# Delta.Chat

## Needfinding report based on interviews in Ukraine, Summer 2018

19 December 2018

# Delta.Chat Needfinding Report

# 19.12.2018

## Table of Contents

# 1. Introduction

This “Needfinding Report” is based on a series of 1-2h interviews with 16 individuals from journalist, digital security trainer and activist contexts in Ukraine in 2018. We will first provide some background and context information and then present key findings and “Delta.Chat takeaways” that aim to help guide the development of Delta.Chat apps (Mobile and Desktop) during and beyond the OTF-funded “Delta.Chat Usability and Robustness” project 2018/2019. The report concludes with an Appendix on the methodology and questionnaires that were used for this research.

One of the key impulses behind the Delta.Chat effort has been to decentralize not only the technical infrastructure and protocols for end-to-end encrypted communication, but to rethink the design and development cycle from the very beginning. This means first and foremost to take user communities as active contributors whose context, needs, desires and insights should inform development priorities. Users become sources of inspiration: living and working in at-risk environments, they develop DIY combinations of tools, practices, tricks and hacks, that may hint towards new interesting features to implement, or suggest novel, original ways to solve existing problems, well-known in secure messaging fields, such as ephemeral messaging, social verification, group chat moderation or secure file sharing.

This needfinding effort has been conducted with this approach in mind, in order to enhance and inform Delta.Chat development. We also used the results of the needfinding research to design and conduct our user-testing sessions, which took place in Kyiv on October 30th-31st 2018. In this report we will first explain the local context in which Ukrainian high-risk user groups are operating. Second, we will expose our key findings and explain how these feed into further Delta.Chat developments. Finally, in the appendix, we present the methodology of our research, explain selection of interview subjects, and include our needfinding guide and the coded table.

## 1.1. About the writers of this report

Ksenia Ermoshina has been involved in the Autocrypt community since December 2016, first as a researcher focused on secure messaging protocols and usage, as well as an active user of  privacy-enhancing technologies (PETs). Her role has progressively evolved, leading to her engagement with Delta.Chat's development team as a “usability” person, though also reflecting upon her personal user-experiences as an activist, and helping with community-growing, local organizing, ensuring constant feedback between the Delta.Chat team, high-risk user groups and a more “tech-oriented” group of testers. Ksenia’s research on digital security for Crimean activists and journalists highlighted the interests of Ukrainian users, among whom Delta.Chat found its main testing playground and community connections.

Vadym Hudyma has long-term experience as a digital security trainer working with high-risk users, NGO activists and journalists in Ukraine, including at-risk groups working on the

frontlines in war-torn zones of the country. Vadym has joined the Delta.Chat effort around spring 2018, and has been working to feed his expertise as a trainer, namely with risk assessment and threat-modeling, into designing more informed and detailed use-cases for Delta.Chat. His immediate knowledge of Ukrainian context helped prepare and conduct a need-finding research in accordance to real user perspective.

## 1.2. Ukraine context information

Ukraine has pretty high Internet penetration, with at least 63% of the adult population being Internet users in 2017[1].

At this point Facebook is the biggest social network in Ukraine with nearly 10 million active users - especially after the government ban of Russia-based social networks Vkontakte and Odnoklassniki in May 2017. Facebook is also used as a major platform for political discussions and group coordination, as well as for work-related communication.

For most services, such as email, online document storage, collaboration and search, Alphabet's Google is the most widely used service. Ukraine-based email and storage providers are also quite popular across the general population but, as we will discuss later, are unpopular among high-risk users.

Successful overthrow of the Yanukovich regime in 2014, the subsequent occupation of the Crimean peninsula by the Russian Federation and war in part of the Eastern Donbass region of Ukraine have created a very complex digital environment, especially for high-risk users such as investigative journalists, human rights defenders and political activists.

While in Ukrainian government-controlled territory risk of device seizure at the moment is considered quite low, people working in or visiting the occupied areas (12,8% of Ukrainian territory[2]) often experience casual and targeted device checks and seizures, so high risk users working in those areas often employ different techniques to keep their data out-of-reach from Russian authorities.

Ukrainian users for the last four years have experienced both country-wide opportunistic waves of malware distribution (to mention just some - NotPetya, BadRabbit and BlackEnergy) and targeted attacks (mostly phishing and malware distribution) against scores of journalists, human rights defenders, civic and political activists[3] attributed to Russian intelligence services.

At the same time many of the high-risk users in Ukraine appear to be direct opponents of current political and commercial Ukrainian ruling elites - due to their work as activists

1 https://www.kiis.com.ua/?lang=eng&cat=reports&id=705&page=5.

2 http://ukraineunderattack.org/en/16245-ukraine-s-territories-occupied-bu-russia-and-pro-russian-militants-2.html

3 https://www.npr.org/2017/11/02/561521906/ap-digital-hit-list-provides-evidence-of-hackers-links-to-kremlin

criticizing government policies, working with vulnerable populations or uncovering corruption. It is widely known that Ukrainian-based service providers (ISPs, mobile carriers, email and hosting providers and so on) can be pretty easily coerced into giving up their users' information in response to legal and "paralegal" requests from government authorities.

Ukrainian journalists were also subject to phishing attacks due to their anti-corruption investigations. At the same time, even while Ukraine is considered to be a strong NATO and US ally, there is almost no evidence of EU- and US-based digital services giving up any information about Ukrainian internet users to Ukrainian authorities. So most users perceive "Western" companies, governments and hackers as much less of a security threat than both Ukrainian and Russian ones.

# 2. Main findings

## 2.1. Multi-device and operating systems usage

As expected, the overwhelming majority of interviewed users have and use, in their work- and activism-related activities, **more than one device**. Most of them use personal devices, with only a few investigative journalists using work-issued phones. There is no uniformity in what they use more often, phones or laptops.

Most interviewees are working on Windows OS but OS X is also popular, especially among journalists. It is important to mention that those activists who are Linux users are generally not tech-savvy.

iOS and Android usage are more or less evenly distributed. Users mention that iOS was preferred for security, but Android phones are more often used as cheaper, throw-away "mission phones".

***Takeaways for Delta.Chat***

*Reality of mixed and multi-device usage calls for uniform design and feature implementation on desktop and mobile devices, as well as across different OS. Desktop and mobile versions are equally important. In case of possible development of Linux, Delta.Chat clients' ease of use and install should be comparable to other OS.*

## 2.2. File management and attachment workflows

Email is still more heavily used for formal communications, especially sending and receiving of official documents. Email service is also perceived as more reliable and better searchable storage for important documents and files, compared to messengers. The sending and receiving of documents, photos, videos and other files happens both through emails and messengers. A common practice is to share attachments via URLs from an external cloud service (mainly Google Drive) over a messaging app.

We have identified an interesting workflow pattern: the attachment is sent by a source or a contact via smartphone using one of the channels perceived as more secure - usually via messengers like WhatsApp or Telegram, but also via Signal. Once the attachment is received, users forward it to themselves using another channel (usually to an email account or via Facebook messenger) in order to download them later and work with them on the Desktop. An often cited reason for this workflow is the ability to store and find those documents later, if needed.

Most of the users interviewed receive attachments at least 2-3 times per day, while others reported to work with attachments only 3-4 times per week. However, this load is not

constant, becoming more or less important during specific events. Thus, journalists and activists reported that sometimes they can get a very heavy load of incoming emails or messages with attachments in a comparatively short time – for example when receiving official responses to requests for public information or batches of photos and text materials from reporters/documenters working "on the ground".

***Takeaways for Delta.Chat***

*The short-term but heavy-load spikes of attachment-related activities, as well peculiar file-management practices suggest a strong need for built-in features for file management – bulk file upload/download, file and link previews, searching/filtering by name and file types and so on.*

## 2.3. Voice and video functionality

Most people use text messages and rely less on video and voice calls, the latter being perceived as more onerous. However, for many high-risk users, the ability to talk with voice is perceived as more secure than texting.

Video chats are rarely used, but sometimes may be used for identity verification of the person on the other side, and then communication switches to a voice call. For group voice and video calls high-risk users rely mostly on WebRTC platforms, Skype being less common. Only one person mentioned a specific tool suggested by their organization for conference calls.

***Takeaways for Delta.Chat***

*These findings suggest that while voice communication is perceived by many users as a basic feature, video conversations are considered more as an additional, inessential feature. Overall video is still considered as a separate service.*

*Users tend to deploy various out-of-band DIY verification methods – and this will happen regardless, even if a messenger implements its own verification process.*

## 2.4. Messengers: usage patterns and choice motivations

Both emails and messengers are equally used for work and activism, while most users reported that they rely more heavily on messengers for personal communications. Most of the interviewed users have between four and ten distinct messaging apps on their devices.

Every interviewee has a separation between colleagues and family, but the majority of respondents were adding separate categories, such as friends, sources, activists. For one respondent it was important to separate long-term and "ad-hoc" project collaborators, and implemented that separation in their contact management.

Tool propagation (how a tool is recommended to others) strongly differs depending on subject groups: while activists are very proactive in pushing their contacts to use tools which they consider as “safe”, most of the journalists and trainers said they would rather ask

a contact which tool they prefer using and then suggest to use the one considered as the safest in their particular environment. In general, tool adoption happens mainly based on the network effect, “a tech friends’ recommendation”, and a tool’s UI/UX or additional features, such as channels. Only one person chose a messaging app based on consulting online guides or materials. Among other curious motivations, "a movie about hackers" was mentioned as the source for a messenger choice.

Due to local context **Facebook Messenger** is listed as the most popular app. Facebook being the most used social media in Ukraine, it has a strong network effect that appeals with features such as contact discovery and contact verification, which are important for high-risk users. Other important functionalities of Facebook Messenger, repeatedly mentioned by interviewees, were the search function and accessibility of files and photos in the message history [with some elements of “dashboard-like” organization by file type and date].

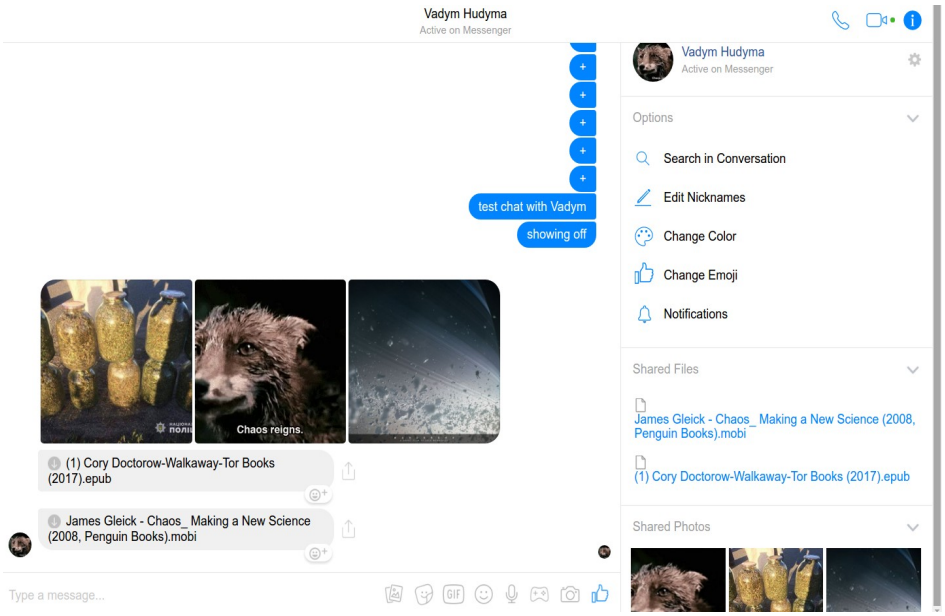


*Fig.1: Example of multimedia and files organization in Desktop Facebook Messenger*

The two next most-used apps mentioned in the interviews were **WhatsApp and Telegram**. Both are perceived as “more secure” than Facebook Messenger, and are chosen for conversations that need more "protection".

Journalists who work with photography emphasize the image compression in popular messengers as a problem, and this becomes the argument to opt for Telegram and Viber, which offer the ability to share photos as “files”, thus avoiding loss of image quality.

The feature of ‘channels’ along with “perceived security” were mentioned as reasons to opt for Telegram.

Contrary to expectations, **Signal** is used by only seven people out of sixteen, and only two of these seven are activists. Users say that they have “very few contacts on Signal”, which leads to infrequent usage and slow reaction to notifications. Users say that they have tried

to move their conversations to Signal but “could not convince others in their network to switch from other apps perceived as “more convenient”, such as Telegram.

Viber is used mostly for family and child-related conversations (kindergarten/school/etc groups)  which is country/region-specific.

Group chats are mainly used for coordination or as a way of introducing people to each other. Also, in some messengers, large group chats are used basically as a substitute for Telegram-like channels – as a broadcasting platform on some very specific topic. Users expressed a need for easier and distinct switching between direct messaging (one-to-one) and group chat contexts.

***Takeaways for Delta.Chat***

*As expected, network effect plays the most important role in the choice of messaging apps. It also helps to realize additional security-related features such as casual contact verification through bundled social network, and assisted contact discovery through shared contacts. For Delta.Chat, which builds upon the largest existing decentralized communication infrastructure – email – there may be a way to help the contact discovery process, for example by indicating if any of a person’s contacts start using Delta.Chat. Simple technical notifications are not a good way to announce this, however, as they are considered to be extremely annoying both on Signal and FB Messenger. Some UI innovation may be required.*

*The multi-messenger usage patterns and compartmentalization practices show that users are not searching for a “perfect app” that would “solve all their problems”, but are used to switch between various tools for various contexts and features. This gives room for Delta.Chat integration within this user workflow, without an ambition to “replace” other tools.*

## 2.5. Email usage and perceptions

Users had between one and ten different email accounts, with the average number of regularly-used accounts being **three**. At least half of the users had a separate account for "spam", junk website registration and other "not important" things. Many users have dedicated work email accounts created by their employers (usually Outlook accounts are provided as a part of Office365 infrastructure), which are rarely used. The majority of users were using Gmail. Only few use local service providers and only for unimportant conversations.

*It was interesting to find that most work- and activism-related communication happens over personal email, even if users may have many different accounts.*

People prefer webmail over email clients which are very rarely used. Amongst email clients: preinstalled Mail for OSX / iOS or Thunderbird were most popular. Shared email is not a totally absent practice: one person said that they have given access to their email account to a trusted contact, and one asked for a feature to be able to do so with a regular reminder

that this option is enabled. Three journalists reported that they access directly a shared editorial inbox or forward their emails there.

Email is preferred to instant messaging in the situations where communication is perceived as "official" or "serious" or "important", while offering less stress and more flexibility for answering. At least two people mentioned that it was easier to write longer messages in email. A few associated a particular temporality with email, considered as a less "urgent" and “stressful” means of communication as opposed to IM. Email is also widely used for registering accounts and confirmation, as well as a place for reviewing security notifications.

Among advantages of email over instant messaging, the following features were mentioned: more usable file sending; better search and storage of files and of the content itself; “drafts" and saved emails.

***Takeaways for Delta.Chat***

*Aforementioned findings show that emails still wins over IM in usage for more official and long-term business conversations. Email is also largely perceived as more usable for file sharing and longer-term work with attachments and texts. This may be related to association between email and Desktop / keyboard, which means that Delta.Chat desktop could offer many of the aforementioned UX-related features associated with emailing, in combination with actually using email infrastructure.*

*The lack of email-client penetration among users means that most of the users have their IMAP settings in the default state depending on email service provider.*

## 2.6. Default settings

When installing tools users tend to change default settings, with only five respondents claiming to have kept default set ups. Out of sixteen interviewees eight have configured two-factor authentication (2FA), three have changed notifications, three have disabled the default back-up function on WhatsApp, and at least two switched off the "last seen" or "last active" indicator. One person set up a passlock, as “protection” against accidental use of the app by children.

***Takeaways for Delta.Chat***

*Users have developed a culture of checking their settings, and have certain experience with adjusting default settings. This gives Delta.Chat some flexibility for inserting some of the advanced features “further” in the app and suggesting various combinations of “defaults” to choose from. However, security/encryption-related parameters should still be an opt-out rather than opt-in.*

## 2.7. Instant messenger account creation: email or phone number?

Overall, email is perceived as safer for account creation compared to phone numbers. Only one of sixteen respondents said they were uncomfortable with their email being used for registering in an IM.

However, users are reluctant to create specific email accounts for registering a new instant messenger. Most of interviewees stated that they would rather use their existing email address to register for a new IM. Two users said they would create a new email address for an instant messenger used for more "dangerous" purposes. One person said they would go for a new email address if it was easy to create.

More than half of the high-risk users considered phone numbers as the primary means of IM registration as problematic. One journalist observed that phone numbers were "hard to change" due to social reasons (network effect), and recalled incidents when journalists' phone numbers were leaked to potential adversaries. The high-risk journalist who was comfortable with phone number as a registration method, also mentioned that phone number was an easy way for contact discovery. One person said that phone numbers provided an additional "verification" of identity, however, this respondent said that they are aware of security issues related to phone usage.

Two respondents (both digital security trainers) stated that phone number is acceptable for IM registration, but only if the IM has 2FA as an option - implying that in this case they are much more concerned about account security than anonymity.

***Takeaways for Delta.Chat***

*While ability to easily generate throwaway or dedicated accounts will be a useful and appreciated feature for high-risk IM users, it should be expected that most users will try to register their new Delta.Chat account using their primary email, unless specifically told to do otherwise. These choices and their consequences for user experience will be discussed further in the user-testing report.*

*As expected, phone numbers are considered a less preferred means for IM registration than an email address. While useful for easy contact discovery, many users are both aware of and uncomfortable with the risks associated with mobile phone networks usage (for example, location monitoring and association of IM account with their primary phone number).*

*It is interesting to note that nobody mentioned the use of burner or secondary phone numbers as a registration method.*

## 2.8. Anonymity and aliases

Contrary to our hypothesis that high-risk users would need anonymity by default, the question about the need for **account anonymity** (anonymity from another users, not from the service provider itself) received mixed responses.

For half of the users it was not important to prevent others users from knowing their true identity. Four users reported, that it may be important while dealing with some, but not all, contacts. Three respondents stated that it was crucially important to stay public.

As for the usage of different **aliases** for the same account (for family and activist groups, for example) responses ranged from “not important” to “useful as an option”.

When asking if users wanted their account handles to be **searchable** in integrated public directories or built-in search engines, we received reactions that ranged from rejection of the idea to considering it an important need.

Other instant messengers have faced this same controversy, such as Wire, against which many users complained to be accidentally able to search for users they had no contact with.

A much more uniform response was received regarding **reachability** or **contact request** features – the ability to start conversation/approve contact only with/without prior consent. All users said they want to have a contact request feature **enabled as a default option,** with some users requesting to be able to switch it off if needed for public-facing accounts or other similar use cases.

***Takeaways for Delta.Chat***

*These findings show that while ideally an application should give users some ability to have account anonymity, this should be offered in the form of an option, even if a default one. Contact request features should also be a default option, with a possibility to opt-out. Aliases and temporary accounts for short-term missions may be a good option for journalists and semi-public activists, as well as for average users. Overall, Multi-account handling features are highly desirable.*

## 2.9. Perception of risks and adversaries

We probed our interviewees against a list of various actors, asking who they would trust with their data. Almost no-one trusted local government and service providers. However, when it comes to foreign entities, interestingly, people tend to trust foreign service providers more than foreign governments. Less than half said it was "totally unacceptable" if foreign service providers had access to their data. One user mentioned that they are OK with access by automatic scanners / bots, but not by a human agent, and one mentioned that they would prefer Facebook accessing their data because they have some kind of transparency of their data policy, but not a foreign ISP who will sell their data for unknown purposes.

Strangely, but as expected - people tend to trust their families even less than foreign service providers: only one user of sixteen reported that it is acceptable to for their family to have any access to their data, and another “specified” that "it is unacceptable if it is something I want to hide from them".

“Privacy” was not an issue in itself, and people tend to trust services such as Gmail and Facebook, based on their transparency of reports and based on the assumption that those actors are outside of their threat model.

## Behavior in risky situations

In terms of risks, the majority of users reported that accidentally sending an unencrypted message would be either “catastrophic” or “very bad”, while accidentally sending a message to a wrong contact is perceived as less disastrous. At the same time, it turns out to be crucial for the majority of users to know if the person on the other end is indeed the correct person: verification was perceived as “very important” or “important” by the majority of those interviewed.  In terms of compromise between archiving and deletion, generally for our respondents the ability to fully delete messages, contacts and files was perceived as more important than the ability to keep access to them.

*Police intervention at a gathering of  an NGO, 2017 [courtesy of an interviewee]*

We have synthesized interviewee responses to various situations in the following table:

| **If your device is broken or stolen, how important is it for you to access your:** | | | | | |
|---|---|---|---|---|---|
| | Very important | Important | Medium | Not very important | Not important |
| Message history | 3 | 2 | 5 | 2 | 4 |
| Contacts | 8 | 5 | 5 | 2 | 4 |
| Files | 5 | 2 | 3 | 1 | 5 |
| **How important is it for you to be able to intentionally delete your:** | | | | | |
| Message history | 13 | 2 | 1 | 0 | 0 |
| Contacts | 4 | 9 | 0 | 0 | 3 |
| Files | 11 | 5 | 0 | 0 | 0 |
| **If your device is broken or stolen, how important is it for you to remote-delete your:** | | | | | |
| Message history | 9 | 6 | 0 | 0 | 1 |
| Contacts | 8 | 6 | 0 | 1 | 1 |
| Files | 10 | 5 | 0 | 0 | 1 |

Users reported vastly different reactions to unusual or risky situations they found themselves in or at least have a perception of being in one. Reactions varied and included creating and using new dedicated email and social network accounts when crossing the border or working in a dangerous area, switching to other tools perceived to be more “secure”, disabling GPS tracking on their phones and enabling 2FA on important accounts or simple temporary log-out. Some users were switching to different (reserve) email addresses to mitigate against contact attacks targeting a publicly known contact. Device encryption was also used, but there were reports of permanent data loss because of it.

Journalists also reported using specific – usually cheaper - devices while conducting work in high risk areas as well as cleaning or wiping devices completely. Users also mentioned the practice of designating a "trusted contact" for emergency scenarios.

In a "high risk" situation, more than half of users mentioned switching to "more secure" end-to-end encrypted messengers: WhatsApp, Signal, Telegram secret chats and Wire. Some of them used Facebook calls or Jitsi, considering voice and video conversation to be more secure than texting. Face-to-face meetings were also mentioned as an option for high-risk scenarios.

Generally, the device itself was perceived as being more at-risk than the server, and the contexts of being “in the field” or situations of “border crossing” were associated with more

risk than everyday office-based work with documents, even if the latter included working with sensitive documents and data.

***Takeaways for Delta.Chat***

*Users highly value remote deletion, and perceive storage and access as less important when compared to security. They also perceive the end-user device as being much more fragile than the server or an office-based machine, which means that, for use-cases of temporary high-risk missions for journalists and activists, one-sided deletion and ephemeral chats should be a feature. Synchronization and remote deletion of messages, files and contacts should be considered as a crucial feature of multi-device operations.*

## 2.10. Storage and Search

All users realize that existing instant end-to-end encrypted messaging applications and clients for email encryption have their limitations. Among the biggest criticisms directed at messengers is the absence of or unreliability of search functions for messaging history and across files. As reported earlier, this was also the main reason for choosing email over instant messengers for important conversations or establishing long-term cooperation.

Many users reported that they were annoyed by notifications. Signal was criticized specifically for its frequent technical notifications about new users and deleted accounts.

Users complained about being added to channels without explicit consent over Telegram. The same applied to Facebook groups. Contact request/approval, such as the one used in Wire, was mentioned by activists and journalists as good feature to have. Telegram was mentioned as having too many annoying bots and a bad system of channel commenting. One user also mentioned the need for a clear separation between or grouping of channels, groups and one-to-one conversations.

Some users were annoyed about the absence of choice as to where to save images (e.g. saving to gallery by default).

When asked to name one feature, absence of which would be a reason to STOP usage of some particular messenger, most of the high-risk users mentioned both disappearing messages (with preset timer) on all devices and remote message deletion (at will) – depending on the messenger they chose to talk about. Only two users mentioned end-to-end encryption as the most important security feature.

Other features frequently mentioned as “crucial” were: the ability to send and download files, file preview, “no” file limit on sent files, ability to sync messages with a laptop, ability to run a messenger on own servers and ability to mute some conversations.

When asked to name the most important features they would like to see in their favorite messengers, **general search** in messages and files was again the priority, especially when talking about end-to-end encrypted messengers.

Users also mentioned file storage as a useful feature – either in the form of integration with some kind of cloud service such as Google Drive or Nextcloud or easily accessible and searchable in-app file storage.

Journalists specifically mentioned that they would appreciate the ability to send photos without compression and associated quality loss.

We heard an interesting suggestion to implement message pinning in groups and channels – having one or a few messages pinned to the top of the screen for newcomers to read or as a place to have general tips for the group/channel readers and participants.

Another feature requested was integration of the messenger with a calendar, with the ability to automatically add dates, times and events from message threads to the calendar – something similar to an existing feature implemented in FB Messenger now.

**Takeaways for Delta.Chat**

*For Delta.Chat these findings indicate a clear roadmap for future feature developments. A fully developed file management system seems to be a worthwhile time and effort investment for a wider user base. Features such as path choice for attachments would be highly appreciated. Additionally, disappearing messages and an easy way to remotely and locally delete messages and conversations was considered a basic requirement in any modern secure messenger.*

*Other important features concern what can be called "organization of workflow": the ability to tag and organize contacts and chats, or pin messages.*

*The ability to curate content and contacts (whom to talk to and what to read), e.g., the contact request feature and the ability to give, or not give, explicit consent before the start of a conversation or before being added to any group or channel, may also be appreciated by both privacy-minded and publicly-exposed users.*

# Appendix: methodology and guide

## I.1. Research Questions

- *What are the current workflows that targeted users have? How do they organize their workday across devices and across multiple communication tools?* This question helps to Identify how Delta.Chat would fit into this workflow, to probe a use-case for media organizations and NGOs that includes remote fieldwork in at-risk areas and desktop-based administration from a central, safer location;
- *How is "identity management" happening? How important are anonymity and metadata protection for users?* This question helps to identify if Delta.Chat should focus on multi-aliases or multi-accounts, or other solutions for users with particular needs for ephemeral or multiple identities.

- *How do targeted groups perceive and define "risk", "security" and "privacy"? What are the various strategies they develop in order to cope with situations described as "risky", or to improve their general feeling of "security"?* To identify how exactly Delta.Chat should inform users about the various security properties it can provide. To improve our wording for notifications and information about various features. To help trainers who may recommend Delta.Chat to better integrate the tool in their risk assessment / threat-modeling activities.
- *What are users' emotions and feelings about the secure messaging tools that they currently use? What are the main positive and useful features of these tools? What are the main blockers and missing features in these tools?* To identify how Delta.Chat can actually differ from other secure messaging applications, without the desire to compete or to do "everything", but better find its own place in the evolving field of secure messaging and respond to urgent and unaddressed needs.
- *What does it mean to "trust" a tool? How do targeted groups choose privacy-enhancing tools? Probing two main aspects:*
    - Identify various sources of information that users build their choices upon, such as: personal search for online materials or advice from a technically experienced colleague / friend or digital security trainings or inner organizational security policy;
    - Do targeted users make their choices based on technical aspects of a tool, or are other factors more important? (such as open source vs closed source; centralized vs decentralized; the reputation of the app's creator; the funding sources of a certain app);

This helps us to understand how to better communicate about Delta.Chat, which strategies to choose in order to let users know about the app, how to work with existing communities and which aspects of Delta.Chat we should better explain to potential users.

# I.2. Methodology and ethics

The interviews were conducted in the period between September 1st and September 15th, 2018. The interviews lasted between 1 hour and 1 hour 30 minutes and were recorded on audio, using an offline recorder for security reasons. The questionnaire was designed to avoid any biographical details or details about the work or activism of our respondents. The questions focus on user behavior and do not request any political information that could put our respondents at risk.

Before the interviews, we explained to the interviewees the goal of this research. We also explained how the data obtained during this research will be stored and used. We explained to the interviewees that no one except for the two interviewers would have access to the audio recordings or transcriptions. We explained that the audio recordings will only be stored until the date when transcription and coding of the interviews is finished, and after that securely deleted (by October 20th, 2018). We explained to the interviewees that the

technical team of Delta.Chat may have access to the anonymized and coded interview results, that will exist in form of a Spreadsheet.

The anonymization process includes attribution of a special coding system: A2... A5 for activists, J2...J5 for journalists, T2...T5 for trainers. No personally identifiable information such as names of the organizations where people work or other names and references are mentioned in the Spreadsheet.

All the interviewees gave their preliminary consent to being recorded. We explained to the interviewees that they have the right to avoid answering any questions that they may find inappropriate, or ask us to stop recording them at any time. When working on the actual questionnaire, we made all the necessary efforts to avoid particular technical terms and to let users define by themselves key notions such as "risk", "threat", "adversary", "privacy" and "security".

## I.3. Interview subjects selection criteria

Interview subjects were selected based on preliminary research and discussions with Delta.Chat developer team, as well as based on experiences of Delta.Chat UX/UI team. Ksenia Ermoshina's postdoctoral fellowship research, focused on Crimean and Ukrainian high-risk journalists and NGO activists, showed that these two groups were particularly interesting to interview, as they were actively using a variety of messaging applications (average of 4 applications). They had interesting workflows, and have developed their own patterns of usage of various privacy-enhancing tools, combining them in an unusual way, in order to fill in the gaps and gain some features that lacked in existing secure messaging solutions.

Vadym Hudyma, working as a digital security trainer for several years, has a rich experience of collaboration with media organizations and human rights groups operating in Ukraine. His training experience has shown that Ukrainian media and activist communities can be a prolific source of insights and inspirations for developers working on secure messaging. The specifics of Ukraine, a country with good Internet penetration, an active Internet freedom community, quite advanced and promising civil society initiatives, coupled with economic crisis and an ongoing armed conflict, itself presents an interesting use-case for needfinding research that differs from "First world problems", but is closer to the Delta.Chat team than more remote regions of the so-called Global South. With Ukrainian user-groups we could achieve a balance between distance, needed to analyze, and proximity, needed to empathize with our users, and properly listen to and understand them.

We have focused on three user groups: human rights activists, journalists and digital security trainers. Activists and journalists may have very similar use-cases, that include remote fieldwork in at-risk areas, with mobile devices, for data collection and real-time reporting. However, from an organizational point of view, these groups differ: for example, Ukraine counts a growing number of freelance journalists, who cannot always rely on their editors for legal support and digital security guidance. NGO workers, as Ksenia's research

on Crimea has shown, have better security policies and often receive more funding for digital security audits and trainings. Also, the kinds of data both groups work with are slightly different: journalists often report information that can be publicly shared, while activists are often engaged in monitoring missions that involve working with very sensitive personal data. Journalists often need to share more multimedia files, in a more urgent way, while activists, especially human rights defenders on monitoring missions, do not work in the same rhythm of "urgency". However, both communities are very closely interrelated: many activists also do reporting work and assume roles as social media streamers during important political events such as rallies, elections, gatherings and court hearings. Journalists may also play a crucial role in making visible various human rights violations.

As for digital security trainers, this group is interesting because trainers deal with many use-cases, are exposed to different user-groups and are aware of their threat-models, misconceptions and preferences. Moreover, trainers are aware of the most recent developments in secure messaging and, as power-users, they can offer a slightly different point of view on existing solutions in the field. Their critical perspective can be interesting for us to understand the propagation of different tools.

# I.4. Needfinding Interview Guide

**User flow**

- How many devices do you have?
- How often do you use your phone vs your laptop?
- How often do you send and receive attachments? How do you like to send / receive them?
- Do you download attachments on your phone or prefer using desktop?
- What operating systems do you use on your devices?
- How do you usually communicate online? What do you prefer: voice vs video-call vs message?

**Messaging apps**

- How many and which messaging applications do you have on your phone?
- How often do you use X vs Y vs Z [rate by popularity]
- How often since this morning have you used this app?
- Why do you use these apps? How did you chose them?
- Do you use group chats? For what?
- Do you have any problems with how group chats work in the apps you use?
- Do you use any group video / voice chats?
- Is there any particular feature you are missing that you would like to have implemented?
- How many members are there in the groups that you are using
- What's the most annoying thing about the app(s) you are currently using?
- Are there features in your current App that you would not want to miss?

**Email**

- How many email accounts do you have? How do you differentiate between them?
- Do you use a standalone email client
- if standalone --> have you configured by yourself? was it hard?
- Does anyone else use or has access to your account?
- Why have you chosen these providers? Do you trust them? Why?
- When do you prefer email over IM?
- Have you ever tried encrypted email?
- If no - why? Have you heard of email encryption?
- If yes - do you still use it? How often? What are your thoughts / experiences with it?
- Do you want to avoid your email to be associated with your messenger?
- Would you rather create new email to avoid messenger account associated with you or use your normal email?

**Installation / Sign-up and permissions**

- can you describe the installation process of X app
- what does it mean for you to use a phone number for signing up
- have you ever looked at permissions of different apps that you use?
- have you ever cleaned your phone memory / RAM / processes?
- do you often stop the applications running on the background?

**Notifications**

- how do you feel about notifications?
- how often do you turn them off?
- what's the acceptable 'degree'/frequency of notifications
- Do you want to have notifications across all your devices (desktop / mobile / other) or only at the most used / most recent used? [probing also wearables like watches]

**Compartmentalization / social graphs**

- could you identify main groups of people to whom you communicate?
- what do you use when you communicate to
- how do you communicate to sources / funders / people at risk
- when you need to contact a person, you:

    A) "force'' / suggest the person to use a specific tool?

    B) the person asks you to use a specific tool?

    C) you both switch to a 'default' tool you both have?

**Organizational policy**

- When you feel you have a technical issue, how do you act?

    A) look for advice online [Google search / forums ...]

    B) ask a tech friend

    C) ask the system administrator from work

    D) call a tech firm/support

does anyone help you with:

    A) your laptop

    B) setting up your accounts (email, messaging... anything else)

- where does this person come from?
- Does everyone in your organization use the same workflow as you?
- Does your organization have any written / taught documentation / advice / roadmap for communications?
- Have you attended any trainings?

**Trust choice**

- Do you know who is the owner / founder of X app that you use?
- Do you know how the app is funded? What does it mean to you?
- Is it important to you that an app is open source? Do you trust closed-source apps at all?
- If yes: Did you er check the code of the App that you use (or any other program)?

**Perception of unusual situations, risks**

- Can you describe the last time when you had to change your usual workflow?
- What tools do you use when you are not sure that a situation is safe / stable ?
- If any of your trusted apps stops working, what would you do?

**Access risks**

- Rate how acceptable it would be if your message could in theory be read by:

    Your Government

    Foreign Government

    Local Service provider

    Foreign Service provider

    Friends/Family

**Identity risks**

- How important is it for you to hide an identity behind your online account (preventing people to know who you are)?
- Do you want to use multiple aliases / addresses? (family knows a different "you" then activists)
- How important is it for you that other people are able to find your account?
- Rate how bad it would be if some messages will be send unencrypted, and someone will read them?
- Rate how bad it would be if some messages are sent to the wrong person in your contact book?
- Is it important to make sure that people on the other end of the line are those they pretend to be?

**Data integrity risks**

**Puddle test**

- If your device is broken or stolen, how important is it for you to access your:

    - Message history: Very Important -> Not Important

- Contact: Very Important -> Not Important
- Files: Very Important -> Not Important

**Hammer test**

- How important is it for you to be able to intentionally delete your:
  - Message history: Very Important -> Not Important
  - Contact: Very Important -> Not Important
  - Files: Very Important -> Not Important

**Hammer vs Puddle**

- What's more important - be able to recover your messages/contacts/files in case of accident or be able to delete them forever?

**If your device is broken or stolen, how important is it for you to remote-delete your:**

- Message history: Very Important -> Not Important
- Contact: Very Important -> Not Important
- Files: Very Important -> Not Important

**Other risks**

- How important are for you the disappearing messages?
- How important for you are messages on the locked screen?
- Are you worried that people around you can read your messages?
- Is there a risk of someone to force you to give access to your device/account?
- Is it a problem if someone will know that you're using some particular app?
- If yes, what you do in that case (open question)

**Needs and desires**

- How would you react if:

        - messages do not arrive at all
        - messages arrive with 30 seconds latency
        - with 2-5 minutes latency
        - with 5-15 minutes
        - 15-30...
        - several hours
- would you want to be able to manually, but reliably, check for new messages and would that change your reaction?
- do you need a tag / label system of managing your contacts / grouping them?
- Would you want your Messaging App to group your chats based on the groups you talk to?
- What would be the most wanted/needed feature you'd want to have in the messengers you're using now?

    - Doodle?

    - File storage?

    - Calendar?

**Extra questions**

- Do you want the app to be able to create a new E-Mail Address for you to use with the app? (Kind of a 'registration' process)
- Do you want to be able to send an Invitation Mail with instructions to new People?
- Do you know if your favorite apps are centralized or decentralized?
- Do you care about decentralization?

## Links to know more:

- ➔ Delta.Chat website: https://delta.chat/en/
- ➔ Delta.Chat repository: https://github.com/deltachat/
- ➔ Join the Delta.Chat mailing list for community discussions: https://lists.codespeak.net/postorius/lists/delta.codespeak.net/
- ➔ Join IRC channel **#deltachat** on freenode!
- ➔ Delta.Chat gathering in Kyiv – sharing our experiences and engagements with local communities: https://delta.chat/en/2018-11-17-deltaxi