [Online]. Available: https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf

[18] F. Jacobs, "On SMS logins II : an example from Telegram in Russia," April 2016. [Online]. Available: https://www.fredericjacobs.com/blog/2016/04/30/more-on-sms-logins/

[19] J. Jakobsen and C. Orlandi, "On the CCA (in) security of MTProto," in *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2016, pp. 113–116.

[20] J. B. Jakobsen and C. Orlandi, "A practical cryptanalysis of the Telegram messaging protocol," Ph.D. dissertation, Master Thesis, Aarhus University, 2015.

[21] J. Lee, R. Choi, S. Kim, and K. Kim, "Security analysis of end-to-end encryption in Telegram," *SCIS 2017*, 2017.

[22] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling usersâĂŹ mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[23] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. Zhang, N. Sadeh, A. Acquisti, and Y. Agarwal, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[24] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*. ACM, 2011, pp. 61–70.

[25] A. McNamara, A. Verma, J. Stallings, and J. Staddon, "Predicting mobile app privacy preferences with psychographics," in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*. ACM, 2016, pp. 47–58.

[26] J. Menn and Y. Torbati, "Exclusive: Hackers accessed telegram messaging accounts in iran - researchers," August 2016. [Online]. Available: http://www.reuters.com/article/us-iran-cyber-telegram-exclusive/exclusive-hackers-accessed-telegram-messaging-accounts-in-iran-researchers-idUSKCN10D1AM

[27] Y. Rashidi, K. Vaniea, and L. J. Camp, "Understanding Saudis' privacy concerns when using whatsapp," in *Proceedings of the Workshop on Usable Security (USEC'16)*, 2016.

[28] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why doesn't Jane protect her privacy?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2014, pp. 244–262.

[29] H. Saribekyan and A. Margvelashvili, "Security analysis of Telegram," 2017. [Online]. Available: http://courses.csail.mit.edu/6.857/2017/project/19.pdf

[30] R. Thaler and C. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press, 2008.

[31] F. Tribune, "Telegram firmly in top place in Iran," March 2017. [Online]. Available: https://financialtribune.com/articles/sci-tech/61147/telegram-firmly-in-top-place-in-iran

[32] J. Turland, L. Coventry, D. Jeske, P. Briggs, and A. van Moorsel, "Nudging towards security: Developing an application for wireless network selection for android phones," in *Proceedings of the 2015 British HCI Conference*. ACM, 2015, pp. 193–201.

[33] W. Turton, "Why you should stop using Telegram right now," Gizmodo, June 2016. [Online]. Available: https://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415

[34] R. Wash, E. Rader, and C. Fennell, "Can people self-report security accurately?: Agreement between self-report and behavioral measures," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 2228–2232.

APPENDIX A
STUDY QUESTIONNAIRE

A. Introduction

Please select the language you are most comfortable with.

Thank you for your participation!

In this study, we are interested in learning about your views on online data privacy and how this affects your use of Telegram. This will help us to design better security and privacy tools for Internet users by understanding of the privacy concerns of people around the world.

Participating in this study involves completing this survey which should take approximately 15 minutes of your time.

Your participation and information will be totally anonymous to us and you will only be contacted again if you choose. You do not have to participate in this study if you do not want to. You do not have to answer any question that you do not want to answer for any reason.

Due to preserve your participation in this study anonymous, you will not be paid for participating in this study. But to compensate you for your time, upon concluding the survey, we provide few guidelines on how to better safeguard your privacy when using Telegram. This survey involves minimal risk to you.

The completion of this survey implies your consent to participate. Thank you!

B. Demographics

In this section we are interested in learning more about you. We will keep this information private and will never share it with anyone.

1) What is your gender?
   - ○ Male
   - ○ Female
   - ○ I prefer not to answer
2) What is your age?
   - ○ Under 18
   - ○ 18-24
   - ○ 25-34
   - ○ 35-44
   - ○ 45-54
   - ○ 55 - 64
   - ○ 65 or older
3) What is the highest degree you have completed or level of school you are in now?
   - ○ Less than high school
   - ○ High school graduate
   - ○ Some college
   - ○ 2 year degree
   - ○ 4 year degree
   - ○ Master degree
   - ○ Doctorate
4) In which country do you currently reside?
   (select from a list)
5) In which country were you born?
   (select from a list)
6) How long have you been living outside Iran?
   - ○ Less than 1 year
   - ○ Less than 2 years
   - ○ Less than 3 years
   - ○ Less than 5 years
   - ○ Less than 10 years
   - ○ More than 10 years
   - ○ I have never lived outside Iran

C. Privacy Preferences

In this section we are interested in learning about your privacy preferences.

7) How important is it to you that messaging applications protect the privacy of your messages from viewing by other parties?
   - ○ Extremely important
   - ○ Important
   - ○ Neither important nor unimportant
   - ○ Unimportant
   - ○ Extremely unimportant
8) I am more likely to trust a secure messaging application to protect my privacy if I pay for it.
   - ○ Strongly agree
   - ○ Somewhat agree
   - ○ Neither agree nor disagree
   - ○ Somewhat disagree
   - ○ Strongly disagree

D. Usage

In this section we are interested in learning about how you use Telegram.

9) How often do you use Telegram?
   - ○ Daily
   - ○ 4-6 times a week
   - ○ 2-3 times a week
   - ○ Once a week
   - ○ Rarely
10) Why do you use Telegram? Check all that apply.
   - ☐ To stay in touch with my friends and family.
   - ☐ It has security and privacy features that I use.
   - ☐ I like to involve in group conversations.
   - ☐ I like to follow some of the channels.
   - ☐ I like to use its stickers.
   - ☐ I use it for free international communications.
   - ☐ I use it for sending others voice messages.
   - ☐ Other
11) Have you ever used Telegram to send private/sensitive information, such as a credit card number?
   - ○ Yes
   - ○ No
12) *If the answer to #11 is No*
   Why don't you send private/sensitive information using Telegram?
   (open response)
13) *If the answer to #11 is Yes*
   How often do you have conversations on Telegram that include private information?

- ○ Often
- ○ Sometimes
- ○ Rarely
- ○ Never

14) *If the answer to #11 is Yes*
What type of private/sensitive information do you discuss on Telegram?
(open response)

15) *If the answer to #11 is Yes*
Why do you feel comfortable sending private/sensitive information using Telegram?
(open response)

16) What strategies do you use to protect your privacy on Telegram?
(open response)

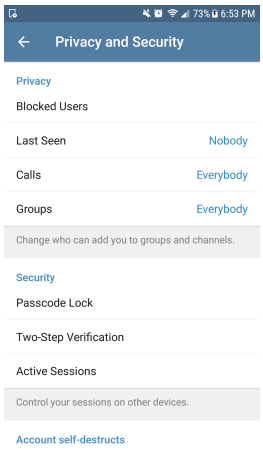
17) Who do you think can read the messages you send on Telegram to your friend, except you and your friend? Check all that apply.
- ☐ Telegram employees
- ☐ Other friends
- ☐ Hackers
- ☐ My government
- ☐ Other governments
- ☐ My Internet provider

E. Privacy Settings

In this section we are interested in how you use the privacy settings in Telegram.

18) Telegram has settings that control how other people can find you. How did you set up your account in Telegram?
- ○ Other people can find me using my phone number.
- ○ Other people can find me using my real name.
- ○ Other people can find me using a nickname.
- ○ I don't remember.

19) How often do you change your privacy and security settings in Telegram? This is a picture of what this looks like.



- ○ Frequently
- ○ Sometimes
- ○ I have never changed these settings

20) Telegram lets you control who can see various information about you. How do you currently control this information?
Last seen:
- ○ Everyone can see this
- ○ My contacts can see this
- ○ Nobody can see this
- ○ I don't use this feature

21) Have you ever blocked a person? You may choose multiple answers.
- ☐ Yes, because I didn't know this person.
- ☐ Yes, I know this person, but I don't want him/her to contact me using Telegram.
- ☐ Yes, I know this person, but I don't want him/her to be able to see my profile photo and/or my status.
- ☐ Yes, because we are not friends anymore.
- ☐ No, I have never blocked a person in Telegram.
- ☐ I can not remember.
- ☐ Others

22) Do you let other people add you to groups?
- ○ I have blocked anyone outside my contact list so that strangers can't send me messages or add me to a group.
- ○ I let other people add me to groups or send me messages, but then I leave the group or report them as spam if I don't like it.
- ○ I have never changed these settings.

23) Have you ever used the feature that lets you delete or edit messages you have already sent? You may choose multiple answers.
- ☐ I usually use it for removing or editing messages I send by mistake.
- ☐ I usually use it to protect my privacy, after the other person reads my message I will delete it.
- ☐ I have never used it but I like this feature.
- ☐ I have no reason to use this feature.

F. Security Features

In this section we are interested in how you use the security features of Telegram.

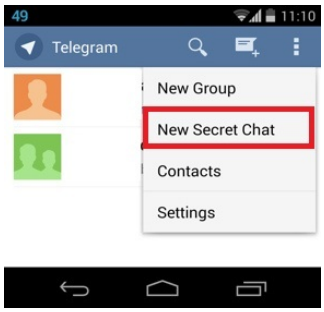
24) You can set a pass code lock in Telegram so that you need to enter this code to access your conversations. This could prevent someone from reading your conversations if they find your phone. Have you set up a pass code lock for your conversations?
- ○ Yes
- ○ No

25) *If the answer to #24 is No*
Why have you never set up a pass code for your conversations? You may choose multiple answers.
- ☐ It is annoying to enter the password every time.
- ☐ I do not use Telegram for sensitive conversations.
- ☐ I think the password for my phone is enough to protect my conversations.
- ☐ I use Secret Chat instead.
- ☐ I have never noticed this feature existed.
- ☐ I have set the self destructive timer for my sensitive conversations instead.
- ☐ I would like to set a pass code but it is hard to figure it out how to do so in Telegram.
- ☐ It never occurred to me that I need a pass code.
- ☐ I didn't know what this feature did.
- ☐ Others

26) Have you set up two-step verification for your Telegram account?
- ○ Yes
- ○ No

27) *If the answer to #26 is No*
Why have you never set up two-step verification for your conversations? You may choose multiple answers.
- ☐ It is annoying to verify the code each time I want to log in.
- ☐ I do not use Telegram for sensitive conversations.
- ☐ I think the password for my phone is enough to protect my conversations.
- ☐ I use Secret Chat instead.
- ☐ I have never noticed this feature existed.
- ☐ I have set the self destructive timer for my sensitive conversations instead.
- ☐ I would like to set it up but it is hard to figure it out how to do so in Telegram.
- ☐ It never occurred to me that I need to set up this feature.
- ☐ I didn't know what this feature did.
- ☐ Others

28) How often do you use the Secret Chat feature in Telegram? This is a picture of what it looks like.



- ○ Often
- ○ Sometimes
- ○ Rarely
- ○ Never

29) *If the answer to #28 is Rarely or Never*
Why have you not used Secret Chat more often? You may choose multiple answers.
- ☐ None of my friends use this feature.
- ☐ I don't use Telegram for sensitive conversations.
- ☐ I think the password for my phone is enough to protect my conversations.
- ☐ I have never noticed this feature existed.
- ☐ I have set the self destructive timer for my sensitive conversations instead.
- ☐ It is hard to figure it out how to work with this feature in Telegram.
- ☐ It never occurred to me that I need to use Secret Chat.
- ☐ I didn't know what this feature did.
- ☐ I don't trust this feature function as it is described.
- ☐ Others

30) What do you think the Secret Chat feature does? How is it different from a regular conversation?
(open response)

31) Who do you think can read your Secret Chat messages with your friend, except you and your friend? Check all that apply.
- ☐ Telegram employees
- ☐ Other friends
- ☐ Hackers
- ☐ My government
- ☐ Other governments
- ☐ My Internet provider

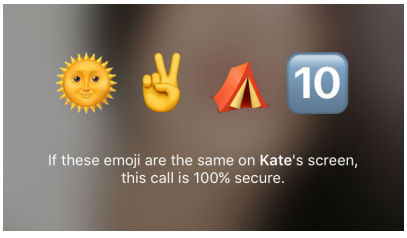
32) How much do you trust Telegram to keep your Secret Chat messages private so that only you and your friend can read them?
- ○ A great deal
- ○ A lot
- ○ A moderate amount
- ○ A little
- ○ None at all

33) *If the answer to #28 is not Never*
Telegram has a feature that lets you verify the encryption key for your Secret Chat. How often do you use this feature? This is a picture of what this feature looks like.

- ○ Often
- ○ Sometimes
- ○ A moderate amount
- ○ Rarely
- ○ Never

34) Have you ever made a phone call through Telegram?
- ○ Yes
- ○ No
- ○ I don't have this feature.

35) *If the answer to #34 is Yes*
How often do you compare emojis when you make a phone call using Telegram? This is a picture of what this feature looks like.



- ○ Often
- ○ Sometimes
- ○ Rarely
- ○ Never

APPENDIX B
TABLES AND ANALYSIS

Our data largely consists of Likert-type items, "mark all that apply"-type questions, and a handful of ordered-category items. For each of these questions, we conduct a two-fold analysis. The first level of analysis is simple: we calculate the ratio of respondents per group–the full population, those living inside Iran, and those living outside–that gave a particular response out of the total from that population that responded to that question. This approach is also used for analysis of "mark all that apply"-type questions, and so percentages reported will not sum to 100%. Instead, each individual response item should be interpreted independently, with the reported percentages characterizing the proportion of the respective population that marked that particular item.

Next, we conduct either a Pearson's chi-squared test of independence or, when appropriate, Fisher's exact test, to evaluate whether there are differences between the responses of those living Iran and those living outside. More specifically, when the following assumptions are not met–i.e., if any of the cells have values below 1 or more than 20% of the cells have values 5 or below–we instead perform Fisher's exact test on the response data. Furthermore, because statistical significance is partially a function of sample size, with large sample sizes, it is possible to have statistically significant results that have little practical meaning. For this reason, we additionally provide Cramer's V values (Φ_c) for each test that returned a statistically significant result. Cramer's V is a measure of effect size that is equivalent to Cramer's phi (Φ) in 2x2 contingency tables, while also extending to contingency tables with larger degrees of freedom. Generally speaking, a rule of thumb used to interpret Cramer's V is that values around 0.1 indicate a small effect, 0.3 indicates a medium-sized effect, and 0.5 indicates a large effect.

TABLE VI: *How important is it to you that messaging applications protect the privacy of your messages from viewing by other parties?*

Answer	Total	Inside	Outside
Extremely Important	64.8%	70.3%	54.4%
Important	28.1%	22.3%	39%
Neither	5.4%	5.9%	4.4%
Unimportant	1.3%	1.6%	0.7%
Extremely Unimportant	0.5%	0%	1.5%

TABLE VII: *I am more likely to trust a secure messaging application to protect my privacy if I pay for it.*

Answer	Total	Inside	Outside
Strongly Agree	14%	11.7%	18.4%
Somewhat Agree	35.2%	37.1%	31.6%
Neither	30.6%	30.9%	30.1%
Somewhat Disagree	10.7%	11.7%	8.8%
Strongly Disagree	9.2%	8.6%	10.3%

TABLE VIII: *How often do you use Telegram?*

Answer	Total	Inside	Outside
Daily	90%	93.4%	83.7%
4–6 times/week	6.1%	4.7%	8.9%
2–3 times/week	0.8%	0.4%	1.5%
Rarely	3.1%	1.6%	5.9%

TABLE IX: *Why do you use Telegram? Check all that apply.*

Options	Total	Inside	Outside
Stay in touch with friends/family	80.9%	81.2%	82.7%
Group conversations	54.3%	58.8%	47.4%
Follow channels	52.6%	64.3%	31.6%
Free international communications	21.9%	19.6%	27.1%
Voice messages	17.9%	16.5%	21.1%
Stickers	13.5%	12.9%	15.0%
Security/privacy features	11.7%	12.2%	11.3%
Other	7.7%	7.5%	8.3%

TABLE X: *Have you ever used Telegram to send private/sensitive information, such as a credit card number?*

Segment	Yes (send sensitive information)
Total	53.1%
Inside Iran	59.8%
Outside Iran	40.3%

TABLE XI: *What type of private/sensitive information do you discuss on Telegram?*

Sensitive information	Percent	Count
Personal photos	31.5%	29
Financial information	20.6%	19
Personally identified (PII)	17.3%	16
Credentials (e.g. password)	13.0%	12
Socially sensitive (e.g. gossip)	8.6%	8
Business (e.g. work related)	2.1%	2
Politically sensitive	1.08%	1
Sensitive document scans	1.08%	1
Religiously sensitive	1.08%	1

TABLE XII: *Why do you feel comfortable sending private/sensitive information using Telegram?*

Reason	Percent	Count
Trust	51.2%	79
Convenience	11.7%	18
Have nothing to hide	6.5%	10
Lack of alternatives	5.8%	9
Ignore the risks	5.2%	8
Taking risk	4.5%	7
Coping with perceived threats	3.9%	6
Authentication features	2.6%	4
Self filtering	2.6%	4
Secret chat	1.3%	2
Not caring about security	1.3%	2
Application fragmentation	1.3%	2
Message impermanence	1.3%	2
Checking for hackers (e.g. active sessions)	0.6%	1

TABLE XIII: Why participants trust Telegram for sharing sensitive information.

Aspect of Trust	Percent	Count
Trust Telegram security	51.8%	41
Trust popularity of the app	16.4%	13
Trust based on experience	15.2%	12
Trust foreign country developers	5%	4
Trust through learning	3.7%	3
General Trust	3.7%	3
Trust based on feeling	2.5%	2
Trust due to message availability	1.3%	1

TABLE XIV: *Why don't you send private/sensitive information using Telegram?*

Reason	Percent	Count
Lack of trust	40.0%	63
No need	23.5%	37
Perceived threats	21.0%	33
Prefers alternative	15.2%	24

TABLE XV: *What strategies do you use to protect your privacy on Telegram?*

Technical strategies	Percent	Count
End-to-end encryption	13.1%	20
Password authentication	7.8%	12
Enable security features	7.2%	11
Message impermanence	6.5%	10
Two-factor authentication	5.9%	9
Session management	4.6%	7
Selective contacts	4.6%	7
Limit the application permissions	0.6%	1
Non-technical strategies	**Percent**	**Count**
Self filtering	32.2%	49
Preferred alternatives	5.2%	8
Side channel	2.6%	4
Have nothing to hide	2.6%	4
Use secret phrases (coding)	2.6%	4
Reliance on platform	1.9%	3
Manual content encryption	0.6	1
Credential impermanence	0.6	1
Anonymity	0.6	1

TABLE XVI: *Who do you think can read the messages you send on Telegram to your friend, except you and your friend? Check all that apply.*

Answer	Total	Inside	Outside
Hackers	57.7%	59%	55.1%
My government	54.1%	57.4%	47.8%
Telegram employees	51%	53.5%	46.3%
Other governments	36%	37.5%	33.1%
My Internet provider	38%	36.3%	41.2%
Other friends	9.7%	9.4%	10.3%

TABLE XVII: *How often do you change your privacy and security settings in Telegram?*

Answer	Total	Inside	Outside
Frequently	6.7%	7.8%	4.5%
Sometimes	64.7%	69.8%	54.9%
Never	28.6%	22.4%	40.6%

TABLE XVIII: *How do you currently control this information? (Last seen status)*

Segment	Total	Inside	Outside
My contacts can see this	37.0%	41.9%	27.7%
Everyone can see this	27.2%	29.8%	22.3%
Nobody can see this	18.5%	15.3%	24.6%
I don't use this feature	17.2%	12.9%	25.4%

TABLE XIX: *Have you ever blocked a person? You may choose multiple answers.*

Reason	Total	Inside	Outside
Yes, because I didn't know this person	33.9%	33.1%	36.6%
Yes, I know this person, but I don't want him/her to contact me using Telegram	31.1%	35.0%	24.6%
No, I have never blocked a person on Telegram	23.0%	21.7%	26.1%
Yes, I know this person, but I don't want him/her to be able to see my profile photo and/or my status	18.1%	18.1%	18.7%
Yes, because we are not friends any more	15.0%	17.7%	10.4%
I can not remember	9.9%	8.3%	13.4%
Other	4.1%	5.9%	0.7%

TABLE XX: *Do you let other people add you to groups?*

Segment	Total	Inside	Outside
Leave this option open	57.0%	61.3%	48.9%
Blocked anyone outside their contact list	25.1%	29.2%	17.3%
Never changing their settings	17.9%	9.7%	33.8%

TABLE XXI: *Have you ever used the feature that lets you delete or edit messages you have already sent? You may choose multiple answers.*

Reason	Total	Inside	Outside
Delete or edit mistakes	66.1%	68.1%	62.4%
Protect privacy	22.4%	22.7%	21.8%
Never used	22.7%	19.1%	27.8%

TABLE XXII: *Why have you never set up a pass code for your conversations? You may choose multiple answers.*

Reason	Total	Inside	Outside
I do not use Telegram for sensitive conversations.	29.8%	26.4%	34.2%
I think the password for my phone is enough to protect my conversations.	29.0%	27.0%	31.6%
I have never noticed this feature existed.	27.5%	26.4%	28.9%
I didn't know what this feature did.	26.0%	29.1%	21.9%
It never occurred to me that I need a pass code.	25.6%	27.0%	23.7%
It is annoying to enter the password every time.	24.0%	23.0%	25.4%
I would like to set a pass code but it is hard to figure it out how to do so in Telegram.	6.1%	6.8%	5.3%
I have set the self destructive timer for my sensitive conversations instead.	5.7%	8.1%	2.6%
Others	3.8%	4.7%	2.6%
I use Secret Chat instead.	2.3%	2.7%	1.8%

TABLE XXIII: *Why have you never set up two-factor verification for your conversations? You may choose multiple answers.*

Reason	Title	Inside	Outside
I have never noticed this feature existed.	31.2%	28.7%	35.4%
I didn't know what this feature did.	28.9%	28.7%	29.3%
It never occurred to me that I need to set up this feature.	25.9%	26.2%	25.3%
I do not use Telegram for sensitive conversations.	22.8%	21.3%	25.3%
I think the password for my phone is enough to protect my conversations.	21.3%	19.5%	24.2%
It is annoying to verify the code each time I want to log in.	17.9%	14.0%	24.2%
I have set the self destructive timer for my sensitive conversations instead.	6.8%	7.9%	5.1%
I would like to set it up but it is hard to figure it out how to do so in Telegram.	5.7%	7.9%	2.0%
Others	1.5%	1.8%	1.0%
I use Secret Chat instead.	1.1%	1.2%	1.0%

TABLE XXIV: *Why have you not used Secret Chat more often? You may choose multiple answers.*

Reason	Percent	Inside	Outside
It never occurred to me that I need to use Secret Chat.	34.7%	39.2%	26.3%
I don't use Telegram for sensitive conversations.	30.0%	23.4%	42.1%
I didn't know what this feature did.	20.7%	24.4%	14.0%
I have never noticed this feature existed.	19.8%	17.2%	24.6%
I think the password for my phone is enough to protect my conversations.	14.2%	15.8%	11.4%
None of my friends use this feature.	12.7%	14.4%	9.6%
I don't trust this feature function as it is described.	10.0%	8.6%	11.4%
I have set the self destructive timer for my sensitive conversations instead.	7.4%	8.1%	6.1%
It is hard to figure it out how to work with this feature in Telegram.	4.6%	6.2%	1.8%
Others	4.6%	5.7%	2.6%

TABLE XXV: *What do you think the Secret Chat feature does? How is it different from a regular conversation?*

Functionality	Percent	Count
Don't know	40.8%	76
Message impermanence	20.4%	38
Encryption	9.6%	18
Protection	9.1%	17
Government filtered	6.9%	13
Restricted sharing	5.9%	11
End-to-end encryption	5.3%	10
Cost saving	1.0%	2
Safe from third parties	0.5%	1

TABLE XXVI: Who do you think can read your Secret Chat messages with your friend, except you and your friend? Check all that apply.

Answer	Total	Inside	Outside
Hackers	47.2%	43.8%	53.7%
My government	43.1%	43.8%	41.9%
Telegram employees	55.6%	59%	49.3%
Other governments	32.4%	30.9%	35.3%
My Internet provider	30.6%	30.9%	30.1%
Other friends	5.1%	4.3%	6.6%

TABLE XXVII: *How much do you trust Telegram to keep your Secret Chat messages private so that only you and your friend can read them?*

Answer	Total	Inside	Outside
A great deal	5.3%	5.5%	4.9%
A lot	16.0%	18.3%	11.5%
A moderate amount	41.7%	43.0%	39.3%
A little	26.3%	25.1%	28.7%
Not at all	10.6%	8.1%	15.6%

TABLE XXVIII: *Telegram has a feature that lets you verify the encryption key for your Secret Chat. How often do you use this feature? This is a picture of what this feature looks like.*

Answer	Total	Inside	Outside
Often	4.9%	4.2%	6.5%
Sometimes	4.9%	4.2%	6.5%
Rarely	19.7%	18.8%	21.7%
Never	70.4%	72.9%	65.2%

TABLE XXIX: *Have you ever made a phone call through Telegram?*

Answer	Total	Inside	Outside
Yes	47.9%	40%	62.5%
No	33.3%	34.5%	31.2%
I don't have this feature	18.7%	25.5%	6.2%

TABLE XXX: *How often do you compare emojis when you make a phone call using Telegram? This is a picture of what this feature looks like.*

Answer	Total	Inside	Outside
Often	15.8%	18.1%	13%
Sometimes	16.4%	14.9%	18.2%
Rarely	21.6%	21.3%	22.1%
Never	46.2%	45.7%	46.8%

TABLE XXXI: Reasons given for using Telegram to share sensitive information. $^{+}$: original quote in Farsi. *: original quote in English

Code	Sample Quote
Trust Telegram security	*Emphasis of Telegram on message encryption and providing security*$^{+}$
Trust popularity of the app	*Never faced any news saying Telegram is not secure*$^{+}$
Trust based experience	*So far no one has issue with it*$^{+}$
Trust foreign country developers	*Because it is a foreign program, it is less likely to be hacked or be abused*$^{+}$
Trust through learning	*As I heard it has good message encryption And maybe as other rely on that!**
General Trust	*Just trusting the host servers*$^{+}$
Trust based on feeling	*I have a good feeling to it*$^{+}$
Trust due to message availability	*Information wouldn't be removed after reinstallation and is easy to access*$^{+}$
Convenience	*It's easier than reading them on phone, It is also available any time.**
Have nothing to hide	*It isn't about nuclear arsenal! Is it?*$^{+}$
Lack of alternatives	*Didn't have other options**
Ignore the risk	*I have never paid attention to its safety and security of my data*$^{+}$
Taking risk	*I share the pictures which are not that important and believe anything is possible*$^{+}$
Coping with perceived threats	*I wouldn't do that as it is possible, and if I do I will delete it imediately afterward*$^{+}$
Authentication feature	*Have high encryption[,] settings password*
Self filtering	*I would send the general parts and hide the more sensitive parts*$^{+}$
Secret chat	*It is possible to use secret chat and Telegram also is encrypted*$^{+}$
Not caring about security	*My work related files are not important*$^{+}$
Application fragmentation	*It is just because other people use it, and I have never heard any misuse of telegram by other parties such as government or hackers**
Message impermanence	*I wouldn't do that as it is possible, and if I do I will delete it imediately afterward*$^{+}$
Checking for hackers	*Because I am aware of security settings of Telegram and check that I wouldn't be hacked [refers to session management setting]*$^{+}$

TABLE XXXII: Reasons given for not using Telegram to share sensitive information. $^{+}$: original quote in Farsi. *: original quote in English

Code	Sample Quote
Lack of trust	*I am not sure if they share the key with anybody else or not for the right price everything is possible**
No need	*Never needed to send such information to the people I am in touch with on Telegram**
Perceived threats	*lack of trust to virtual networks*$^{+}$
Prefers alternative	*I prefer to say it over the phone [call] to feel more comfortable and secure*+

TABLE XXXIII: Quote samples corresponding to codes. $^{+}$: original quote in Farsi. *: original quote in English

Code	Sample Quote
	Technical Strategies
E2E encryption	*Sometimes I use secret chat*$^{+}$
Password authentication	*Give a password to mey telegram**
Message impermanence	*Sometimes I delete files I sent in the past from directory.**
Enable security features	*[Not] Showing last seen to strangers is one of them[,] Blocking Reporting[,] Not Using personal picture for profile**
Two factor authetication	*Just I am depending on codes that were sent to my by telegram, after signing out**
Session management	*Lock for the phone, if it needed [using] terminate session [option]*$^{+}$
Selective contacts	*Private groups only**
Credential impermanence	*I avoid sharing my information in Telegram, but if it is needed I have changed the information afterward*$^{+}$
Limit the app permissions	*I limited access of Telegram to some of data on my phone, for example my gallery*$^{+}$
	Non-technical Strategies
Self filtering	*Not very sensitive information, for example [sending] bank account without access code*$^{+}$
Preferred alternatives	*I send sensitive information via email as much as possible*$^{+}$
Side channel	*Sometimes I send half of the information via other messaging applications.**
Reliance on platform	*Use] features of the mobile phone*$^{+}$
Have nothing to hide	*I don't have sensitive information that I need to be worried about their sevurity*$^{+}$
Use secret phrases (coding)	*I try to write information in a way that only receiver can make sense of them*$^{+}$
Manual content encryption	*I usually save the information in a file, encrypt the file then send it*$^{+}$
Anonymity	*No profile picture, no full name etc**

TABLE XXXIV: User perception of what secret chat does. $^{+}$: original quote in Farsi. *: original quote in English

Code	Sample Quote
Message impermanence	*It deletes messages automatically after a specific amount of time*$^{+}$
Encryption	*It is a strictly encoded channel, I think**
Protection	*It is more secure**
Government filtered	*It is not accessible in Iran*$^{+}$
Restricted sharing	*It doesn't let the files and photos to be saved, I consider it safer*$^{+}$
E2E encryption	*Probabely it encrypt the sent signal and it is only can be decoded by the receiver phone*$^{+}$
Cost saving	*It is cheap and has high quality*$^{+}$
Safe from none-provider	*It protect information from people who don't have access the main server* *I don't have specific information that would be useful for such people.*$^{+}$