



HUMANITARIAN FUTURES FOR MESSAGING APPS

UNDERSTANDING THE OPPORTUNITIES AND RISKS
FOR HUMANITARIAN ACTION

THE
ENGINE
ROOM



ICRC

Syrian refugees, landed on Lesbos in Greece, looking for a mobile signal to check their location and notify relatives that they arrived safely.



ICRC

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01 F +41 22 733 20 57
E-mail: shop@icrc.org www.icrc.org
January 2017

Front cover: I. Prickett/UNHCR

HUMANITARIAN FUTURES FOR MESSAGING APPS

**UNDERSTANDING THE OPPORTUNITIES AND RISKS
FOR HUMANITARIAN ACTION**

This report, commissioned by the International Committee of the Red Cross (ICRC), is the product of a collaboration between the ICRC, The Engine Room and Block Party. The content of this report does not reflect the official opinion of the ICRC. Responsibility for the information and views expressed in the report lies entirely with The Engine Room and Block Party.

Commissioning Editors: Jacobo Quintanilla and Philippe Stoll (ICRC).
Lead Researcher: Tom Walker (The Engine Room).
Content: Eytan Oren (Block Party), Zara Rahman (The Engine Room), Nisha Thompson, and Carly Nyst.
Editors: Michael Wells and John Borland.
Project Manager: Waiyee Leong (ICRC).

The ICRC, The Engine Room and Block Party request due acknowledgement and quotes from this publication to be referenced as: ICRC, The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*, January 2017.

This report is available at www.icrc.org, <https://theengineroom.org> and <http://weareblockparty.com>.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit: <http://creativecommons.org/licenses/by-sa/4.0/>.



TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
INTRODUCTION	9
1. THE GLOBAL MESSAGING-APP MARKET	15
The rise of messaging apps	16
Emerging trends: Broadcast Lists, encryption and chatbots.....	18
Access to messaging apps: Affordability, connectivity, gender and age.....	21
2. HOW ARE PEOPLE USING MESSAGING APPS IN SITUATIONS OF CRISIS OR ARMED CONFLICT?.....	31
Overview: Variation and fragmentation	32
Which apps are people using?	34
How are people using messaging apps in humanitarian crises?.....	37
What are people in crisis situations using messaging apps for?.....	38
What don't we know?	41
3. HOW ARE HUMANITARIAN ORGANIZATIONS USING MESSAGING APPS?	45
How organizations are using messaging apps.....	46
Why are organizations adopting messaging apps?.....	46
How are apps being incorporated into organizations' work?	51
Potential applications.....	54
<i>Using one platform to send messages from multiple messaging apps</i>	<i>54</i>
4. CONSIDERATIONS WHEN USING MESSAGING APPS IN HUMANITARIAN SITUATIONS	59
Working with messaging app providers: Challenges and risks.....	60
Threats to messaging app users' security and privacy	61
Consent.....	65
Messaging app features related to privacy and security	67
Operational considerations	71
5. RECOMMENDATIONS.....	75
General principles.....	76
<i>Privacy, security and data protection</i>	<i>77</i>
<i>Implementation</i>	<i>78</i>
<i>Collaboration with local media and other partners</i>	<i>78</i>
<i>Practical considerations.....</i>	<i>79</i>
ANNEX	
WHAT KIND OF MESSAGING APPS ARE AVAILABLE, AND WHAT ARE THE KEY DIFFERENCES BETWEEN THEM?	81
Operational considerations.....	83
<i>Registration.....</i>	<i>83</i>
<i>Connecting with users.....</i>	<i>83</i>
<i>Encryption</i>	<i>87</i>
<i>Other functionalities.....</i>	<i>89</i>
<i>Data protection.....</i>	<i>89</i>



P. Yazdi/CRC

A Somali woman using her phone at a camp for internally displaced people in Beletweyne, Somalia.

EXECUTIVE SUMMARY

Messaging apps are the fastest growing digital communication phenomenon ever. Messaging apps like WhatsApp, Snapchat, Viber, WeChat, Telegram and LINE are becoming the primary mode of communication for hundreds of millions of people around the world, including people affected by natural disasters or caught up in armed conflicts.

Already, more than 2.5 billion people around the world use messaging apps¹ – a figure that is expected to grow to 3.6 billion by 2018.² As of November 2016, more than one billion people – nearly one in seven people on Earth – were reportedly using WhatsApp.

As smartphone ownership and messaging-app usage continues to rise, it is clear that messaging apps are here to stay. However, humanitarian organizations have so far only conducted limited research into where and how messaging apps could help improve their work. Using messaging apps also introduces critically important questions about security, data protection and privacy, and creates technical challenges for information management and data analytics.

These unresolved questions are hampering discussions in humanitarian organizations about the practical uses of messaging apps as an operational tool, both for two-way communication with local communities, and for internal coordination, information-sharing and management.

Humanitarian organizations need to better understand how to make use of the opportunities that messaging apps offer. To do so, they should establish strategies and standards to determine where messaging apps might be appropriate, how to use them effectively and how to meet the responsible data challenges they pose.

Here is an overview of the report's recommendations, which are given in full in Section 5.

GENERAL PRINCIPLES

- **Conduct detailed, locally focused research into factors affecting how crisis-affected groups use and share information.** Before adopting any new communications channel, organizations should learn how the people they want to reach communicate and which channels they already use and trust.³ On this basis, they can determine whether using a messaging app is appropriate in that situation.
- **At a minimum, humanitarian organizations should systematically include questions on access to and use of mobile telephony into humanitarian needs assessments.** Failing to ask such questions can lead organizations to make assumptions that significantly limit their effectiveness and accountability to people affected by crises.
- **Use a range of communications channels, rather than relying on one messaging app.** Organizations should ensure that any use of messaging apps forms part of a multi-platform, multi-channel communications strategy rooted in a deep understanding of the local information ecosystem.
- **Plan well in advance.** Put in place strategies and processes for using messaging apps well before they are needed in a humanitarian crisis.

1 Activate, *2016 Tech and Media Outlook*, 2016: http://www.slideshare.net/ActivateInc/activate-tech-and-media-outlook-2016/2-Over_the_next_five_years.

2 Activate, *The Messaging Phenomenon Has Hardly Begun*, 2016: <https://medium.com/the-activate-outlook/the-messaging-phenomenon-has-hardly-begun-cdaef735cb2#.n4z29ppml>.

3 For an example of how to approach this, see Kelly Church and Laura Walker McDonald, "Announcing SIMLab's framework for context analysis of inclusive technology in social change projects", August 2016: <http://simlab.org/resources/contextanalysis>.

- **Consider who messaging apps won't reach.** As with any technology, messaging apps can exacerbate inequalities associated with gender, age, literacy and experience with technology, as well as access to energy, mobile phones and network connectivity. Organizations should therefore conduct thorough research into factors that affect messaging apps' accessibility and usability.
- **Test, test and test again.** Approaches that are successful in some areas will fail in others. Organizations should build in enough flexibility to allow for iteration and adaptation in response to feedback.
- **Deploying messaging apps may be the easy part - building trust with communities is much harder.** Developing strong local relationships depends on providing effective on-the-ground support, accompanied by information that is up-to-date, timely, actionable and trustworthy. Introducing messaging apps will have very limited impact if organizations do not also invest in ensuring that these apps are part of a reliable, sustainable and useful information distribution service.

PRIVACY, SECURITY AND DATA PROTECTION

- **Assess the risks that any messaging app introduces.** Organizations should assess what data and metadata different apps collect, and whether the collection of that data could increase risks (and the type of risks) to individuals or groups if a particular app was used in a given country or region.
- **Prioritize individuals' privacy and security when choosing a messaging app.** Organizations that decide to use messaging apps should aim to select apps with end-to-end encryption enabled by default, run by organizations that collect and retain minimal amounts of data and which have a strong record of resisting unlawful demands for private data from law-enforcement and other agencies.
- **Collect the minimum amount of data needed to conduct operations and emphasize to users that any data they submit is never fully secure.** All data collected, generated and stored by humanitarian agencies is incredibly sensitive and should be given the strongest possible protection.
- **Ensure that your organization has and complies with a data protection or responsible data policy.** This should proactively address the intersecting issues of consent, data protection, organizations' ethical obligations and privacy rights, and identify measures to mitigate risks wherever possible.⁴

⁴ For examples of a rights-based, responsible data approach to dealing with these challenges, see: Oxfam, "Responsible Program Data Policy": <http://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950>; Electronic Cash Transfer Learning Action Network, "A Data Starter Kit for Humanitarian Field Staff": <http://elan.cashlearning.org/>; The Engine Room, "Médecins Sans Frontières case study": <https://www.theengineroom.org/projects/msf-responsible-data/>.

IMPLEMENTATION

- **Consider how your organization will manage and respond to the information it receives.** Messaging apps can introduce large quantities of data from many different sources. Without proper planning, this can overwhelm organizations, increase the risk that organizations fail to respect users' privacy, and frustrate local communities who find that their questions and complaints are not being acknowledged or addressed.
- **Prepare to invest considerable time and resources in verifying and validating any information received through messaging apps.** Data can only lead to better decisions and more effective communication if it is managed effectively, analysed accurately and incorporated into the organization's decision-making processes.

COLLABORATION WITH PARTNERS

- **Work with local media to tailor messages and promote humanitarian services.** Local media have enormous potential to provide people with relevant, trustworthy and timely information, particularly when people need such information urgently.
- **In urban areas, consider network connectivity as a basic urban service that needs to be restored.** Network connectivity cannot solve all problems in conflict areas or urban settings damaged by conflicts or disasters. However, restoring connectivity can quickly enable people to reconnect with their own communities and others (including humanitarian organizations), and better organize their own response.
- **Consider collaborating directly with messaging-app companies.** Research and pilot projects demonstrate the potential messaging apps have to support humanitarian initiatives. The humanitarian community should consider collectively approaching selected messaging app companies to propose practical collaborations or partnerships.



M. Henley/UNHCR

At Keleti Railway Station in Budapest, Hungary, a refugee checks his phone.

INTRODUCTION

Humanitarian organizations recognize that if their work is to be relevant and effective, it is vital to engage with and make themselves accountable to people affected by crises.

Over the last decade, studies have found that timely, actionable, trusted information - provided in the right format, in the right languages and through appropriate channels - can save lives, help people access the support they need and improve their resilience in crisis situations. Humanitarian organizations which communicate effectively with the people they seek to help are better able to respond to needs and are more accountable.

However, experience also suggests that humanitarian organizations need to pay more attention to how crisis-affected communities actually find, use and share information, and adjust their activities accordingly.⁵ This means building sustained, direct, trusted and secured connections with affected communities - but it also means constantly evaluating how the information ecosystem is changing and evolving,⁶ identifying which communications channels people use to share information, and understanding how they use them.

In this context, humanitarian organizations cannot ignore the growth of mobile messaging applications (apps) - mobile-phone-based software programmes that allow people to send text, images, audio and video to their contacts' phones over an internet connection. Over the last four years, messaging apps have become regular communication tools for people worldwide. In some cases, messaging apps are even becoming platforms where people can directly access services offered by other organizations, which range from receiving news updates and booking flights to getting a mortgage and making investments.

This report argues that, in many regions, messaging apps have become so widespread that they deserve to be considered strategically for use in humanitarian operations alongside other communication channels and platforms.

However, there are clear gaps in humanitarian organizations' understanding of the implications of introducing this new technology into crisis situations. If left unaddressed, these gaps may prevent organizations from using apps responsibly and effectively. This report identifies areas where there is a need for standards for using messaging apps in crisis situations and suggests preliminary steps towards a "responsible data" approach, which can ensure that humanitarian initiatives respect individuals' rights to consent, privacy, security and ownership.

SCOPE

This report discusses the implications of adding messaging apps to the range of communications channels currently used by humanitarian organizations, which includes face-to-face communication, print materials, SMS messaging, social media, radio and television. The report does not include detailed discussions of the uses or functionalities of these other channels, which have been discussed and researched extensively elsewhere (particularly in the context of natural disasters).

⁵ Elizabeth Scheper, Arjuna Parakrama and Smruti Patel, *Impact of the tsunami response on local and national capacities*, Tsunami Evaluation Commission, 2006: <http://www.alnap.org/initiatives/tec/thematic/capacities.aspx>; Theodora Hannides, Nicola Bailey and Dwan Kaoukji, *Voices of Refugees*, BBC Media Action, 2016: <http://www.bbc.co.uk/mediaaction/publications-and-resources/research/reports/voices-of-refugees>.

⁶ Jacobo Quintanilla, Ten lessons on communicating with communities in complex emergencies, *Humanitarian Practice Network*, 23 October 2015: <http://odihpn.org/blog/ten-lessons-on-communicating-with-communities-in-complex-emergencies/>.

The report's focus on messaging apps is not intended to imply that messaging apps are superior to existing communications channels, or that they are a "silver bullet" or universal panacea that can improve humanitarian operations in all situations. Rather, they are presented as a potential additional channel for humanitarian organizations to consider, on the basis of a strong understanding of local information ecosystems and any risks that pertain in that context.

The report places a particular emphasis on messaging-app usage in areas experiencing armed conflict or high levels of migration, but also includes an assessment of usage in humanitarian responses to natural disasters and epidemics, other development sectors and the media.

Although the vast majority of humanitarian responses and funding programmes focus on environments affected by armed conflict, the implications of engaging with communities in these settings are less well-known and documented. This is primarily due to operational complexities that include insecurity and limited physical access to local communities; disrupted energy, media and telecommunications infrastructures; communities' limited access to and experience with using digital communications technologies; and, crucially, surveillance and data protection considerations.

In today's armed conflicts, the information environment is increasingly contested and misinformation, propaganda and rumours travel more swiftly than was previously the case. In order to identify relevant approaches for communicating in these situations, humanitarian organizations need to understand more clearly how all these challenges affect their operations.

METHODOLOGY

This report is based on a survey of relevant literature, interviews with staff working in humanitarian organizations (including technology specialists, logistics officers and field workers), representatives of messaging app companies, and organizations that focus on providing technology for humanitarian organizations.

Interviewees were identified through the authors' and advisory groups' networks, and through responses to an open call publicized on mailing lists and through social media. In total, researchers spoke with more than 45 people working in Asia, Europe, sub-Saharan Africa and the Middle East.

This report, as conceptualized by the International Committee of the Red Cross (ICRC), is intended as a first step towards understanding how messaging apps are used in the humanitarian sector, particularly in conflict situations. It also aims to clarify the opportunities and challenges this technology presents and identify avenues for future research and action.

It is based on a small sample of interviewees and is not therefore comprehensive. We hope it can serve as a building block for future efforts to improve the effectiveness of humanitarian organizations and allow them to engage more effectively with the people they endeavour to protect and assist.

GLOSSARY

- **2G, 3G or 4G wireless network technology:** the G here refers to the “generation” of the underlying wireless network technology. 1G was a purely analogue network designed to carry voice and nothing else; 2G arrived in the early 1990s and transported data via a digital signal. 3G was launched in the early 2000s and offered significantly improved speeds and higher traffic capacity. 4G purely carries data and offers the highest upload and download speeds available at the time of writing.
- **API (application program interface):** A set of functions and procedures within an operating system, application or other service that enables external applications to access that service’s features or data. In some senses, this is analogous to a customer service window at a bank; just as a customer must go through a certain process of verification to withdraw or deposit money at the bank, an external application must follow the API’s rules to interact with the host service.
- **Bot or “chatbot”:** A piece of code that performs specific automated functions within an app. For example, it may provide information when a user requests it (often in natural language that makes it resemble a human operator – hence “chatbot”), request information from another user, or provide a means of linking to other web services.
- **Bulk or broadcast messaging:** The capacity to send messages or other content to a large number of people.
- **Feature phone:** A mobile phone with the capacity to make calls and send SMS messages, but with few other advanced capabilities. The term is used to distinguish these devices from more advanced “smartphones”.
- **GPRS (General Packet Radio Service):** a mobile data service that works on 2G mobile-phone connections.
- **GPS (Global Positioning System):** a satellite-based navigation system, now available in many smartphones. GPS is a specific system operated by the US government. Several other comparable satellite systems are in place and may be used by some devices in some regions of the world.
- **Information ecosystems:** complex adaptive systems that include information infrastructure, tools, media, producers, consumers, curators, and sharers. Within these systems, different types of news and information may be received from outside then passed on to others through word of mouth, key community members, telephone, the internet and other media. The term broadly refers to a loose, dynamic configuration of different sources, flows, producers, consumers, and sharers of information interacting within a defined community or space.⁷
- **Messaging app:** a mobile-phone-based software programme that allows users to send and receive information from and to their phones over an internet connection (either via Wi-Fi or mobile data networks).
- **Mesh network:** originally developed for military applications, a mesh network is a communications network, usually wireless, made up of radio nodes, consisting of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices. When one node can no longer operate for some reason, the rest of the nodes can usually still communicate with each other. In a wireless mesh network the connection is spread over dozens or even hundreds of wireless mesh nodes that “talk” to

⁷ Tara Susman-Peña, “Why Information Matters: a foundation for resilience”, Internews and the Rockefeller Foundation, 2015: www.rockefellerfoundation.org/blog/why-information-matters/.

each other to share the connection across a large area. They thus provide a decentralized alternative to traditional networks, which rely on a small number of wired access points.

- **Metadata:** In the context of the present report, this means data about the transmission of information on messaging apps. This can include the date and time at which messages or files were sent, the user's location, the identity of the person to whom data was sent, and in some cases even the phone's manufacturer and operating system. Metadata can be used to link an individual with other individuals or groups, or be combined with other datasets to infer details about an individual; studies demonstrate that it is possible to extrapolate information such as health conditions, gun ownership and even literacy from mobile phone metadata.
- **MMS (Multimedia Messaging Service):** a standard way to send messages with multimedia content to and from mobile phones over a mobile (cellular) phone network. They are sometimes referred to as picture or multimedia messages. MMS can deliver up to forty seconds of video, one image, or a slideshow of multiple images and audio.
- **SIM card (Subscriber Identity Module):** a portable memory chip used mostly in mobile phones, which holds the personal information of the account holder including the phone number, text messages, and other user data. When a user wants to change devices, they can usually remove the card from one handset and insert it into another. SIM cards have evolved over the years - their thickness has remained relatively stable (just under 1mm) but their surface area has decreased steadily, so that there are now micro- and nano-SIMs.
- **Smartphone:** A mobile phone offering advanced features, typically including a GPS sensor, the ability to access the internet over mobile-phone networks and Wi-Fi connections, and the capacity to download apps from the internet.
- **SMS (Short Message Service):** commonly referred to as "text messaging", is a service for sending short messages of up to 160 characters to mobile devices, including mobile (cellular) phones and smartphones, digital phones and web-based applications within a web browser.
- **USSD (Unstructured Supplementary Service Data):** a communication technology used to send text between a mobile phone and the service provider's computers. Sometimes referred to as "Quick Codes" or "Feature Codes", messages are up to 182 alphanumeric characters long, and can be used for prepaid callback services, information services and mobile-money services.

ACKNOWLEDGEMENTS

The ICRC, the Engine Room and Block Party would like to sincerely thank all participants in the advisory group who helped prepare this report. These participants were requested to serve in a personal capacity, based on the depth and diversity of their experience and expertise within their agencies and organizations. The advisory group participants included:

Jacobo Quintanilla, Massimo Marelli and Vincent Graf (ICRC)

Antoine Bertout and Jean-Martin Bauer (World Food Programme, WFP)

John Warnes (UN High Commissioner for Refugees, UNHCR)

Ombretta Baggio (International Federation of Red Cross and Red Crescent Societies, IFRC)

Alexandre Sicotte-Levesque (UN Office for the Coordination of Humanitarian Affairs, UNOCHA)

The ICRC, the Engine Room and Block Party would also like to thank all those who participated in the general consultative process, including: Jeff Wishnie (Digital Impact Alliance, DIAL), Aurelio Salas, Monique Crettol and Victorien Hanche (ICRC), Nathaniel Raymond (Harvard Humanitarian Initiative), Mark Latonero (Data & Society), Indra de Lanerolle (University of the Witwatersrand), participants at the Brussels Privacy Hub's Data Protection and Humanitarian Action event series, Kareem Elbayer (United Nations Office for Project Services, UNOPS), Tin Geber (The Engine Room), Jacob Korenblum and Michael Moszczynski (Souktel), Sacha Robehmed (REFUNITE), Jesco Weickert (WeltHungerLife), Heather Leson (Qatar Computing Research Institute), Sultan Haider, Sofia Fernandes, Alice Rizzo and Thomas Seropian (Internews), Chris Habib, Amanda Maher and Shabib Al-Qubati (IMMAP), Ciarán Duffy (Refugee Text), Ly Nguyen (IFRC), Marc van den Homburg, Rosalia Gitau (UNOCHA) and Trushar Barot (BBC). Any errors remain the authors' responsibility alone.

3.600.000.000



By 2018, 3.6 billion of people are expected to be using messaging apps – that's almost half of the world's population.

1. THE GLOBAL MESSAGING-APP MARKET

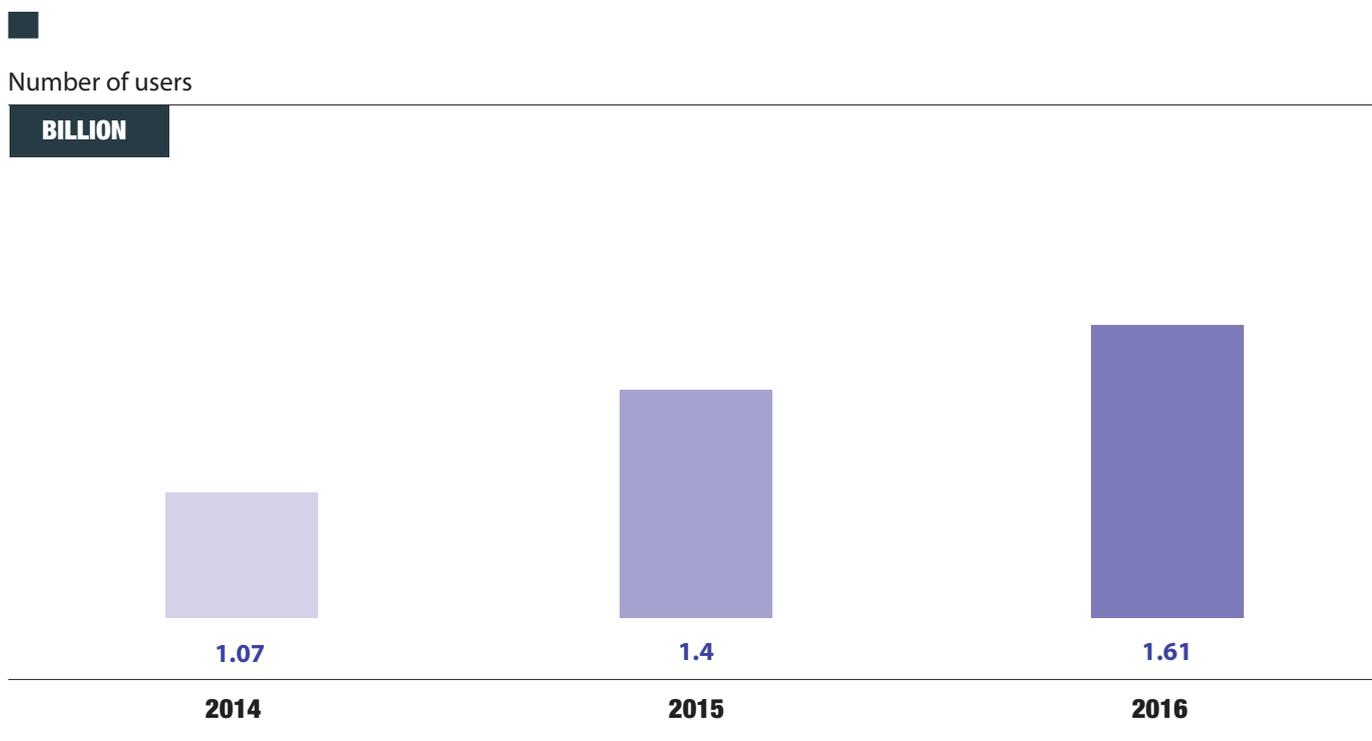
THE RISE OF MESSAGING APPS

Mobile messaging is the fastest growing digital communication phenomenon ever. Mobile messaging has been adopted more quickly, and by more people, than virtually any other digital communications technology before it. This section discusses the global growth of messaging apps, and identifies key trends in their development.

Already, more than 2.5 billion people around the world use messaging apps⁸ – a figure that is expected to grow to 3.6 billion by 2018.⁹ As of February 2016, for example, 1 billion people – nearly one in seven people on Earth – were reportedly using WhatsApp.

Some studies predict that smartphone subscriptions will almost double from 3.4 billion to 6.3 billion by 2021, meaning that most adults on earth will have access to some form of connected mobile device.¹⁰

ACTUAL MESSAGING APP USERS WORLDWIDE, 2014-2016



Note: Mobile phone users of any age who use over-the-top (OTT) messaging apps via mobile phone (browser or app) at least once per month.

Source: eMarketer, November 2015.

8 Activate, *2016 Tech and Media Outlook*, 2016: http://www.slideshare.net/ActivateInc/activate-tech-and-media-outlook-2016/2-Over_the_next_five_years.

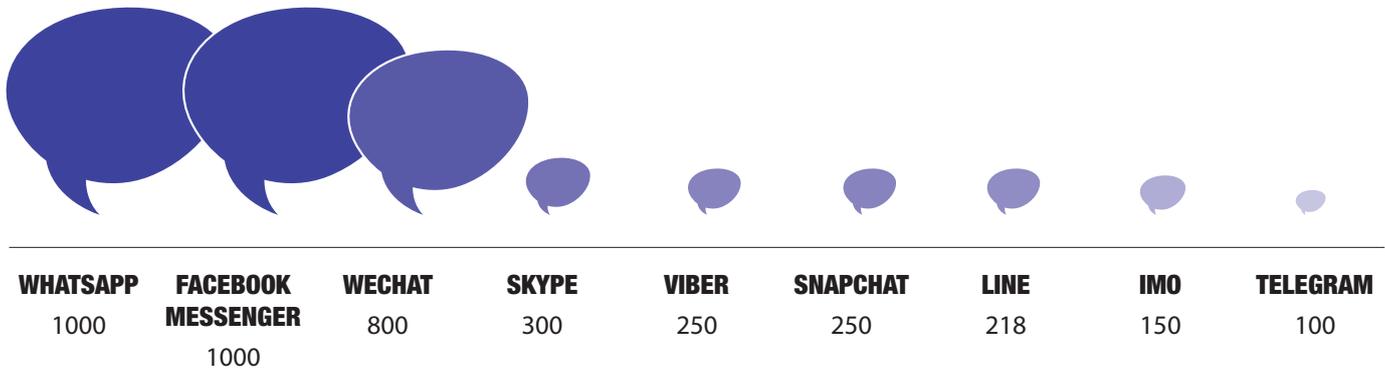
9 Activate, *The Messaging Phenomenon Has Hardly Begun*, 2016: <https://medium.com/the-activate-outlook/the-messaging-phenomenon-has-hardly-begun-cdaeaf735cb2#.n4z29ppml>.

10 *Financial Times* June 1, 2016 Daniel Thomas Smartphone use forecast to beat feature phones this year.

TOP GLOBAL CHAT APPS – 2016

Monthly Active Users

MILLION



Source: Figures reported by messaging app companies as of November 2016.

Messaging apps are not just being used widely, but intensively too. Recent data suggests that worldwide, the average user spends four hours per day using their phone, 80% of which is spent on an average of just three apps (one or more of which are frequently messaging apps).¹¹

The global ascension of messaging apps has been swift, surpassing SMS in daily message volume by 2013 and overtaking social networks in monthly active user accounts in 2015.

Initially, the shift to messaging apps was powered by simple economics. Billions of people flocked to apps that allowed them to send text messages essentially as they had previously done with SMS, but at a lower (or no) cost. As smartphone ownership and Wi-Fi and mobile-internet access has expanded, many messaging apps have evolved into multimedia hubs offering advanced features, new ways of sharing data and heightened levels of security.

Messaging apps surpassed SMS in daily message volume in 2013, and overtook social networks in monthly active user accounts in 2015.

WHAT IS A MESSAGING APP?

A messaging application (or app) is a mobile-phone-based software programme¹² that allows users to send and receive information using their phones. There are two key differences between communication through messaging apps and communication through mobile-phone networks:

- Messaging apps can transmit and receive a much wider range of data types than is possible using SMS or even its multimedia-enabled successor, MMS. In addition to voice

¹¹ GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>, p. 65; Google, "Mobile app marketing insights: how consumers really find and use your apps", 2015: <https://www.thinkwithgoogle.com/articles/mobile-app-marketing-insights.html>; Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger and Gernot Bauer, "Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage", *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, Stockholm, 30 August–2 September 2012; Chad Tossell, Philip Kortum, Clayton Shepard, Ahmad Rahmati and Lin Zhong, "An empirical analysis of smartphone personalisation: measurement and user variability", *Behaviour & Information Technology*, Vol. 31, No. 10, pp. 995-1010, 2012.

¹² Users typically need a mobile phone to access these apps, though apps such as Facebook Messenger and Slack can be used solely through a desktop computer, without the need for a mobile phone.

calls and text, messaging-app users can also send and receive files, including photos, images and (in some cases) documents;

- Unlike SMS messages, which are transmitted over conventional telephone networks, messaging apps use a Wi-Fi internet connection or a mobile data connection to transmit and receive data, including:
 - audio recordings, including voice recordings that act in the same way as a voicemail message;
 - data identifying their current location, based on their phone’s GPS sensor;
 - (in the case of some apps) live video calls; and
 - emojis (pictographic representations of emotions or specific objects).

Messaging apps have a well-documented tendency to borrow each other’s best ideas and have developed more similarities than differences over time.

Because messaging apps have a well-documented tendency to borrow each other’s best ideas, they have developed more similarities than differences over time. Messaging apps were primarily designed to allow private communication between individuals or small groups (unlike social networks such as Twitter and Facebook, which allow users to “broadcast” content to large numbers of personal contacts or followers).

However, the distinctions between social networks and messaging apps are becoming increasingly blurred, as networks such as Twitter and Instagram increasingly adopt person-to-person chat features, and messaging apps introduce the capacity for users to broadcast information to large groups.

When apps do allow users to communicate with large numbers of people simultaneously, they typically use an interface format that emulates a one-to-one chat conversation rather than the “news-feed” format seen in social networks such as Facebook, which allows users to comment on or “like” posts.¹³ (For a breakdown of some key messaging app features, see Annex).

A very short history of instant messaging

In the early 1960s, the Massachusetts Institute of Technology (MIT) Computation Center’s experimental Compatible Time Sharing System (CTSS) allowed up to 30 people to chat electronically at the same time.

In 1980, CompuServe launched CB Simulator, the first online chat platform, to allow people to communicate using text in real time via their home computers.

Instant messaging hit the mainstream in the late 1990s with the enormously popular AOL Instant Messenger (AIM).

Today’s messaging apps are direct descendants of these early instant-messenger programmes, but they have been reinvented for the mobile era.

EMERGING TRENDS: BROADCAST LISTS, ENCRYPTION AND CHATBOTS

The past year has been defined by three emerging trends within the mobile-messaging realm: changes to support communication with large groups (broadcast or bulk messaging), the addition of encryption and the increasing use of chatbots.

¹³ There are some exceptions to this. For example, the LINE messaging app offers both newsfeed and mass one-to-one push notifications.

1. BROADCAST OR BULK MESSAGING

Broadcast or bulk messaging is the ability to send a single message to a large number of users simultaneously.

In comparison with social networks such as Facebook or Twitter, broadcast messaging through messaging apps currently represents an efficient way for organizations to reach their target audiences. On social networks, users often miss or simply ignore messages from organizations, as hundreds of daily posts scroll by. Algorithms designed by social network providers also automatically decide what information users are shown, with organizations rarely being able to access information about why more users will see some posts rather than others.

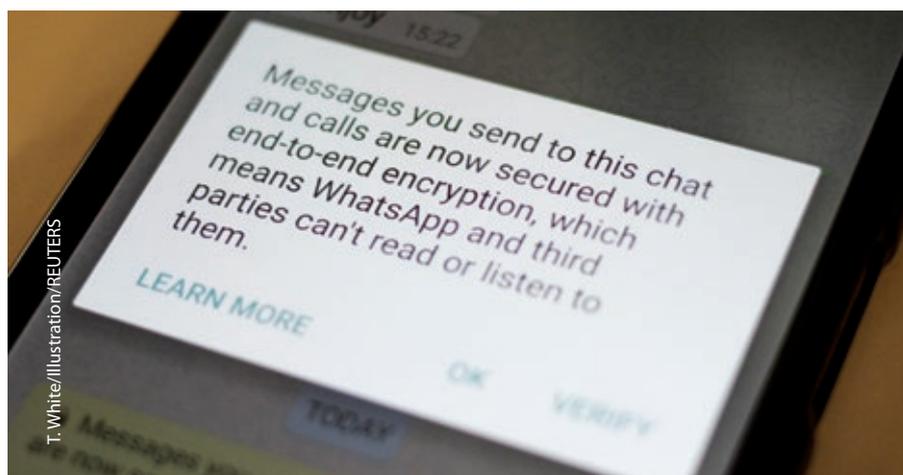
By contrast, messaging-app users are more likely to open and read the messages they receive (in communications circles, this is known as having a high “open rate”). For example, the company that produces the LINE app claims that its users read 55.8% of the notifications that businesses send to them.¹⁴ Experimental scientific research has produced similar findings.¹⁵

Trend summary

Although high message-reading rates (or “open rates”) are encouraging today, they are likely to decline in the future. Over time, chat apps are likely to limit companies’ or organizations’ ability to send bulk notifications, both as a way to safeguard user experience and as a means of gaining new revenue themselves. This has already started to happen in some parts of Asia, where businesses already market their services through messaging apps more regularly than is the case in Europe or the United States.

2. ENCRYPTION

Pavel Durov, the founder of the Telegram app, was among the first to recognize that popular messaging apps were well-suited for entertainment and casual conversation, but that none offered security strong enough to withstand hacking attempts or unwanted surveillance. His app launched in 2013 with the promise of end-to-end encryption. This means that the content of a message can be viewed only by the people sending and receiving messages, and cannot be decrypted and read by the company itself.



The extent to which messaging app companies open up the technical details of their encryption varies considerably.

14 James Cook, “Japanese Messaging App LINE Is Blowing Up, And These Stats Prove It”, Business Insider, 2015: <http://www.businessinsider.com/interview-with-jeanie-han-from-line-2015-3>.

15 Natalie (Talia) Jomini Stroud, Cynthia Peacock and Alex Curry, “Mobile News Notifications,” October 2016: <https://engagingnewsproject.org/research/mobile-news-notifications/>; Alireza Sahami Shirazi, Niels Henze, Tilman Dangler, Martin Pielot, Dominik Weber and Albrecht Schmidt, “Large-scale assessment of mobile notifications”, March 2014, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3055-3064: <http://dl.acm.org/citation.cfm?doid=2556288.2557189>.

Telegram was an immediate viral hit, especially in countries with a heightened fear of surveillance, and by early 2016 counted more than 100 million monthly active users.¹⁶ Telegram's mainstream success has since inspired other popular messaging apps to jump on the encryption bandwagon. Viber introduced end-to-end encryption in April 2016, and other platforms such as WeChat and KakaoTalk have been publicly criticized after revelations of potential collaboration with governments in response to requests for user data. Snapchat, which casual observers may assume is secure due to its disappearing messages, currently offers no end-to-end encryption.

Although a range of app companies now state that they have end-to-end encryption, they provide widely varying levels of information about the way in which this encryption is implemented.

Signal, an app developed by the non-profit organization Open Whisper Systems, was one of the first messaging apps to combine end-to-end encryption and openly auditable encryption protocols (that is, with technical details open to security professionals who may be able to discover and remedy flaws). Moxie Marlinspike, the encryption expert who founded Open Whisper Systems, subsequently worked with WhatsApp to implement the same type of encryption as used on Signal.

In mid-2016, this was rolled out by default to every WhatsApp user on any device. This development represented the most important step towards normalizing encryption as a standard for messaging apps, reaching more than one billion users in one stroke.

The same year, Facebook Messenger followed suit and implemented end-to-end encryption using the same protocol (albeit only as an opt-in feature).¹⁷ However, it is not possible for external security professionals to view and verify the way that the protocol has been implemented in either WhatsApp or Facebook Messenger. Apple also states that all the messages sent using its iMessage service are encrypted end-to-end, and has been steadfast in defending this stance, even against heavy pressure from governments. (See Annex for a breakdown of key apps' features and encryption protocols.)

Trend summary

Other top messaging apps are likely to introduce end-to-end encryption features in the near future. However, there will be considerable variation in the extent to which companies open up the technical details of their encryption, with some publicly publishing their code for inspection and validation by digital security experts, and others expecting users to accept their public statements on trust.

3. CHATBOTS

Chatbots or "bots", like instant-messaging services, have existed for decades,¹⁸ but are now finding new life due to the rise of smartphones, artificial intelligence and advances in natural-language processing.

The complexity and degree of artificial intelligence in the bots currently available through messaging apps ranges fairly widely. However, rather than engaging in free-form conversation, most bots perform simple functions such as prompting users to press suggested response buttons, or replying to users' questions with short pieces of information. These basic bots are relatively inexpensive to deploy and have no "mind of their own" that could take conversations into unpredictable places.

¹⁶ Telegram, "100,000,000 Monthly Active Users," 23 February 2016: <https://telegram.org/blog/100-million>.

¹⁷ Andy Greenberg, "Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us," *Wired*, 31 July 2016: <https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/>.

¹⁸ Early chatbots include ELIZA, developed by Joseph Weizenbaum at the MIT Artificial Intelligence Laboratory between 1964 and 1966, as well as Kenneth Colby's PARRY, designed in 1972 to emulate a paranoid schizophrenic.

As of November 2016, the messaging apps Facebook Messenger, Telegram, Skype, WeChat, LINE, Kik and Slack all supported bot technology, thus enabling users to chat with fictional characters, US supermarket chains and government entities. Bots have also been employed to obtain news updates, help learn languages or even register to vote in the US.¹⁹

To date, the only chatbot that has risen to the level of a cultural phenomenon has been Microsoft's Xiaoice. This bot has been deployed in several Chinese social-media platforms and messaging services including WeChat. Microsoft claims that over 40 million people²⁰ have installed the bot, with users interacting with it an average of 60 times per month.²¹ In a 2015 New York Times feature on Xiaoice, users described the bot as a "friend" that could remember personal stories shared with it and reference these in future interactions.²²

Ironically, Microsoft's Tay – Xiaoice's sister product for the US market, which was programmed to learn from its interactions with users – became a public-relations disaster after a group of online pranksters trained it to make offensive and racist comments. With the Tay experience in mind, many businesses and organizations are unlikely to opt for high-intelligence chatbots until the technology is perfected.²³

Trend summary

Despite mixed reviews for the first generation of messaging-app bots, which users often described as glitchy or limited in their ability to understand users' intent, other major messaging apps are expected to support similar technology by the end of 2016. For the foreseeable future, the landscape is likely to be dominated by simple, functional bots that stick reliably to a pre-defined script.

ACCESS TO MESSAGING APPS: AFFORDABILITY, CONNECTIVITY, GENDER AND AGE

AFFORDABILITY

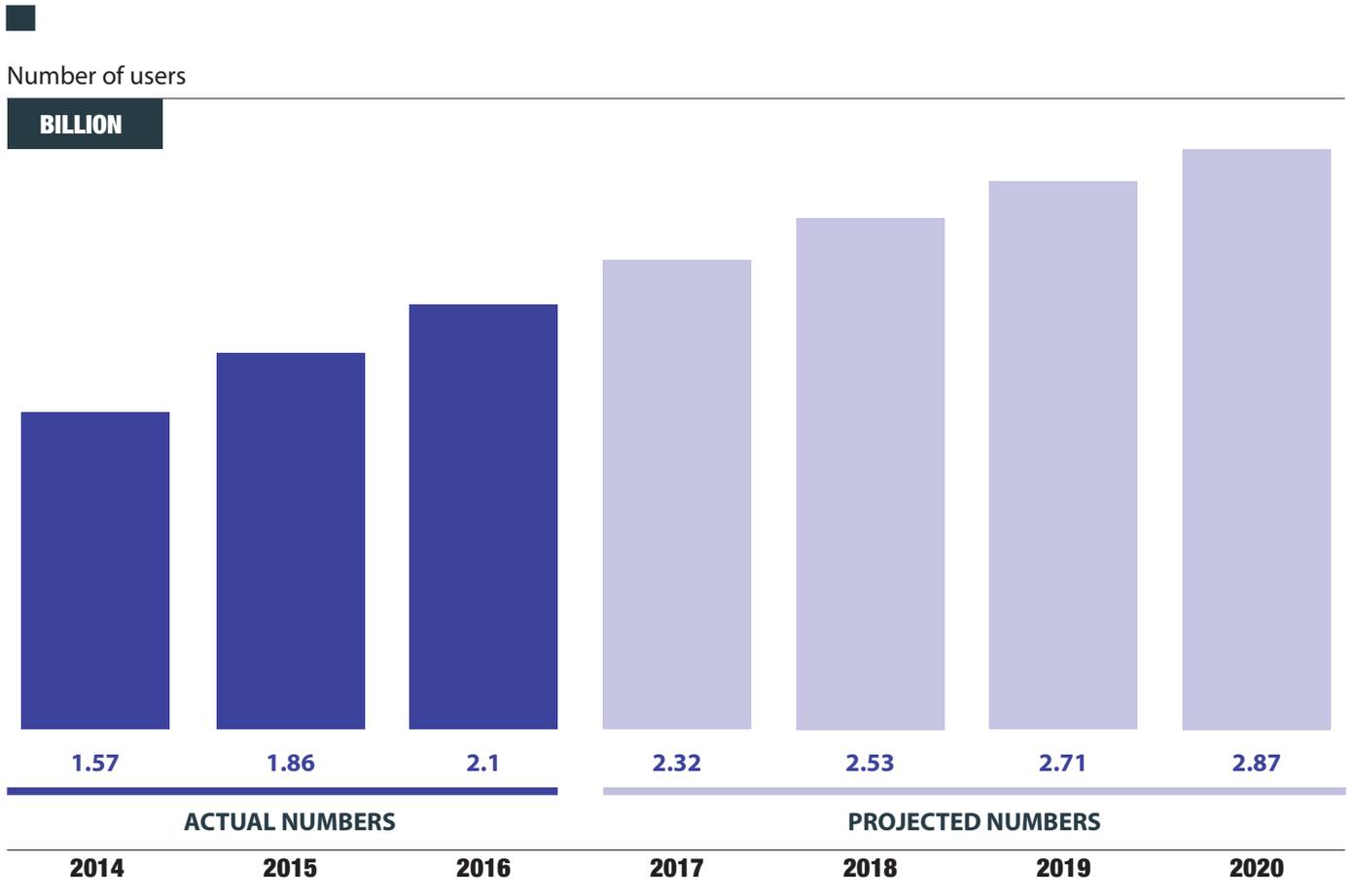
Most messaging apps are only usable on smartphones, although some basic feature phones can access mobile data through a GPRS²⁴ connection and are sold with versions of WhatsApp and Facebook pre-installed.

Smartphones are typically more expensive than feature phones (with prices usually starting at around 100 US dollars), although lower-priced smartphones are becoming increasingly available around the world.²⁵ The use of messaging apps is still associated with a clear upfront cost for the user, thereby limiting the number of people who can access them.

-
- 19 Drew Olanoff, "Go Chat With Miss Piggy On Facebook Messenger", 7 December 2015: <https://techcrunch.com/2015/12/07/go-chat-with-miss-piggy-on-facebook-messenger/>; John Brandon, "Whole Foods just launched a Messenger chatbot for finding recipes with emojis", 16 July 2016: <http://venturebeat.com/2016/07/12/whole-foods-just-launched-a-messenger-chatbot-for-finding-recipes-with-emojis/>; Jessica Davies, "One month in: What CNN has learned from Facebook Messenger bots", 31 May 2016: <http://digiday.com/publishers/one-month-cnn-learned-facebook-messenger-bots/>; Pavithra Mohan, "This Chatbot Will Register You To Vote By Text, So Now You Have No Excuse", *Fast Company*, 2016: <https://www.fastcompany.com/3063969/mind-and-machine/this-chatbot-will-register-you-to-vote-by-text-so-now-you-have-no-excuse>.
- 20 Matt Weinberger, "Microsoft Taught A Computer To "Make Chit Chat," – and Now 40 Million People Love It", *Business Insider*, 2016: <http://www.businessinsider.com/microsoft-research-peter-lee-xiaoice-tay-2016-8>.
- 21 Bing, "Meet Xiaoice, Cortana's Little Sister", 5 September 2015: <https://blogs.bing.com/search/2014/09/05/meet-xiaoice-cortanas-little-sister/>.
- 22 John Markoff and Paul Mozur, "For Sympathetic Ear, More Chinese Turn To Smartphone Program", *The New York Times*, 4 August 2015: <http://www.nytimes.com/2015/08/04/science/for-sympathetic-ear-more-chinese-turn-to-smartphone-program.html>.
- 23 Ted Livingstone, "Bots are Better Without Conversation", *Medium*, 2016: <https://medium.com/@tedlivingstone/bots-are-better-without-conversation-fcf9e7634fc4#ve27kpf5e>.
- 24 General Packet Radio Service (GPRS) is a mobile data service that works on 2G mobile-phone connections.
- 25 See Mary Meeker's reports, which include information on smartphone pricing worldwide: <http://www.cnet.com/news/mary-meeker-sees-messaging-taking-over-mobile/#!>; Sibusiso Tshabalala, "Africa's smartphone market is on the rise as affordable handsets spur growth", 13 July 2015: <http://qz.com/451844/africas-smartphone-market-is-on-the-rise-as-affordable-handsets-spur-growth/>.

Rates of smartphone adoption are growing rapidly in all countries, with penetration rates currently standing at roughly one-third of adults in developing markets and 68% in advanced economies.²⁶ Smartphone penetration rates are expected to rise considerably faster than incomes in many developing countries, reaching 60% to 70% in some countries by 2020.²⁷

NUMBER OF SMARTPHONE USERS GLOBALLY (CURRENT AND PROJECTED), 2014-2020



Note: Individuals of any age who own at least one smartphone and use smartphones at least once per month.

Source: eMarketer, April 2016.

However, access to smartphones varies significantly depending on geography. Pew Research reports that as of spring 2015, 43% of adults worldwide owned smartphones. However, those numbers varied greatly from country to country, reaching rates as high as 88% in South Korea, and as low as 4% in Ethiopia and Uganda.²⁸

In every country, higher levels of education and income are reliably associated with a significantly increased likelihood of smartphone ownership. As mentioned above, the number of smartphone subscriptions is expected almost to double by 2021.²⁹

26 See: <https://www.gsmainelligence.com/> for up-to-date figures.

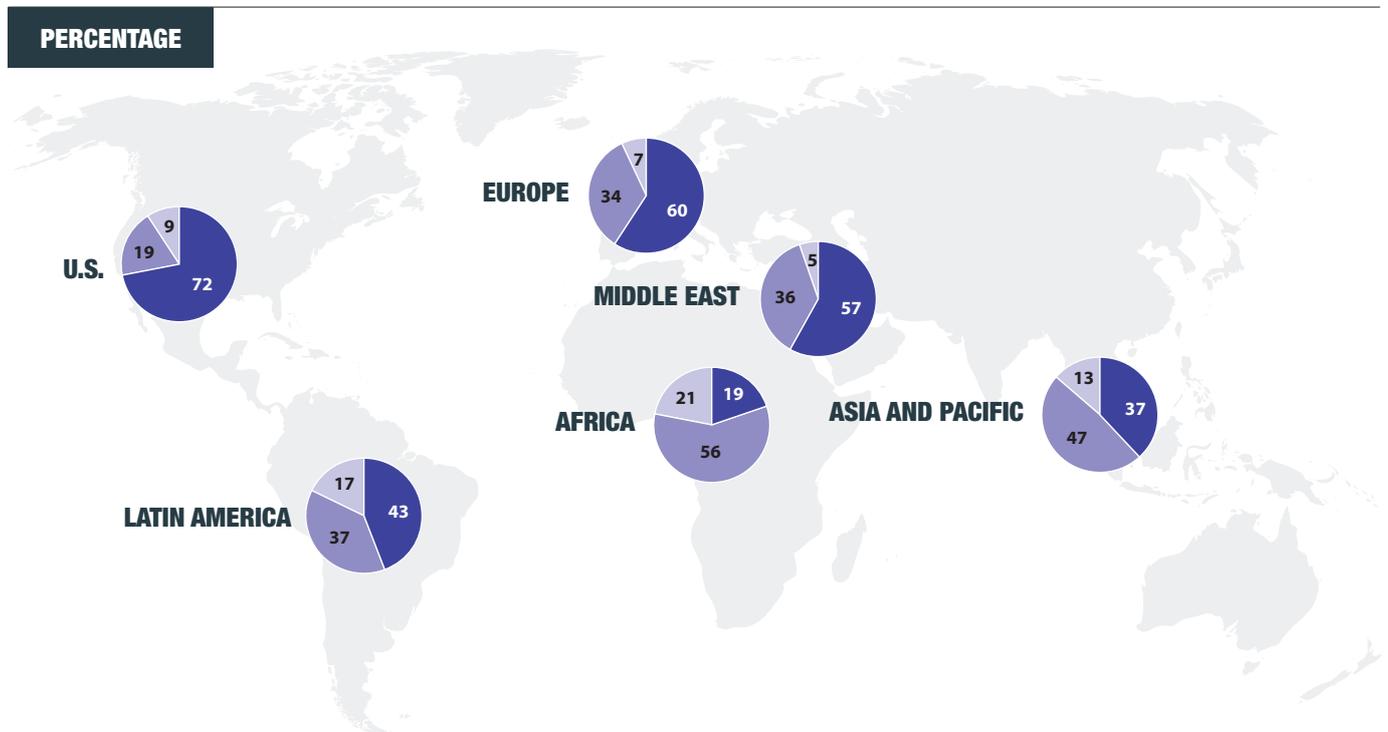
27 GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>, p. 21.

28 Jacob Poushter, "Smartphone Ownership and Internet Usage Continues To Climb In Emerging Economies", *Pew Research Center*, 2016: <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.

29 Financial Times, 1 June 2016, Smartphone use forecast to beat feature phones this year.

SMARTPHONES ARE MORE COMMON IN THE U.S., EUROPE AND THE MIDDLE EAST

● Smartphone ● Cellphone but NOT smartphone ● No cellphone



Note: Percentages based on total sample. Russia and Ukraine not included in Europe median.

Source: Spring 2015 Global Attitudes survey, Pew Research Center.

UNHCR research indicates that refugees are around 50% less likely to own a smartphone than the global population as a whole, and that 29% of refugee households have no phone at all.³⁰

Anecdotally, interviewees working in East Africa and the Middle East said they had seen increasing rates of smartphone ownership among refugees and other low-income groups.³¹ As factors behind this trend, many cited the falling cost of phones that use the Android operating system – as opposed to Apple’s iOS – and the availability of inexpensive second- or third-hand smartphones.

Other studies have found that smartphones outnumber feature phones by two to one in some refugee camps in the Middle East,³² and that refugees also frequently share phones.³³ This ratio may continue to rise in some areas. A recent UNHCR survey of almost 2,000 refugees in Lebanon found that the proportion of respondents with access to a mobile phone had risen to 92%, up from 54% when the same population had lived in Syria. The proportion with access to the internet had risen to 75% from 10%.³⁴

30 UNHCR, *Connecting Refugees: How Internet and Mobile Connectivity can Improve Refugee Wellbeing and Transform Humanitarian Action*, 2016: <http://www.unhcr.org/en-us/connectivity-for-refugees.html>. UNHCR, *Connecting Refugees*, <http://www.unhcr.org/en-us/connectivity-for-refugees.html>.

31 Ben Mason and Dennis Buchman, *ICT4Refugees: A report on the emerging landscape of digital responses to the refugee crisis*, 2016: https://regasus.de/online/datastore?epk=74D5roYc&file=image_8_en; Sacha Robehmed, “Getting online in the Kurdistan region of Iraq”, 6 May 2016: <https://refunite.org/getting-online-in-the-kurdistan-region-of-iraq/>.

32 REACH and UNHCR, *Mass Communications Assessment in Azraq Camp (December 2015)*, April 2016: <http://data2.unhcr.org/en/documents/details/43703>.

33 Linda Leung, “Phoning home”, *Forced Migration Review*, 38, October 2011: <http://www.fmreview.org/technology/leung.html>.

34 Matthew Saltmarsh, “Facebook group helps Syrian refugees navigate life in Lebanon”, 13 July 2016: <http://www.unhcr.org/en-us/news/latest/2016/7/577e16064/facebook-group-helps-syrian-refugees-navigate-life-lebanon.html>.

However, this trend is not uniform. In particular, refugees living in urban areas are significantly more likely than those in rural areas to be using smartphones. According to the most recent UNHCR overview, 68% of refugee households in urban locations had an internet-capable mobile phone in 2015, compared to just 22% of those in rural areas.³⁵

The cost of data packages enabling mobile phones to access the internet is another restricting factor. For example, research by FireChat indicates that around one-third of smartphone users in Manila, Mumbai and Mexico City have periods every month where they cannot use messaging apps because they have spent all their mobile data allowance.³⁶

However, the cost of mobile data has been forecast to fall worldwide in the coming years.³⁷ Anecdotal evidence suggests some groups such as Syrian refugees often regard paying for data as a top priority, and that individuals find the overall cost of sending messages using a smartphone with a data plan to be lower than that of sending large numbers of SMS messages, even with a lower-cost feature phone.

Additionally, some organizations provide free Wi-Fi internet hotspots in sites with high numbers of refugees, or offer reduced-price data packages.³⁸

CONNECTIVITY

Because messaging apps rely on transmitting data over mobile-data connections or Wi-Fi networks, they will not work in areas lacking these types of connectivity. Many such areas also lack reliable electricity. The most recent data indicates that as of October 2016, mobile-internet penetration rates in sub-Saharan Africa had reached 26%, as compared to 34% in the Middle East and North Africa and 39% in developing countries in Asia.³⁹ UNHCR research found that 90% of refugees living in urban areas could access 3G networks in 2015 – a share similar to that within the global urban population as a whole. However, only 17% of refugees in rural areas could access 3G networks, while 20% of rural refugees had no mobile-phone coverage at all.⁴⁰

Some organizations are actively working to increase internet provision in sites such as refugee camps, but coverage, connection speeds and reliability vary dramatically between locations.⁴¹

Some organizations are actively working to increase internet provision in sites such as refugee camps, but coverage, connection speeds and reliability vary dramatically between locations.

35 UNHCR, *Connecting Refugees*, 2016: <http://www.unhcr.org/en-us/connectivity-for-refugees.html>.

36 Unpublished FireChat research, February 2016, based on a sample of 200 smartphone users in Mumbai, 200 in Mexico City and 200 in Manila.

37 GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>, p. 21.

38 Sacha Robehmed, "Getting online in the Kurdistan region of Iraq", 6 May 2016: <https://refunite.org/getting-online-in-the-kurdistan-region-of-iraq/>; Sacha Robehmed, "Syrians with smartphones", 11 February 2016: <https://refunite.org/syrians-with-smartphones-where-does-refunite-fit-in/>.

39 GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>.

40 UNHCR, *Connecting Refugees*, 2016: <http://www.unhcr.org/en-us/connectivity-for-refugees.html>.

41 Alyssa Cogan, "How technology is affecting the refugee crisis", 9 June 2016: <https://www.mercycorps.org/articles/afghanistan-iraq-syria/how-technology-affecting-refugee-crisis>; Jacobo Quintanilla, "Ten lessons on communicating with communities in complex emergencies", 23 October 2015: <http://odihpn.org/blog/ten-lessons-on-communicating-with-communities-in-complex-emergencies>; <http://www.mercycorps.org/articles/syria/how-technology-affecting-refugee-crisis>; Ben Mason and Dennis Buchman, *ICT4Refugees*, 2016: https://regasus.de/online/datastore?epk=74D5roYc&file=image_8_en.



Burundian refugees line up behind an ICRC staff member for the free phone-charging service in the Mahama refugee camp in Rwanda.

Finally, the presence of network coverage alone is not enough to ensure that people actually go online. Recent research suggests that 35% of the world's population lives in an area with 3G or 4G network coverage but has never used the mobile internet, due to limited digital literacy, affordability concerns, or a lack of awareness and relevant local content.⁴²

Anecdotal evidence supports these findings, with this report's interviewees frequently noting that many people in conflict-affected areas either lack access to or do not use internet-enabled smartphones. Crucially, all these services require strong and fundamentally intact energy and communications infrastructure – a particular challenge in situations affected by armed conflict, where energy, telecommunications and media infrastructure is often severely disrupted or deliberately targeted by parties to the conflict.⁴³ In some countries affected by conflict, the authorities cite security concerns to limit access to communications networks at certain periods of time.

The presence of network coverage alone is not enough to ensure that people actually go online. Limited digital literacy, affordability concerns, lack of awareness and relevant local content are key factors.

GENDER

Men report smartphone ownership at markedly higher rates than women in many countries, as indicated in the chart below.

Interviewees working in crisis-affected areas reinforced this point, with some emphasizing that this divide is even wider among vulnerable groups in such areas.

Others reported that even in situations in which women own or have access to phones, male members of their household often restrict or control their phone usage.

Men report smartphone ownership at markedly higher rates than women in many countries, particularly in crisis-affected areas.

⁴² GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>, p. 38.

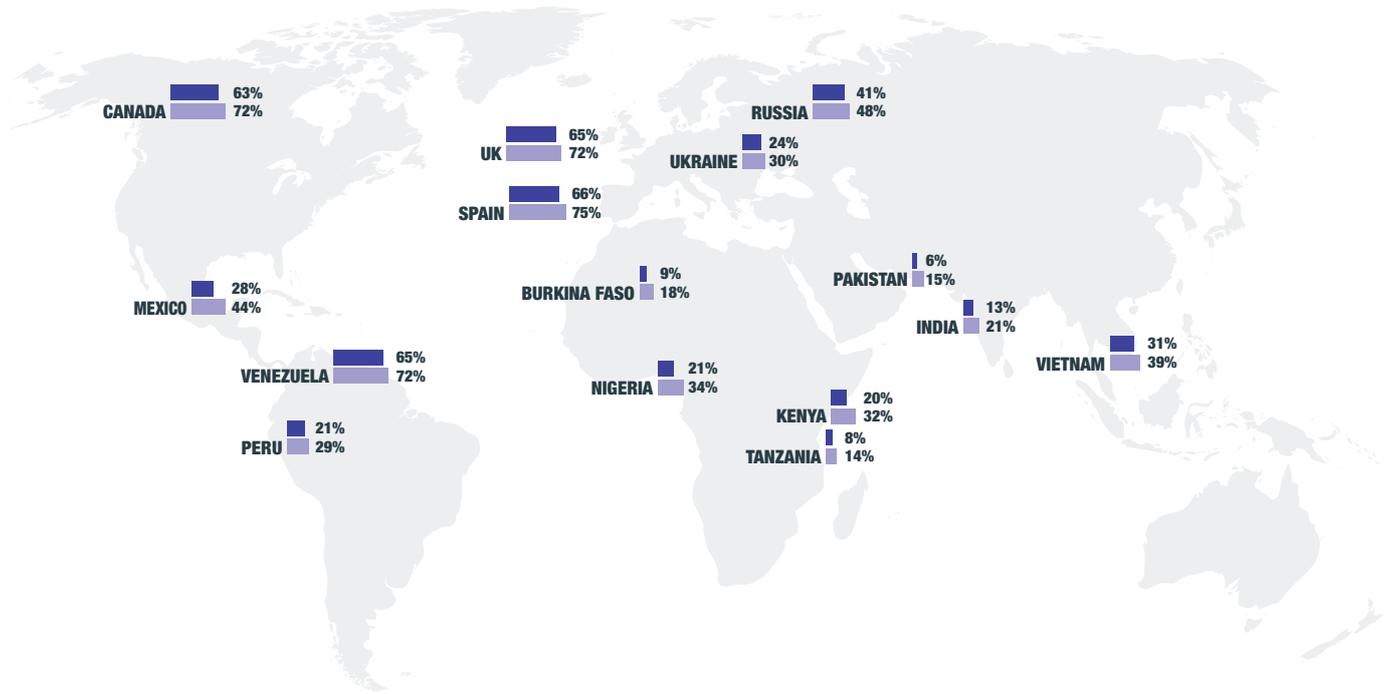
⁴³ See, for example, in Afghanistan: Mohammad Humayon Zahid, "Cell phone towers destroyed in Farah", *Pajhwok News*, 6 May 2013: <http://www.pajhwok.com/en/2013/05/06/cell-phone-towers-destroyed-farah>.

GENDER DIVIDE IN MANY NATIONS ON SMARTPHONE OWNERSHIP



Smartphone owners: ● Women ● Men

PERCENTAGE



Note: Percentages based on total sample. Only statistically significant differences shown.

Source: Spring 2015 Global Attitudes survey, Pew Research Center.

Several studies confirm that this can significantly limit the extent to which women participate in technology-based communication initiatives, highlighting the importance of including alternative communication mechanisms that may be easier and safer for women to access.⁴⁴

⁴⁴ See, for example, Social Impact Lab Foundation, INTRAC and World Vision UK, *Low-cost mobile-enabled feedback mechanisms for solicited and unsolicited feedback*, 2016: <http://cdn.worldvision.org.uk/files/3514/6056/3545/SIMLab1.pdf>.

AGE

As may be expected, there is a significant generational divide in smartphone ownership: people aged 18–28 often purchase smartphones at rates several times higher than those of older consumers. In Ukraine, for example, 56% of 18- to 34-year-olds have smartphones compared to 13% of those over 35. In the Palestinian Territories, 73% of 18- to 34-year-olds and 39% of adults over 35 own smartphones.⁴⁵

Research from October 2016 also indicates that globally, 18- to 34-year-olds now use messaging apps with greater frequency than they do SMS or voice calls – a trend that is reversed among those over 35.⁴⁶

Information regarding the age of people affected by conflict or displacement is limited, though some of the studies and anecdotal evidence provided by interviewees for this report indicate that older, low-income people are much less likely than their younger, wealthier peers to own and use smartphones.⁴⁷

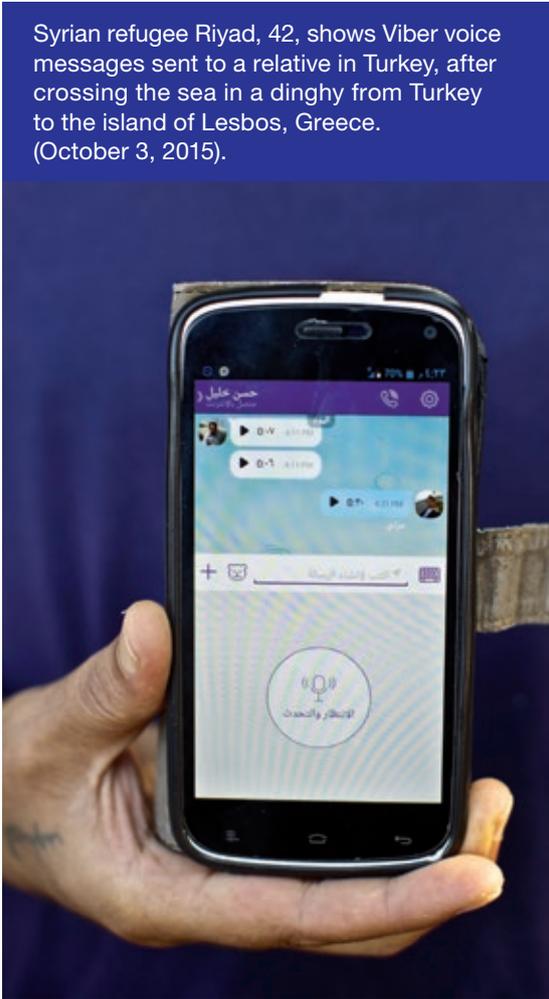
Globally, 18- to 34-year-olds now use messaging apps with greater frequency than they do SMS or voice calls.

⁴⁵ Jacob Poushter, "Smartphone Ownership and Internet Usage Continues To Climb In Emerging Economies", *Pew Research Center*, 2016: <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.

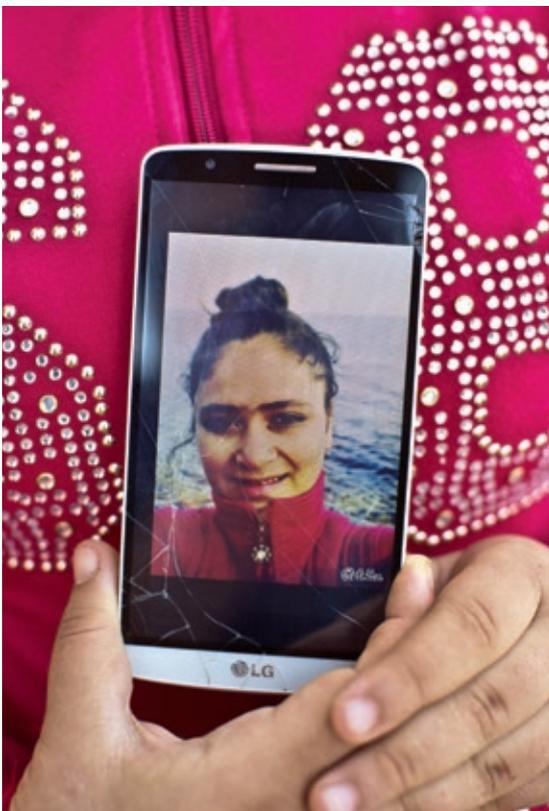
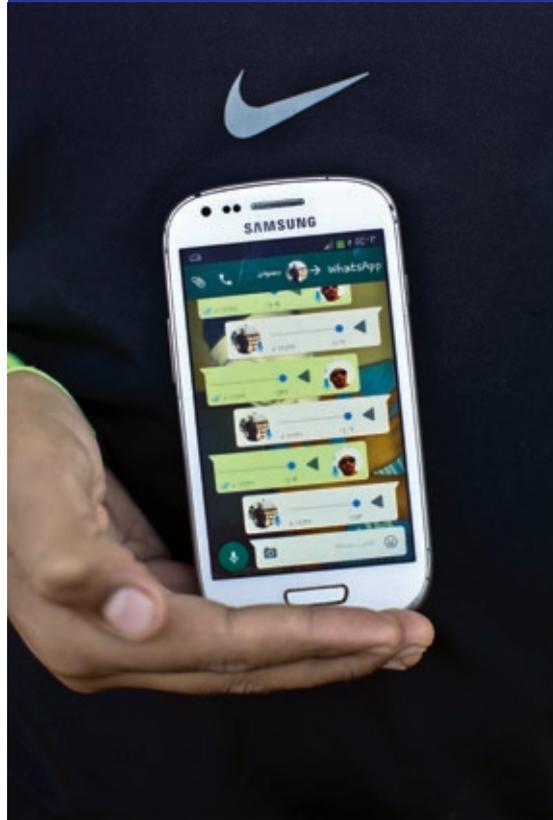
⁴⁶ GSMA, *Global Mobile Trends*, October 2016: <http://www.gsma.com/globalmobiletrends/>.

⁴⁷ REACH and UNHCR, *Mass Communications Assessment in Azraq Camp* (December 2015), April 2016: <http://data2.unhcr.org/en/documents/details/43703>.

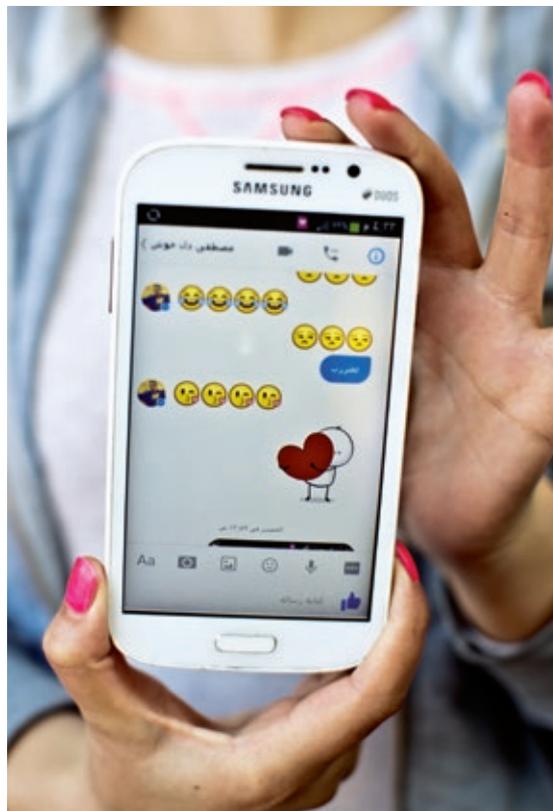
Syrian refugee Riyadh, 42, shows Viber voice messages sent to a relative in Turkey, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece. (October 3, 2015).



A Syrian refugee boy, 14, shows WhatsApp voice messages sent to his father in Germany, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 3, 2015).



Syrian refugee Lailav Khalil, 15, shows a selfie on her phone, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 3, 2015).



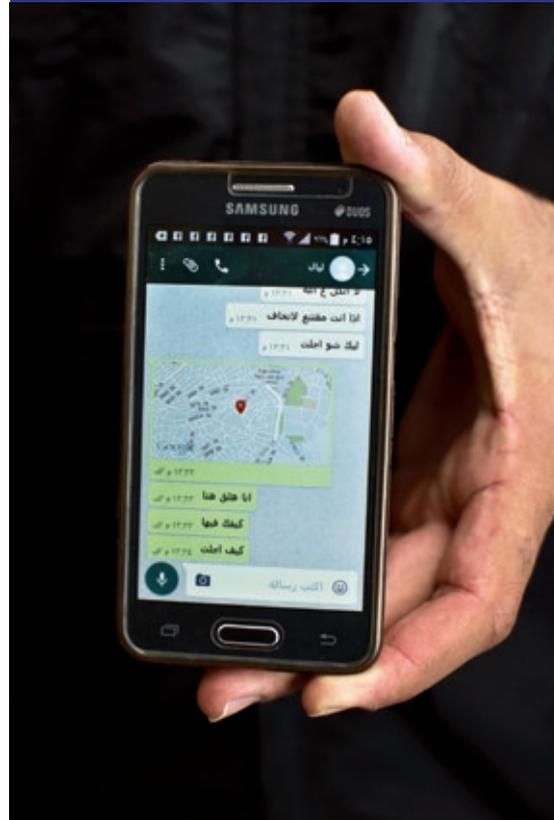
A Syrian refugee woman, 20, shows Facebook Messenger exchanges with her fiancée, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 3, 2015).

All photos on this page: M. Muheisen/AP/Keystone

A migrant shows a selfie of himself and friends somewhere in the Balkans, after he spent the night in a shelter near Graz, Austria (September 22, 2015).



Syrian refugee Firas Alhadi, 35, shows WhatsApp messages to and from his wife in Syria, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 2, 2015).



Iraqi refugee Khubyb Luai, 29, shows his phone with a picture of himself and his family, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 3, 2015).



A Syrian refugee shows his phone, after crossing the sea in a dinghy from Turkey to the island of Lesbos, Greece (October 2, 2015).



K. Abdulilah/REUTERS

A woman uses her mobile phone to take photos in Yemen's capital Sana'a, 14 July 2015.

2. HOW ARE PEOPLE USING MESSAGING APPS IN SITUATIONS OF CRISIS OR ARMED CONFLICT?

OVERVIEW: VARIATION AND FRAGMENTATION

This section sets out some of the available evidence regarding the ways messaging apps are used by refugees, migrants, internally displaced people (IDPs) and other groups of people affected by armed conflict.

- **Very little high-quality, disaggregated data is available regarding which apps people are using and how they are being used.** Some data is available on smartphone and messaging app usage in areas affected by conflict or violence. However, there is limited data specifically on usage by refugees, with disaggregated data broken down by age or gender being particularly rare. This seems to indicate that questions on access to and use of mobile telephony are not systematically included in humanitarian needs assessments.
- **Even minor changes between regions appear to significantly influence the type of apps used and the extent of their usage.** While a small number of apps are used worldwide (if to varying extents), many apps are popular only in a small number of countries due to localized factors including cost, security considerations and the availability of specific functionalities such as security features.⁴⁸ Variability in app usage is also evident when comparing groups of IDPs and refugees; for example, one interviewee working in Iraq noted that the range of internet connectivity options (and thereby app usage patterns) differed significantly between refugee and IDP camps that were only 30 minutes' drive apart.⁴⁹
- **App usage patterns can change dramatically over short periods of time.** This factor is exacerbated by the speed at which apps are developing and adding new features. Even apps that are widely used in certain countries can be overtaken rapidly by competitors, particularly if the original market leader becomes perceived as being insecure or subject to surveillance by the authorities. Telegram and Signal, for example, regularly report rises in downloads in specific countries in response to fears of increased government surveillance.⁵⁰ In the Middle East, for example, several interviewees described seeing one app replace a previously popular competitor within the space of a year.
- **In order to engage with local communities effectively, detailed and regular research aimed at understanding the local information ecosystem is crucial.** This includes systematically incorporating questions on access to and use of mobile telephony into humanitarian needs assessments. This was repeatedly emphasized by this report's interviewees, as well as in evaluations of past humanitarian initiatives. Focus groups, user testing and surveys can help guide decisions on how people in a particular situation are likely to respond to the use of a particular communications channel.⁵¹

For all these reasons, this report does not make broad generalizations about app usage in conflict or violent situations. Organizations should conduct a thorough context analysis of usage patterns, market environments and community factors before deciding to use any messaging app. SIMLab provide a framework for conducting such context analysis in projects that include technology, which discusses these issues in more detail.⁵²

48 Trushar Barot and Eytan Oren, *Guide to Chat Apps*, Tow Center, 2015: <http://towcenter.org/research/guide-to-chat-apps/>.

49 Sacha Robehmed, "Getting online in the Kurdistan region of Iraq", 6 May 2016: <https://refunite.org/getting-online-in-the-kurdistan-region-of-iraq/>.

50 See, for example, Dominique St John, "South Koreans boycott messaging app Kakao Talk en masse for Telegram", 8 October 2014: <http://www.dw.com/en/south-koreans-boycott-messaging-app-kakao-talk-en-masse-for-telegram/a-17981983>; Joshua Kopstein, "Signal Downloads Spiked After Election Results", 12 November 2016: <http://motherboard.vice.com/read/signal-downloads-spiked-after-election-results>.

51 Humanitarian Technologies Project, 2015: <http://humanitariantechnologies.net/lessons-from-haiyan/>; Jacobo Quintanilla, "Ten lessons on communicating with communities in complex emergencies", 23 October 2015: <http://odihpn.org/blog/ten-lessons-on-communicating-with-communities-in-complex-emergencies>; UNICEF, "Wat bother u d most abt Ebola: the design of UReport Liberia", 2014: <http://www.unicefstories.org/2014/10/29/wat-bother-u-d-most-abt-ebola-the-design-of-u-report-liberia/>.

52 Kelly Church and Laura Walker McDonald, "Announcing: SIMLab's framework for context analysis of inclusive technology in social change projects", August 2016: <http://simlab.org/resources/contextanalysis>.

Certain apps boast gigantic user bases, but tend to dominate a fairly limited set of countries or continents. Others, like **WhatsApp** and **Facebook Messenger**, are truly global and have a genuine population of users in almost every market. That said, it would be a mistake to assume that the market will consolidate and there will be an eventual “winner”.

On the contrary, there is ample evidence that a number of messaging apps can coexist and succeed – in part because individual users often use multiple messaging platforms to talk to different people or to share different types of content.⁵³

In 2014 and 2015, most major apps raced to outmanoeuvre competitors and conquer new markets, but several have recently retreated to defend core geographic strongholds.

WeChat, for example, has a 93% penetration rate within China’s major cities, but has struggled to make inroads in North America.⁵⁴ Its parent company **Tencent** has since curtailed attempts to expand in the US market directly, opting instead to invest in messaging apps like **Kik** that are popular with North American teenagers.

LINE continues to dominate in Japan, Thailand, Taiwan and Indonesia, and has had notable successes in countries such as Spain, but has failed to dethrone popular messaging apps in North America.

Viber is also building on successes in key markets including Russia, Ukraine and Australia, while pulling back somewhat on other expansion efforts.

Snapchat is arguably emerging as a truly global force and could join the ranks of ubiquitous messaging platforms such as WhatsApp and Facebook Messenger.

Relative newcomer **imo** has also reached the top ranks of app-download charts in countries such as Yemen, Liberia, India, Pakistan, Sri Lanka, Nigeria, Zimbabwe and Iran.

Data on usage patterns in countries affected by armed conflict is limited. However, the table below sets out available information on smartphone and app usage in several key countries affected (or recently affected) by armed conflicts or situations of violence:

It would be a mistake to assume that the messaging app market will consolidate and there will be an eventual “winner”. On the contrary, there is ample evidence that a number of messaging apps can coexist and succeed.

53 Madeline E. Smith, “‘They’re blowing up my phone’: Group Messaging Practices Among Adolescents”; Siu-Tsen Shen, 2016, “People and their smartphones – mapping mobile interaction in the modern connected world”, *Engineering Computations*, Vol. 33 Iss 6 pp. 1642 - 1658: <http://dx.doi.org/10.1108/EC-06-2015-0153>.

54 eMarketer, “In China, WeChat Is Widely Used,” 1 December 2015: <http://www.emarketer.com/Article/China-WeChat-Widely-Used/1013285>.

Country	Top three messaging apps ⁵⁵	Smartphone penetration rate	Other popular messaging apps ⁵⁵	Share of mobile users who access social media on their phone	Social media users that are on WhatsApp
Yemen	WhatsApp, imo, Messenger	Not available	WeChat, Telegram, Snapchat, LINE, Tango, Viber	5%	92%
Ukraine	Viber, Skype, WhatsApp	27%	Messenger, Telegram, LINE	27%	n/a
Syria	WhatsApp	23%	Not available	Not available	98%
Iraq	Messenger, Viber, WhatsApp	17%	Telegram, imo, Truecaller	26%	77%
Afghanistan	Not available ⁵⁶	Not available	Not available	5%	Not available
Palestinian Territories	Not available ⁵⁷	57%	Not available	32%	47%
Chad	Not available	Not available	Not available	1%	Not available
Niger	Messenger, imo, Viber	Not available	Skype, Snapchat	1%	Not available
South Sudan	Not available	26%	Not available	1%	Not available
Somalia	Not available	Not available	Not available	4%	Not available

Sources: Pew Research Center⁵⁸, GSMA⁵⁹, We Are Social⁶⁰, TNS Arab Social Media Report⁶¹.

The following section summarizes findings from available research on the use of messaging apps in situations of armed conflict or among refugees and migrants.

WHICH APPS ARE PEOPLE USING?

Most publicly available evidence on messaging-app usage in conflict-affected areas focuses on defined groups operating in specific regions, typically with small sample sizes. Such information frequently takes the form of blogs by organizations and short articles in the media, as well as academic studies and information needs assessments by humanitarian organizations.

55 Based on recent iOS and Android top free apps charts, as reported by App Annie and iOSAppStats.com.

56 Other research indicates that Facebook Messenger and Viber are the most popular apps among some user groups: <http://dai-global-digital.com/consumer-insights-afghanistan-how-young-women-are-using-tech.html>.

57 According to research focused on specific user groups, Facebook Messenger and WhatsApp are the most popular apps in some scenarios: <http://dai-global-digital.com/consumer-insights-palestine-e-governance-readiness.html>.

58 Jacob Poushter, "Smartphone Ownership and Internet Usage Continues To Climb In Emerging Economies", *Pew Research Center*, 2016: <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.

59 GSMA, *The Mobile Economy - Arab States*, 2015: <http://www.gsma.com/mobileeconomy/>.

60 We Are Social, "2016 Digital Yearbook", 26 January 2016: <http://www.slideshare.net/wearesocialsg/2016-digital-yearbook>.

61 <http://www.dmc.ae/wp-content/uploads/2016/05/ArabSocialMediaReport-2015.pdf>.



A Honduran migrant in Tapachula, Mexico, calls relatives in the U.S. via WhatsApp, 17 December, 2016.

Most evidence to date has been focused on the Middle East, and particularly on Syrian refugees. There is a notable lack of research on refugees and IDPs in all other regions.

In the Middle East, media reports and interviewees have regularly suggested that the most popular apps were Facebook Messenger, WhatsApp and Viber,⁶² with anecdotal evidence and personal observations suggesting that other apps are significantly more popular in other regions.

Some reports have suggested that refugees use different apps for specific purposes: using Viber to talk to their family while engaging with local authorities on WhatsApp.⁶³

62 Alyssa Cogan, "How technology is affecting the refugee crisis", 9 June 2016: <https://www.mercycorps.org/articles/afghanistan-iraq-syria/how-technology-affecting-refugee-crisis>; Katie Drew, "The European Refugee crisis: 10 Communications with Communities challenges", 6 January 2016: <http://innovation.unhcr.org/the-european-refugee-crisis-10-communications-with-communities-challenges/>; Naline Malla, Ayla Jean Yackley, Marton Dunai and Aleksandar Vasovic, "For many refugees, journey to Europe begins on Facebook", 2 September 2015: <http://www.ekathimerini.com/201112/article/ekathimerini/community/for-many-refugees-journey-to-europe-begins-on-facebook>; Bassam Sebti, "4 smartphone tools Syrian refugees use to arrive in Europe safely", 17 February 2016: <http://blogs.worldbank.org/voices/4-smartphone-tools-Syrian-refugees-use-to-arrive-in-Europe-safely>; Bram Frouws et al, *Getting to Europe the WhatsApp Way*, Danish Refugee Council, 2016: <http://www.regionalmms.org/index.php/10-briefing>.

63 Syrene Assir, "Syrians use Facebook to plan, document journey to Europe," 19 August 2015: <https://www.yahoo.com/news/syrians-facebook-plan-document-journey-europe-074314678.html?ref=gs>.

The table below summarizes a selection of the available findings related to people in situations of conflict or mass migration:

Location	Sample	Summary of findings
Multiple refugee sites in the Middle East	Survey responses from 95 UNHCR staff members representing 44 countries, 2016	Around 85% of staff respondents said refugees at the site where they worked used Facebook Messenger at least once a week. With regard to other apps, 60% said refugees used WhatsApp at least once a week, and a respective 55% and 50% citing use of Skype and Viber, again at least once per week. ⁶⁴
Refugees in Zaatari camp, Jordan	234 people in the Zaatari refugee camp aged 15–45, 47% female, with surveys carried out in January 2015	<p>A total of 86% of young people owned mobile handsets, while 83% owned SIM cards. Even with these reasonably high levels of SIM-card ownership, 79% of young people also said they borrowed SIM cards from friends and family. Unsurprisingly, mobile phones were the most popular medium for accessing the internet.</p> <p>In the camp, over half of the youth population reported accessing the internet one or more times per day. In terms of communications services, WhatsApp was the messaging app most frequently used for communication with people in Jordan and Syria. However, mobile voice calls were used more frequently overall for communicating within Jordan itself.⁶⁵</p>
Refugees in transit camps in Macedonia	107 refugees from various countries in Tabanovce transit camp, ⁶⁶ 48% female, interviewed March–April 2016	<p>Respondents were more connected than anticipated – 90% indicated they used the internet to contact friends and family; with Viber and WhatsApp cited as the most frequently used tools. Respondents over 55 had a slightly lower than average use of Viber and WhatsApp.</p> <p>Face-to-face communication was overwhelmingly the preferred choice of communication with UNHCR. Limited numbers of respondents referenced social media or [messaging apps].⁶⁷</p>
Syrian refugees in camps and urban areas in Lebanon	More than 100 people, 26% female, interviewed in 2013	<p>Most Syrian refugees reported having a cell phone. Only 14% of interviewees did not have access to a mobile phone. 40% of those who have access to a cell phone own a smartphone.</p> <p>While not all had the capability to make immediate calls, many reported paying for data in order to use applications such as WhatsApp. Reliance on word of mouth as a primary source of information for most refugees has extended to significant reliance on mobile phone and SMS (WhatsApp for those with enabled phones who can afford data bundles) as the main channels of information flow both inside Lebanon and cross-border.⁶⁸</p>
Refugees in Greece Turkey and Jordan	108 people, 50% female interviewed in 2015 ⁶⁹	[Refugees'] use of these smartphones is overwhelmingly focused on social messaging apps: above all Facebook and WhatsApp, with small numbers additionally using others including Viber, Telegram, Line and WeChat. WhatsApp messages are sent one-to-one and in groups, but as far as we saw these groups did not extend beyond a person's circle of acquaintances. Our impression was that Facebook too was being used above all as a messaging service. ⁷⁰
Women in Afghanistan	50 women aged 18–30, interviewed in 2016	More than 75% of respondents own smartphones, and for a plurality (41%), mobile 3G is the only source of internet access. 73% are active on social networks, and Facebook by far was the most popular social-networking platform (used by 73% of those active on social networks). Viber is the most common messaging app, preferred by about 47% of respondents. ⁷¹
People living in the Palestinian Territories	81 people, 32% female, interviewed in 2016	Every respondent owns at least one mobile phone (two in five own multiple phones). The overwhelming majority own smartphones, which they identify as their primary gateway to the internet. 95% use Facebook regularly and 85% use WhatsApp (which is used more than text). ⁷²

64 UNHCR, Connecting Refugees, 2016: <http://www.unhcr.org/en-us/connectivity-for-refugees.html>.

65 Carleen Maitland and Ying Xu, "A Social Informatics Analysis of Refugee Mobile Phone Use: A Case Study of Za'atari Syrian Refugee Camp", TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper, 31 March 2015: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588300.

66 Breakdown: 48% from Afghanistan, 42% Syria, 9% Iraq, 1% Iran.

67 UNHCR, Information and Communication Needs Assessment, March 2016 - Tabanovce, 2016: <https://data.unhcr.org/mediterranean/documents.php?page=1&view=grid&Org%5B%5D=75>.

68 Janine di Giovanni et al, Lost: Syrian Refugees and the Information Gap, Internews, 2013: <https://internews.org/research-publications/lost-syrian-refugees-and-information-gap>.

69 Detailed breakdown: 35 in Greece, 40% female; 23 in Jordan, 30% female; 50 in Turkey, 90% female.

70 Ben Mason and Dennis Buchman, ICT4Refugees: A report on the emerging landscape of digital responses to the refugee crisis, 2016: https://regasus.de/online/datastore?epk=74D5roYc&file=image_8_en.

71 Anand Varghese, "Digital Insights Afghanistan: How Young Women are Using Tech", 18 February 2016: <https://dai-global-digital.com/consumer-insights-afghanistan-how-young-women-are-using-tech.html>.

72 Karim Bin-Humam, "Digital Insights Palestine: E-Governance Readiness", 22 June 2016: <https://dai-global-digital.com/consumer-insights-palestine-e-governance-readiness.html>.

HOW ARE PEOPLE USING MESSAGING APPS IN HUMANITARIAN CRISES?

There is little verified, disaggregated data about messaging-app usage patterns among people in crisis situations. Most data come from people on the move. Many interviewees emphasized that refugees and IDPs preferred to communicate with humanitarian organizations in face-to-face interactions, noting that this was often seen as the best way of getting trustworthy information.⁷³

Interviewees who had used messaging apps to communicate with people in humanitarian situations noted that they were used in a more conversational way than was true of SMS use – a finding backed up by scientific studies of user behaviour in Europe and North America.⁷⁴ Thus, rather than attempting to summarize content into a single SMS message, individuals tend to send multiple messages to communicate a single point, write longer messages and generally view interactions as more fluid and longer-lasting.

Experimental research indicates that users expect faster response times when using apps, particularly because many apps show a user when another person has read their message.⁷⁵

In Arabic-speaking situations, a range of interviewees described usage as “much more vocal and voice-driven” than in Europe or the United States. They also noted that voice messages were particularly common, which could be because voice messages avoid the need for the user to be fully literate, and are faster and easier than typing Arabic or Latin letters.⁷⁶

Several interviewees also said that messaging apps had given some users with limited literacy skills (often older people) a way to interact with humanitarian organizations, noting that they had seen users in Turkey and Syria recording and sending voice messages because they did not have to type them.

In Arabic-speaking situations, a range of interviewees described usage as “much more vocal and voice-driven” than in Europe or the United States, and suggested that this gave those with limited literacy skills (often older people) a way to interact with humanitarian organizations.

Using WhatsApp to register refugees for a cash-transfer programme

A humanitarian organization collecting numerical information from refugees as part of a cash-transfer programme began asking beneficiaries to send photographs of the relevant form over WhatsApp, rather than requiring them to accurately type or read out the number over the phone. The beneficiaries found this easy to do and it became part of the organization’s regular process, with the data from the photograph being manually entered into the database.

The organization found that this was more reliable than previous methods, but noted that it was also a time-consuming process. Staff members said they were actively looking for ways to collect data using messaging apps in such a way that the information could be added automatically into their database.

73 Corinne Gray, “Is your app the best way to help refugees? Improving the collaboration between humanitarian actors and the tech industry,” 14 October 2016: <http://innovation.unhcr.org/app-best-way-help-refugees-improving-collaboration-humanitarian-actors-tech-industry/>.

74 Karen Church and Ricardo Oliveira, “What’s up with WhatsApp? Comparing Mobile Instant Messaging Behaviors with Traditional SMS,” *MobileHCI*, 2013, August 27–30, 2013: <https://doi.org/10.1145/2531602.2531679>; Kenton P. O’Hara, Michael Massimi, Richard Harper, Simon Rubens, and Jessica Morris, “Everyday dwelling with WhatsApp,” 2014, *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, 1131–1143: <http://doi.acm.org/10.1145/2531602.2531679>.

75 Martin Pielot, Rodrigo de Oliveira, Haewoon Kwak, Nuria Oliver, “Didn’t You See My Message? Predicting Attentiveness to Mobile Instant Messages,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3319–3328: <http://dl.acm.org/citation.cfm?id=2556973>.

76 Interviews; Timo Luege, “The WhatsApp response,” 22 August 2016: <http://sm4good.com/2016/08/22/whatsappresponse/>; Ben Mason and Dennis Buchman, *ICT4Refugees*, 2016: https://regasus.de/online/dastore?epk=74D5roYc&file=image_8_en; Comments on Techfugees Slack group: <https://techfugees.slack.com/archives/general/p1458825187000058>.

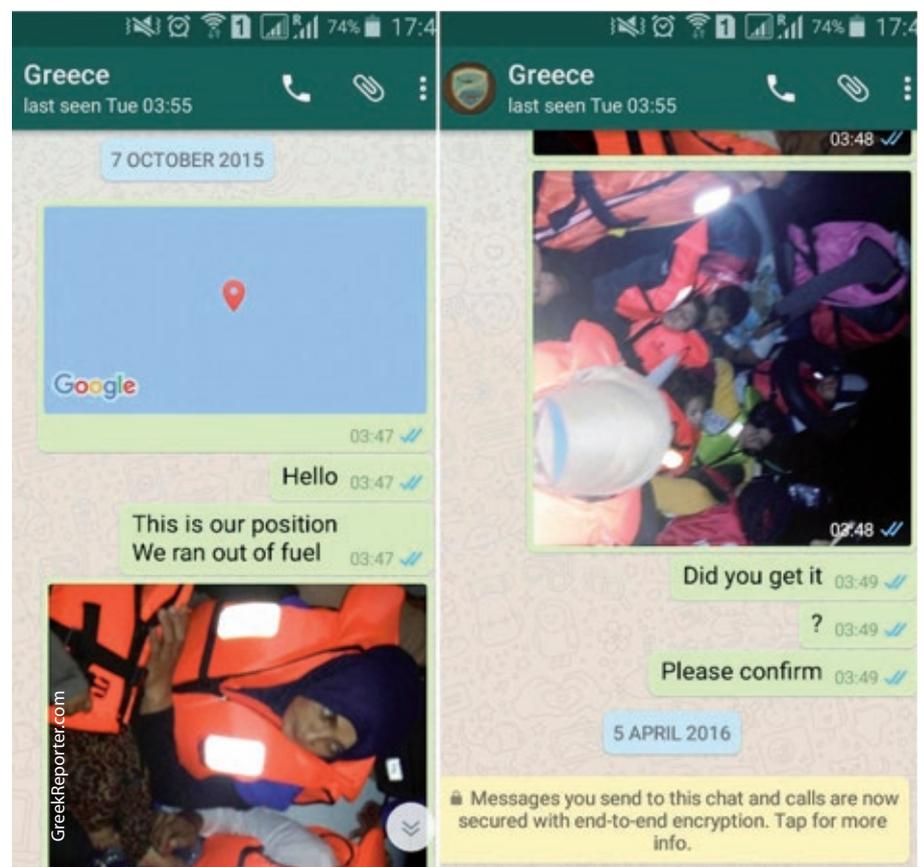
WHAT ARE PEOPLE IN CRISIS SITUATIONS USING MESSAGING APPS FOR?

The tasks that messaging apps are used to perform are also likely to differ significantly depending on the situation - existing research has tended to focus on the Middle East, and its findings should not be applied to other geographic areas.

Refugees and migrants in transit

Research by the Danish Refugee Council has identified a typology of usages of digital communications technologies by people migrating to Europe.⁷⁷ These include:

- finding data on the intended country of destination (including legal information);⁷⁸
- initiating contact with smugglers or brokers;
- getting updated information on migration routes, particularly attempting to verify rumours; and
- accessing safety and rescue services while in transit.



Screenshots of the messages, location and pictures that 30-year old Syrian lawyer Mahmoud Alkuder sent to the Greek Coast Guard in October 2015 to alert them to his position when the vessel that he and some 60 other people were on ran out of fuel. The boat was rescued by the Coast Guard and towed to the nearby island of Lesbos.

⁷⁷ Bram Frouws, Melissa Phillips, Ashraf Hassan and Mirjam Twigt, *Getting to Europe the WhatsApp Way: The use of ICT in contemporary mixed migration flows to Europe*, Danish Refugee Council, 2016: <http://www.regionalmms.org/index.php/10-briefing>.

⁷⁸ John Warnes, "Update: 10 CwC challenges in the new face of the European Refugee crisis": <http://innovation.unhcr.org/update-10-cwc-challenges-new-face-european-refugee-crisis/>.

Messaging apps were described as being most frequently used to contact others (primarily existing friends and family) to share information about their situation or verify information that they had found elsewhere.

Research on smartphone usage among refugees in transit to Europe has suggested that rather than viewing smartphones as a way of accessing the internet, refugees prefer to see “phones as phones,” primarily using them to stay in touch with people they know.⁷⁹

Some anecdotal evidence indicates that refugees also use apps to communicate with people that they do not know - ranging from investigative journalists keen to gain information about refugees' living conditions, smugglers or organizations that could directly respond to their needs such as rescue services and humanitarian organizations.⁸⁰ However, there is little detailed information available about the nature of these interactions.

Communications with the diaspora

In some regions, messaging apps seem to play a crucial role in making connections between diaspora members and individuals in their home country.⁸¹ Sacha Robehmed of REFUNITE, a non-profit organization with a platform that helps refugees and IDPs search for and reconnect with their families using their mobile phone, stated: “Syrian refugee populations are so connected that most don't need a service like REFUNITE - they are already in contact with relatives dispersed globally, using WhatsApp, imo, Viber and Facebook.”

Messaging apps were most frequently used to contact friends and family, share information about their situation or verify information.

In many cases, members of the diaspora are now directly involved in sharing and disseminating information about routes and conditions in other countries.



Internet café at the Nakivale refugee settlement, six hours' drive west of Kampala, capital of Uganda.

In many cases, members of the diaspora are now directly involved in sharing and disseminating information about routes and conditions in other countries.⁸² Some refugees and former refugees actively participate as members of information networks for others who are

79 Aviva Rutkin, “Phoning in refugee aid”, *New Scientist*, 16 April 2016: <http://www.sciencedirect.com/science/article/pii/S0262407916306595>; Janine di Giovanni et al, *Lost: Syrian Refugees and the Information Gap*, Internews, 2013: <https://internews.org/research-publications/lost-syrian-refugees-and-information-gap>; REACH and UNHCR, *Mass Communications Assessment in Azraq Camp (December 2015)*, April 2016: <http://data2.unhcr.org/en/documents/details/43703>; Ben Fox Rubin and Richard Nieva, “Seeking shelter”, 3 August 2016: <https://www.cnet.com/special-reports/road-trip-greece-refugee-crisis/>.

80 Claire Reilly, “WhatsApp messages from a ‘prison’ island, thousands of miles away”, 18 August 2016: <https://www.cnet.com/news/whatsapp-messages-from-detention-a-thousand-miles-away-refugee-crisis/>; Lina Srivastava, “The if and when of technology for the global refugee crisis”, 20 June 2016: <http://civichall.org/civiciist/the-if-and-when-of-technology-for-the-global-refugee-crisis/>.

81 Jodi Kantor and Catrin Einhorn, “What Does It Mean to Help One Family?”, 8 September 2016: https://www.nytimes.com/interactive/2016/10/22/world/americas/canada-refugees-syria.html?_r=0.

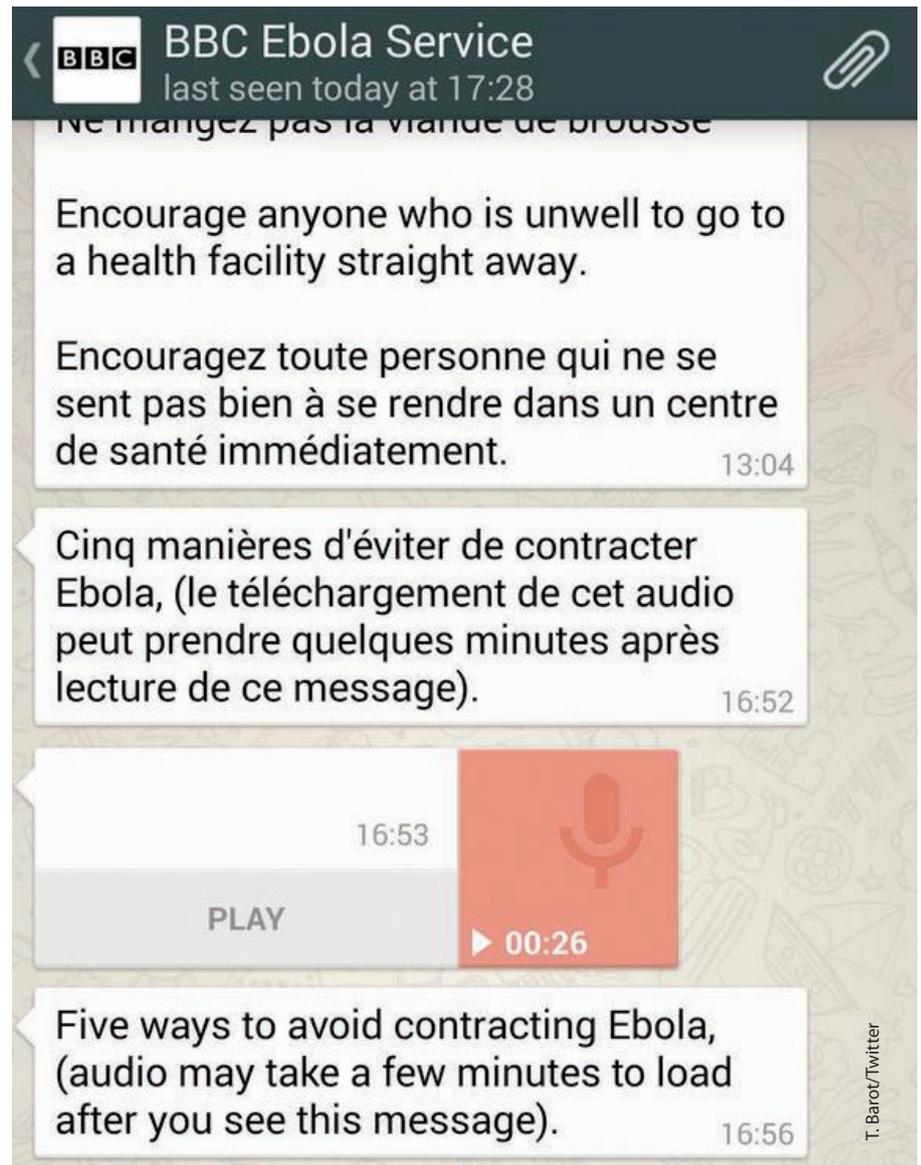
82 See, for example, Nicholas Shmindle, “Ten Borders”, *New Yorker*, 26 October 2015: <http://www.newyorker.com/magazine/2015/10/26/ten-borders>.

in transit between locations, sharing up-to-date information about sea conditions, border crossings and rescue organizations' contact details.⁸³

Epidemics

Research by BBC Media Action found that during the Ebola crisis, people appreciated using messaging apps to hear “people like them” voice their concerns, as well as to access accurate information and ask questions about their situation.

Separate BBC Media Action research found that many people set up small, private WhatsApp groups where they shared quotes from press releases and news briefings, updates on aid facilities throughout the country, and reports on incidents, and asked questions about their own situation.⁸⁴



In October 2014 the BBC launched an Ebola public health information service on WhatsApp to help people get the latest public health information to combat the spread of Ebola in the region.

83 Theodora Hannides, Nicola Bailey and Dwan Kaoukji, *Voices of Refugees*, BBC Media Action, 2016: <http://www.bbc.co.uk/mediaaction/publications-and-resources/research/reports/voices-of-refugees>.

84 BBC Trending, “#BBCtrending: Talking privately about Ebola”, 11 October 2014: <http://www.bbc.co.uk/news/blogs-trending-29574923>.

But people have also shown a willingness to share personal information about their own experiences. During the 2014 Ebola crisis in Sierra Leone, more than 12,000 people signed up for WhatsApp groups organized by BBC Media Action which allowed them to send comments, questions and programming requests.⁸⁵

An evaluation of the project also found that people were keen to share their experiences publicly, suggesting that this activity may meet refugees' psychosocial need to express themselves.⁸⁶

Natural disasters

In the immediate aftermath of natural disasters, people use messaging apps for three purposes: to contact friends and family, access accurate information about the situation and express their most urgent needs.⁸⁷

For example, the LINE app was created after the 2011 Japanese earthquake by employees of a company who wanted to communicate with family members while phone networks were unavailable. The BBC has also used Viber to distribute verified information about relief efforts and public safety in Nepal (although low literacy levels and connectivity gaps limited its usage outside the capital, Kathmandu).⁸⁸

It is also important to note that any attempt by organizations to use messaging apps for humanitarian purposes could be appropriated in unexpected, unplanned ways. For example, in the Philippines, radio stations that used Frontline SMS, an SMS messaging platform, to receive feedback on their humanitarian programmes found that the service was mainly used for song requests and dedications to friends and family members.⁸⁹

During the 2014 Ebola crisis in Sierra Leone, more than 12,000 people signed up for WhatsApp groups organized by BBC Media Action that allowed them to send comments, questions and programming requests.

In the immediate aftermath of natural disasters, people use messaging apps for three purposes: to contact friends and family, access accurate information about the situation and express their most urgent needs.

Turkey: When WhatsApp unexpectedly becomes 50% of your hotline interaction

As part of a cash-card programme for Syrian refugees being implemented in Gaziantep (Turkey), German private aid organization Welthungerhilfe set up a hotline service to provide support to users. At no time did the group advertise that it would be using WhatsApp. However, soon after establishing the hotline number, people started spontaneously contacting the group using the messaging app rather than by making conventional phone calls.

About 50% of the contact the organization receives is now through WhatsApp. Staff members note that they are often contacted this way by elderly people who have difficulties typing (or are illiterate), and who prefer to send voice messages instead of text.

WHAT DON'T WE KNOW?

This brief overview highlights a series of knowledge gaps that humanitarian organizations and researchers should aim to address in order to make an informed decision on whether it is appropriate to adopt a messaging app in a particular context, and how it can be responsibly and effectively done.

85 BBC Media Action, *Humanitarian Broadcasting in Emergencies: A Synthesis of Evaluation Findings*, 2015: <http://www.cdacnetwork.org/tools-and-resources/i/20151006113456-dir49>.

86 BBC Ebola, "What do you miss about life before Ebola?", 23 January 2015: <https://medium.com/@bbcebola/what-do-you-miss-about-life-before-ebola-9fa92d26fd89#np9188hzh>.

87 Imogen Wall, Citizen Initiatives in Haiti. *Forced Migration Review*, 38, October 2011: <http://www.fmreview.org/technology/wall.html>.

88 Digital News Asia, "BBC Nepali earthquake lifeline public chat channel on Viber", 6 May 2015: <https://www.digitalnewsasia.com/digital-economy/bbc-nepali-earthquake-lifeline-public-chat-channel-on-viber>; Online Khabar, "In terms of popularity, Nepali Viber users make it to top 10 in the world", 24 June 2016: <http://english.onlinekhabar.com/2016/06/24/380043>.

89 See the Humanitarian Technologies Project: <http://humanitariantechnologies.net/publications/>.

There is a lack of empirical data in many countries worldwide on smartphone and messaging app usage by refugees, IDPs and other groups or persons in crisis situations, particularly (but not exclusively) in sub-Saharan Africa.

More work is needed to understand levels of access to these apps, how frequently they are used in comparison to other communication channels, and what they are used for. Any such research should also pay particular attention to inequalities in access, with a focus on gender, age, socio-economic background and experience with technology. A good starting point will be for humanitarian organizations to systematically include questions on access to and use of mobile telephony in humanitarian needs assessments.

The fact that people in some situations are using messaging apps to contact their friends and family does not mean that they will necessarily want to use the same apps to interact with humanitarian agencies.

There is also limited research on whether people use apps differently when they interact with humanitarian organizations. As UNHCR's Emergency Lab Manager Katie Drew points out, the fact that people in some situations are using messaging apps to contact their friends and family does not mean that they will necessarily want to use the same apps to interact with humanitarian agencies.⁹⁰

Research on social media- and SMS-based initiatives to collect feedback in the Philippines following Typhoon Haiyan found that people were more likely to share views with their peers than aid agencies.

Separate research suggests that refugees typically prioritize information about how to get work over information about how to get aid.⁹¹ Qualitative and ethnographic research methods may produce particular insights in this area.⁹² More research is needed to investigate how people interact with messaging apps, whether they are appropriate in particular situations and what kind of information such apps are best suited to distribute.

90 Katie Drew, "The European Refugee crisis: 10 Communications with Communities challenges", 6 January 2016: <http://innovation.unhcr.org/the-european-refugee-crisis-10-communications-with-communities-challenges/>.

91 Humanitarian Technologies Project, 2015: <http://humanitariantechnologies.net/lessons-from-haiyan/>; Janine di Giovanni et al, *Lost: Syrian Refugees and the Information Gap*, Internews, 2013. <https://internews.org/research-publications/lost-syrian-refugees-and-information-gap>.

92 Jonathan Ong, "Appealing to Agencies in Only 140 Characters? Towards More Compassionate Communication Architectures in Community Engagement", 2015: http://cooperation.epfl.ch/files/content/sites/cooperation/files/Tech4Dev%202016/1277-Ong-SE01-HUM_FullPaper.pdf.



in a nutshell – kurz gesagt

Humanitarian organizations need to develop responsible, effective ways to use messaging apps in order to meet people's needs.

3. HOW ARE HUMANITARIAN ORGANIZATIONS USING MESSAGING APPS?

This section describes humanitarian organizations' current approaches to using messaging apps, as well as the challenges they see and benefits they expect as they make decisions about which apps to use. It is based on desk research and interviews with staff members and technical personnel who work for humanitarian organizations.

HOW ORGANIZATIONS ARE USING MESSAGING APPS

Most humanitarian organizations contacted for this research said they were not using messaging apps in any formalized, official way. When asked why, most indicated that smartphone ownership rates among the people they worked with were too low to justify the use of messaging apps and mentioned SMS-based programmes as their primary method of communication.

For example, representatives of one large international non-governmental organization (INGO) operating in a conflict-affected area stated that they had considered using messaging apps, but had instead decided to continue with SMS-based methods after extensive surveys of affected people indicated that the vast majority lacked access to the internet or internet-enabled smartphones.

Another interviewee working in East Africa said: "I do believe smartphone access is pretty limited within most refugee communities in Africa, and an SMS solution ... is simpler and more accessible to far more [people]." Similar views were expressed by interviewees working in South Asia, sub-Saharan Africa and parts of the Middle East.

Where messaging apps were being used, organizations had often adopted them in an ad hoc way - with an organization realizing that its staff or affected people were already using an app and then looking for ways to utilize it effectively. In these cases, organizations often lacked defined procedures and protocols for using apps and did not always demonstrate that they had considered whether additional steps were needed to ensure that data was collected and managed responsibly. Section 4 below looks at these questions in greater detail.

However, there were signs of growing interest among interviewees in developing longer-term plans to incorporate messaging apps into their overall communications and operational strategies.

A small number of interviewees said they were considering introducing messaging apps into their work in 2016, while technical service providers said they were experiencing increased interest in the topic from a range of humanitarian organizations.

WHY ARE ORGANIZATIONS ADOPTING MESSAGING APPS?

Staff at humanitarian organizations interviewed for this report said they were considering incorporating messaging apps (in addition to existing communications methods such as SMS, voice calls or radio) for the following reasons:

- **Target audiences (staff or affected people) are already using messaging apps.** Interviewees typically said the app they were considering for use was already being widely used by the people they aimed to reach, or that people were already spontaneously contacting them using that app. As one interviewee, describing the situation in Iraq, put it:

"Any number you put out there, you can expect that strangers will use it to try to connect via WhatsApp and Viber. It has happened to me and it happens to pretty much everyone here. People just assume that you can be reached that way - and they do not hesitate to try - at all hours of the day and night."

For example, Yotam Polizer of the Israeli non-governmental, non-political aid organization IsraAID said that the organization uses LINE in Japan and KakaoTalk in Korea, “because that’s what people use,” while the American Red Cross delegation in Vietnam uses Zalo, an app popular in that country, to share information among volunteers.

Separately, there have been increasingly widespread suggestions that refugees are comparatively less likely to download new, bespoke apps to communicate with humanitarian agencies, particularly given the recent proliferation of such new apps.⁹³

- **Messaging apps can help reduce communications costs.** This is true both for the humanitarian organizations themselves (which otherwise have to pay fees for SMS or interactive voice response (IVR) services), and for the refugees or other target populations (who would otherwise send SMS messages or make conventional phone calls). A number of interviewees said that some organizations were starting to find the costs of SMS-based initiatives prohibitive, with long-term trends looking particularly difficult to sustain.



Syrian refugee making a phone call after disembarking from a Hungarian bus that brought her to the border.

- **Messaging apps offer a reliable way of maintaining contact with people (whether staff or refugees) in transit.** Apps make it easier to communicate across borders without increasing costs, while mitigating problems raised by the fact that refugees frequently change SIM cards or use multiple SIM cards for different purposes.⁹⁴ Some interviewees also said that using messaging apps to contact staff members for the purposes of internal coordination was easier than using email.

⁹³ For some examples of this viewpoint, see: Corinne Gray, “Is your app the best way to help refugees? Improving the collaboration between humanitarian actors and the tech industry”, 14 October 2016: <http://innovation.unhcr.org/app-best-way-help-refugees-improving-collaboration-humanitarian-actors-tech-industry/>; Ben Mason, “The Refugee Tech Crisis”, 29 March 2016: https://ssir.org/articles/entry/the_refugee_tech_crisis; Lina Srivastava, “The if and when of technology for the global refugee crisis”, 20 June 2016: <http://civichall.org/civicist/the-if-and-when-of-technology-for-the-global-refugee-crisis/>; Krithika Varagur, “Refugees Don’t Need Your Apps”, July 2016: http://www.huffingtonpost.com/2016/06/30/refugees-dont-need-your-a_n_10757006.html.

⁹⁴ Linda Leung, “Phoning home”, *Forced Migration Review*, 38, October 2011: <http://www.fmreview.org/technology/leung.html>.

WhatsApp improves staff communication, speeds refugee-support efforts

IsraAID (see above) uses a WhatsApp group for staff communications in each of the 19 countries in which it works. IsraAID's Yotam Polizer said the organization chose WhatsApp because it allows staff to send information quickly, uses relatively small amounts of data, and allows staff from different parts of the organization (from coordinators to nurses) to share information about their work. "Our main form of communication is still email. But most people have to read it in their office and don't have time to read it in a crisis," Polizer said.

In Lesbos (Greece), IsraAID also created WhatsApp groups that included volunteers working to support refugees. First responders seeking to meet refugees arriving on Lesbos additionally formed ad hoc WhatsApp groups that included numerous support organizations.

Groups were either organized by area ("the south beach") or according to the humanitarian cluster system (with one group for each cluster). Members of each group used WhatsApp's location function to share their location every time a boat landed, thus making it easier for others to plan how to get to the location, as the app's location-sharing feature allows users to connect directly to Google Maps' route-planning function.

The groups naturally developed a structured process for sharing information and reporting incidents, without any explicit instructions being given. However, participants said this could have developed more quickly with some guidance. "It took two to three months for everyone to get to this point of coordination. If the crisis were to start again, I would push for it from day one," Polizer said and suggested that a manual setting out processes for internal communication could be a helpful step towards this.

- **Messaging apps enable communication with people in environments where other communications methods are unavailable.** This is particularly true of apps that work well over low-bandwidth internet connections. This capability can be useful in a wide range of circumstances, including when infrastructure has been damaged by conflict or a natural disaster.

Interviewees cited situations such as that in post-earthquake Nepal, where messaging apps remained operational when other communications networks were unavailable.⁹⁵ Mesh-network technologies such as Open Garden's FireChat app and its MeshKit software module offer further potential to connect phones when internet and telephone networks are unavailable, by using smartphones' in-built Wi-Fi and radio transmitters. The usefulness of mesh technology is currently limited by the fact that a significant proportion of people in a given area need to have downloaded and enabled it for the network to function (FireChat suggest that this is around 5% of the total number of smartphone users in any urban area). However, it has been already used in the aftermath of a small number of natural disasters - for example, FireChat has stated that 23,000 people in Chennai downloaded the app in a five-day period in 2015 following flooding in the area.⁹⁶

⁹⁵ As Natalie Miller from the BBC's User-Generated Content Hub described the situation in Nepal: "Phone lines were down in the affected areas and we can be waiting a long time for an email to be received and answered, whereas WhatsApp is quick and allows people to share their views, pictures, and videos with us all via the same channel" - See Trushar Barot and Eytan Oren, *Guide to Chat Apps*, Tow Center, 2015: <http://towcenter.org/research/guide-to-chat-apps/>; Yotam Polizer, "WhatsApp in Nepal - How one little app saves lives", *Times of Israel*, 15 September 2014: <http://blogs.timesofisrael.com/whatsapp-in-nepal-how-one-little-app-saves-lives/>.

⁹⁶ <http://www.opengarden.com/meshkit.html>; Indian Express Tech Desk, "#ChennaiRains: With networks down, people turn to FireChat again", *Indian Express*, 3 December 2015: <http://indianexpress.com/article/technology/social/chennairains-with-networks-down-people-turn-to-firechat-again/>. FireChat also state that in 2015, 26,000 people signed up for the service in Mexico in advance of hurricane Patricia.

- **Messaging apps can increase the speed of communications.** Several interviewees said that messaging apps allowed them to communicate more quickly than had been possible using SMS, particularly when conventional phone network capacity was limited or overloaded during crisis situations. One interviewee described an occasion when SMS messages designed to be sent in quick succession as part of a situational-analysis initiative during a crisis response were ultimately transmitted with 60- to 90-second delays between each message. This frustrated users and reduced the amount of information submitted, the interviewee said.
- **To a limited extent, messaging apps can improve digital-communications security as compared with existing methods of communication.** Very few interviewees cited security and privacy considerations as a major reason underlying their decisions to consider using a messaging app. However, several noted that despite the security limitations currently associated with messaging apps, information transmitted via SMS or conventional phone calls over telephone networks was likely to be even easier for adversaries to access. They cited the potential benefits of end-to-end encryption of message content, the inherent insecurity of the mobile-phone network infrastructure, and the fact that the message content of all SMS messages could be accessed by mobile-network operators, and thus potentially governments if pressure was brought to bear.⁹⁷
- **Messaging apps help organizations gather information from hard-to-reach areas.** Humanitarian organizations working in conflict-affected situations often find it difficult to conduct face-to-face meetings with individuals in remote areas, due to security concerns, official restrictions or the difficulty of travel. Several interviewees said that messaging apps can facilitate communication with people whose voices might otherwise not be heard.

WhatsApp offers remote-reporting capabilities in dangerous conflict areas

A UN agency working in a conflict-affected area has been using WhatsApp to collect information about the situation since early 2016.

To carry out this process, a single staff member sets up a number on WhatsApp and uses it to communicate directly with people in the area. Individual contacts are added by going through trusted networks of people. The staff member asks the people contacted short questions about their situation and then enters the data manually into spreadsheets.

The agency subsequently cross-checks the information with data from other sources and includes it directly in reports.

The agency said that using the app allowed it to obtain information it would otherwise have been unable to access, as the risks of making randomized phone calls were too great, and some individuals in remote locations who were unable to access phone networks were able to send information online.

Most importantly, this method allowed the agency staff member to build up a relationship of trust with the individuals contacted, which in turn helped to speed up data entry over time as these contacts learned more about the process. Agency staffers described the process as “quite manageable” and suggested that it was not overly labour-intensive, as they were speaking to only a small number of people.

⁹⁷ For a more detailed overview of these risks, see Frontline SMS, “User Guide on Data Integrity”: <http://www.frontlinesms.com/impact-of-frontline/guides-tools-and-case-studies/>.

- **Features unique to messaging apps can provide additional information that speeds up data collection or increases efficiency.** Interviewees cited the ability of many apps to send the location of a user's phone using its inbuilt geolocation system as a useful feature for security teams seeking to locate a particular staff member.⁹⁸ The ability to send comparatively long messages can also help overcome challenges imposed by the character limit on SMS messages.
- **Messaging apps can improve inter-office coordination.** Some interviewees said the various apps' ability to distribute text, voice messages, documents and other files among small groups had made it easier and faster to coordinate activities between organization offices. This can be particularly important in crisis situations, when communication is time-sensitive.

WhatsApp bridges gaps between far-flung offices in Indonesia

Markas Pusat from the Palang Merah Indonesia (PMI), the Indonesian Red Cross Society, uses WhatsApp to help coordinate activities between the organization's headquarters and branch offices, both in normal and emergency or conflict situations.

Each branch office creates its own group, which is then linked with the organization's headquarters, especially the Health and Communications Division. Staff members share documents, location information, photos and audio within the group, and also make calls using the app. They report that it makes communications run "well and fast".

98 Timo Luege, "The WhatsApp response", 22 August 2016: <http://sm4good.com/2016/08/22/whatsappresponse/>.

HOW ARE APPS BEING INCORPORATED INTO ORGANIZATIONS' WORK?

Humanitarian organizations are currently experimenting with messaging apps for two main purposes: to communicate with people affected by crisis or conflict, and to coordinate tasks and actions internally. Within each of these categories, the apps are used for a variety of specific purposes.

COMMUNICATING WITH COMMUNITIES

As organizations seek to work and communicate with people in crisis- or conflict-affected areas, messaging apps are currently being used in the following ways:

- **As a hotline.** Since June 2015, the ICRC's Yemen delegation has used WhatsApp as a dedicated hotline to enable people to report incidents or request assistance. As reports are received, the communications department manually clusters the most frequently recurring and relevant messages into a Microsoft Excel spreadsheet and shares this information with the appropriate department within the delegation. The most urgent messages (such as security incidents or requests for lifesaving assistance) are immediately shared with relevant departments by phone and/or email.



The ICRC in Yemen uses WhatsApp to disseminate information about its activities and messages to increase awareness of health epidemics, the protection of humanitarian personnel and other topics.

- **In collaboration with local media.** BBC Media Action used WhatsApp as part of a broader public-health information programme to disseminate information about Ebola. The organization set up a communications hotline through the app for around 19,000 subscribers across West Africa, pushing out messages in collaboration with various UN agencies, and also created content that responded directly to questions from users. Versions of the service were also offered in various local languages.
- **To broadcast information to groups of various sizes.** The Yuva Community Centre in Gaziantep, Turkey, uses Telegram and WhatsApp, as well as SMS, to send refugees information about the services provided by the centre. Tolga Güleç, Yuva's communications

coordinator, said that the organization had found Telegram to be better suited to broadcasting one-way information to comparatively large groups (of around 40–50 people), while WhatsApp was easier to use for two-way communication with smaller groups. SMS, by contrast, was used for communication with all beneficiaries (a population of 1,000 people or more).⁹⁹

- **To support existing discussions in parallel with existing communication channels.** Since it was set up in 2014, the Facebook group “I am a Syrian in Lebanon”¹⁰⁰ has gained almost 35,000 members. It currently receives over 200 questions daily on topics ranging from methods of reporting child abuse to means of accessing services provided by UNHCR and its partners. Its popularity and the increasing difficulty of keeping up with the flow of information led its creator, Oum Nidal, to create a weekly compilation newsletter, sent out on Saturdays, which summarizes and collates comments, questions and replies on a specific issue, such as child labour. UNHCR used the data from the group to inform the analysis made by its Communication with Communities programme and also publicized the group itself through channels including WhatsApp and Facebook.¹⁰¹

INTERNAL COORDINATION

Messaging apps have also proven invaluable in overcoming challenges of communication and coordination within organizations themselves. To this end, organizations are currently using apps in the following ways:

- **To share information about tasks or problems and provide updates.** Interviewees in many countries ranging from Greece to Nepal have used messaging apps to share information about tasks, discuss potential activities, make requests and monitor progress. A range of apps were mentioned by interviewees, with WhatsApp by far the most common.

These organizations typically used the apps’ location-sharing function, exchanged photos, and shared information rapidly among large numbers of staff through the group-discussion feature.¹⁰² Although no interviewees mentioned it in relation to humanitarian work, Slack, a software application designed to facilitate communication within organizations and which works on smartphones and desktop computers, is becoming increasingly popular in other sectors.¹⁰³

- **For internal coordination within a humanitarian organization.** A number of organizations have found that messaging apps enable staff members in remote locations, working in the field or simply in different offices, to coordinate activities more efficiently than is possible simply with email or voice calls. The apps’ ability to use Wi-Fi or mobile phone-network connections make it easier for staff members to stay in touch even when internet or electricity infrastructures are unreliable.

99 Ben Mason and Dennis Buchman, *ICT4Refugees: A report on the emerging landscape of digital responses to the refugee crisis*, 2016: https://regasus.de/online/datastore?epk=74D5roYc&file=image_8_en.

100 <https://www.facebook.com/groups/172406933094432>.

101 UNHCR, “Facebook group helps Syrian refugees navigate life in Lebanon”, 2015: <http://www.unhcr.org/en-us/news/latest/2016/7/577e16064/facebook-group-helps-syrian-refugees-navigate-life-lebanon.html>.

102 Timo Luege, “The WhatsApp response”, 22 August 2016: <http://sm4good.com/2016/08/22/whatsappresponse/>; Deepak Malik, “Emergency response in the WhatsApp era!”, 2 March 2016: <https://blogs.worldbank.org/endpovertyinsouthasia/emergency-response-WhatsApp-era/>; Yotam Polizer, “WhatsApp in Nepal – How one little app saves lives”, *Times of Israel*: <http://blogs.timesofisrael.com/whatsapp-in-nepal-how-one-little-app-saves-lives/>.

103 Josh Constine, “Slack’s growth is insane, with daily user count up 3.5X in a year”, *Techcrunch*, 2016: <https://techcrunch.com/2016/04/01/rocketship-emoji/>.

WhatsApp proves more reliable than email for coordination in East Africa

An organization working directly with refugees in East Africa uses WhatsApp to share information about logistical tasks among groups of staff members, both for teams in the field and for middle managers in the group's offices. One staff member said: "We've never really had an official set-up or plan to use the app. All supervisors have a work-issued office phone and had already downloaded the app without prompting, as it is extremely useful to keep in communication with our staff regardless of their location, which changes from week to week."

The organization uses WhatsApp exclusively for internal coordination, and does not share information about the people they assist. Staff find the app useful because it allows people working in remote areas to share information when email access is unavailable.

As the staff member put it: "Previously, staff in far-off regions might not see email for days if internet access was not reliable. Having WhatsApp ensures important messages can be seen more quickly and acted on."

- **To share security information.** One interviewee described messaging apps as the most convenient means of staying in contact with a security team in an area affected by armed conflict, with conventional landline phones, satellite phones and radio serving as parallel means of communication. Digital security was rarely referenced in this context as a reason for using apps, and it was notable that interviewees generally did not believe that the information sent using messaging apps was more secure than that sent by SMS or other methods. There have been suggestions that using mobile phones to communicate may be useful in areas where possession of a satellite phone or radio can draw negative attention towards the person using it.¹⁰⁴

Processes described included direct one-to-one contact with an organization's security contact person, sending broadcast messages to all members of a group of staff, and sharing information using a "tree" model, in which each person who receives a message is responsible for passing it on to others. Interviewees did not describe providing additional training or guidelines on how to use messaging apps specifically although several mentioned that this would be useful.

- **To share information about progress or individual successes.** As one humanitarian worker noted, describing experiences in Greece: "When something worked – be it the successful move to a new and better camp, or something small like additional drinking-water taps – my colleagues invariably took photos and shared one or two with the WhatsApp Group."¹⁰⁵ A number of interviewees indicated that sharing positive news in this way helped boost staff morale.

104 Athalie Mayo, "SMS Technology and Bulk SMS Delivery Systems: Their Role in Security Management for the Humanitarian Community," in Raquel Vazquez Llorente and Imogen Wall (eds.) "Communications technology and humanitarian delivery: challenges and opportunities for security risk management", 2014, European Interagency Security Forum (EISF): <https://www.eisf.eu/library/communications-technology-and-security-risk-management/>.

105 Timo Luege, "The WhatsApp response", 22 August 2016: <http://sm4good.com/2016/08/22/whatsappresponse/>.

POTENTIAL APPLICATIONS

The following section highlights several potential applications of messaging apps, although researchers are not aware of instances where these features have been used in humanitarian operations.

USING ONE PLATFORM TO SEND MESSAGES FROM MULTIPLE MESSAGING APPS

Most messaging apps use a relatively similar process for sending messages to large groups of people. This means it is becoming increasingly possible to use a central third-party platform to communicate with people on different channels, including one or more messaging apps as well as SMS.

For example, Twilio, a third-party company that has provided bulk SMS software tools to a broad range of organizations, is now expanding into messaging-app marketing. Its messaging toolbox¹⁰⁶ aims to integrate SMS and messaging-app functions in order to identify users across various communications channels, thus ensuring people are not bombarded with the same message on multiple services.

Other organizations are offering or developing similar systems for use in the development and humanitarian sectors.¹⁰⁷ However, there is still more work to be done, and third-party companies are constantly scrambling to keep up with changes to messaging-app products.

ANALYTICS

Interviewees who had worked with messaging apps regularly noted that analysing and processing the data they received was time-consuming and difficult.

At present, most apps provide fairly limited capabilities to access and analyse data on users' interactions with an app. However, as messaging apps take on a larger role in private-sector marketing and communications strategies, app developers may place increasing emphasis on providing analytics tools.

LINE currently offers a dashboard providing real-time information on the number of followers and the performance of specific posts, while Viber sends bi-weekly reports with metrics on subscribers and visitors to Public Chats and Telegram offers details on a post's "reach" (how many users have read or interacted with the content).

A number of third-party companies now provide in-depth analytics on user interaction with bots, which are increasingly being used as a mechanism for bulk messaging through chat apps.

BOTS

All communication with communities must be accompanied by on-the-ground, face-to-face communication and direct assistance.¹⁰⁸ It is important to stress that any attempt to introduce automated processes such as bots risks increasing the perception of distance between a humanitarian organization and the people it works with. That said, interviewees cited several situations in which they felt bots might be appropriate, for instance:

106 <https://www.twilio.com/messaging>.

107 Souktel (<http://souktel.org>) has built custom systems that allow organizations working in international development to send messages to groups of people through either SMS, Viber or WhatsApp; and InSTEDD (<http://instedd.org/>) is working with the World Food Programme to develop a bot that works on Telegram (see World Food Programme mobile Vulnerability Analysis and Mapping project, "Introducing our chatbot", 21 July 2016: <http://mvam.org/2016/07/21/introducing-our-chatbot/>).

108 Rose Foran, "The refugee crisis will not be hacked", 29 July 2016: <http://news.trust.org/item/20160729132618-0oczq/>.

- Allowing the collection of structured survey data, including media such as photos. Several interviewees suggested that bots could potentially increase the accuracy of survey data by introducing questions that can only be answered by selecting one of several predetermined responses or using artificial intelligence to automatically recognize and highlight common data entry errors.
- Providing a user with tailored answers to questions, by using the bot to ask a set of questions and retrieve from a database information that is relevant to the user's needs.

UNICEF launches chatbot to survey young people on issues that affect them

In April 2016 at F8, Facebook's annual developer conference, UNICEF launched a chatbot that integrates with U-Report, a service running in 28 countries worldwide that allows young people to answer polls and report on a broad range of development issues in their communities.¹⁰⁹

U-Report, which uses the open source software platform RapidPro, was built to receive information primarily through SMS. Although it will continue to do so, Blair Palmer, Lab Lead at UNICEF Innovation, said that they had decided to add messaging apps as another communication channel because they recognized that "as people have more access to the internet, people want to use the thing [messaging apps] that they already use." Palmer also added that UNICEF sees adopting messaging apps as a way of reducing messaging costs, noting that "SMS is expensive in a lot of places."

The bot is integrated with Facebook Messenger and Telegram, and UNICEF worked directly with a team from Messenger to implement the integration. It asks young people a weekly series of questions about issues that affect them, including education, sexual and reproductive health, access to health services and their legal rights. UNICEF separately noted that Messenger has enabled them - and their partners who run the platform - to connect a wide range of countries.

Users' answers are recorded in a database, analysed in real-time and shared in aggregated form on public websites and with decision-makers. When UNICEF and the U-Report partners receive unsolicited messages on a specific issue from members known as 'U-Reporters', UNICEF's partner organizations can log in and respond using a separate piece of software (CasePro) that recognizes keywords relating to those partners' areas of expertise. For example, in Uganda UNICEF's partner, the HIV/AIDS organization Mildmay, will respond to messages received asking questions about HIV/AIDS.¹¹⁰

Messaging apps themselves are a relatively new technology, but messaging app bots are even newer. As such, humanitarian organizations should conduct extensive research to identify implications and potential risks in a particular situation before adopting them.

Interviewees highlighted the importance of clearly explaining to a user that they were interacting with a bot rather than a human, suggesting that this was communicated using an automated system that required users to select one of a set of options. However, organizations will need to balance this against the need to provide engaging content using locally relevant slang or dialects and encouraging the user to continue using the bot.

To provide accurate, up-to-date information, a bot also needs to be able to retrieve information from a database or content management system. Because many humanitarian situations change rapidly, it can be challenging for humanitarian organizations to keep information about a particular situation up-to-date at all times, which would require significant investment in time and resources. In crisis situations, it may also be unclear in advance what kind of information will be needed, or what can be organized and structured effectively in advance.

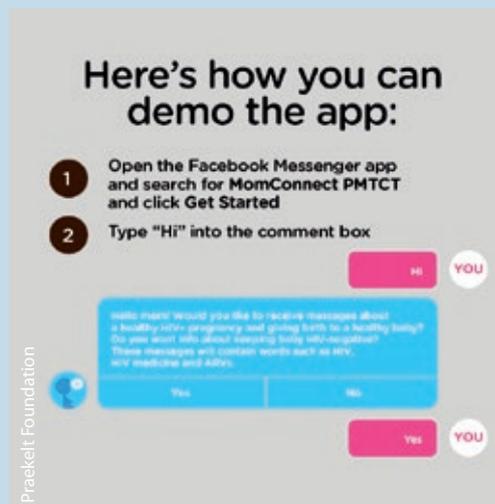
109 See details on various U-Report implementations here: <http://www.unicefstories.org/tag/ureport/>.

110 Facebook, "Building Bots for Messenger – Tips from the Experts: UNICEF", Messenger Blog: <https://messengerblog.com/bots/building-bots-for-messenger-tips-from-the-experts-unicef/>.

However, content that is changed less frequently may be easier to manage. For example, a bot created by the non-profit design organization Refugee Text, which allows users to ask and receive information about asylum requirements in several European countries, retrieves content from a database of relevant legal advice that is updated on a monthly basis by legal advisers from humanitarian organizations.¹¹¹

To take another example, the WhatsGerman app provides German language lessons targeted at refugees currently based in Germany.¹¹² The World Food Programme's mobile Vulnerability Analysis and Mapping (mVAM) project is currently testing a chatbot that works on Telegram (and will be implemented on other platforms) to collect information about food security; many of the lessons it has learned regarding using bots with refugees have been published on the project's blog.¹¹³

South Africa: Using bots to support maternal health



In July 2016, the Praekelt Foundation, an African non-profit organization, launched a bot as part of MomConnect, a programme conducted jointly with South Africa's National Department of Health. It provides pregnant women and new mothers with personalized information and support according to their stage of pregnancy, time until delivery or child's age.¹¹⁴

Praekelt General Manager Debbie Rogers stated that her group had started investigating messaging apps due to the high cost of SMS message fees, because they felt that chatbots offer a more engaging way of delivering content and because she and her colleagues felt that "in a few years SMS is going to become a fairly obsolete service in some of the areas where we're working."

Praekelt.org also runs similar maternal and child health programmes in Nigeria and Uganda and said that they intend to introduce messaging apps in those countries for similar reasons.

The MomConnect bot works with Facebook Messenger, WeChat and Telegram. Praekelt believes that the Messenger version is "showing the most promise" due to Facebook's high penetration rates in South Africa. When a woman registers as pregnant at a clinic, she gives her phone number and is signed up to the service, which primarily works over SMS and USSD. Users who are identified as being able to use the Facebook Messenger service (those who have mobile data access on their phones) are then sent a link to the MomConnect Facebook page, where they can sign up to the bot.¹¹⁵ The bot asks the user a predefined set of questions (similar to those in a conventional survey), recognizes their responses and provides replies from a database of relevant information that is used as part of the MomConnect service.

In the longer term, Praekelt plan to include the ability for users to access the MomConnect helpdesk via the Messenger bot. This helpdesk is currently operated by trained midwives, who respond to users who cannot find the information they get from the stage-based service (allowing users to submit information in a free text input field); this is only currently available to SMS users.

111 <http://refugeetext.org/>. Refugee Text currently works with SMS and is being integrated with Facebook Messenger, Telegram and Viber. A demo of the Facebook Messenger app is available at: www.m.me/refugeetext.

112 WhatsGerman: http://www.whatsgerman.de/whats_app_sprachkurs_eng.html.

113 World Food Programme mobile Vulnerability Analysis and Mapping project, "Chatbot: back to the drawing board", 13 September 2016: <http://mvam.org/2016/09/13/chatbot-back-to-the-drawing-board/>; <http://mvam.org/2016/07/21/introducing-our-chatbot/>.

114 Praekelt, "Curing Pilot-itis for mHealth", 19 July 2016: <http://blog.praekeltfoundation.org/post/147639334452/curing-pilot-itis-for-mhealth>.

115 MomConnect Facebook page: <https://www.facebook.com/MomConnect-PMTCT-1554302084863313/>.

Third-party companies such as ChatFuel offer free, self-service platforms enabling bots to be created for specific purposes and deployed to Facebook Messenger and Telegram.¹¹⁶

Other companies such as ChatSuite, Massively and Sequel offer a greater degree of customization and complexity, while also charging monthly fees for product maintenance and the distribution of messages to users.¹¹⁷ Developers such as Imperson, Msg.ai and Pandorabots also aim to help organizations with larger budgets to build bots with a higher degree of artificial intelligence and the ability to carry on a convincingly human conversation.¹¹⁸

Furthermore, third-party bot platforms have been helping private sector organizations syndicate their bots and track user-interaction statistics across multiple messaging apps. Many third-party bot companies price their services based on the number of messages sent to users, i.e. the more notifications you send, the more you are likely to pay.

Finally, bots pose important questions about the way in which humanitarian agencies engage with people. Any efficiency gains that bots may offer need to be matched by the humanitarian organizations' capacity to provide on-the-ground, practical support to complement any communication.

However, if a bot is unable to 'understand' or answer a user's questions, it may simply increase levels of frustration and decrease trust in the humanitarian organization as a whole.

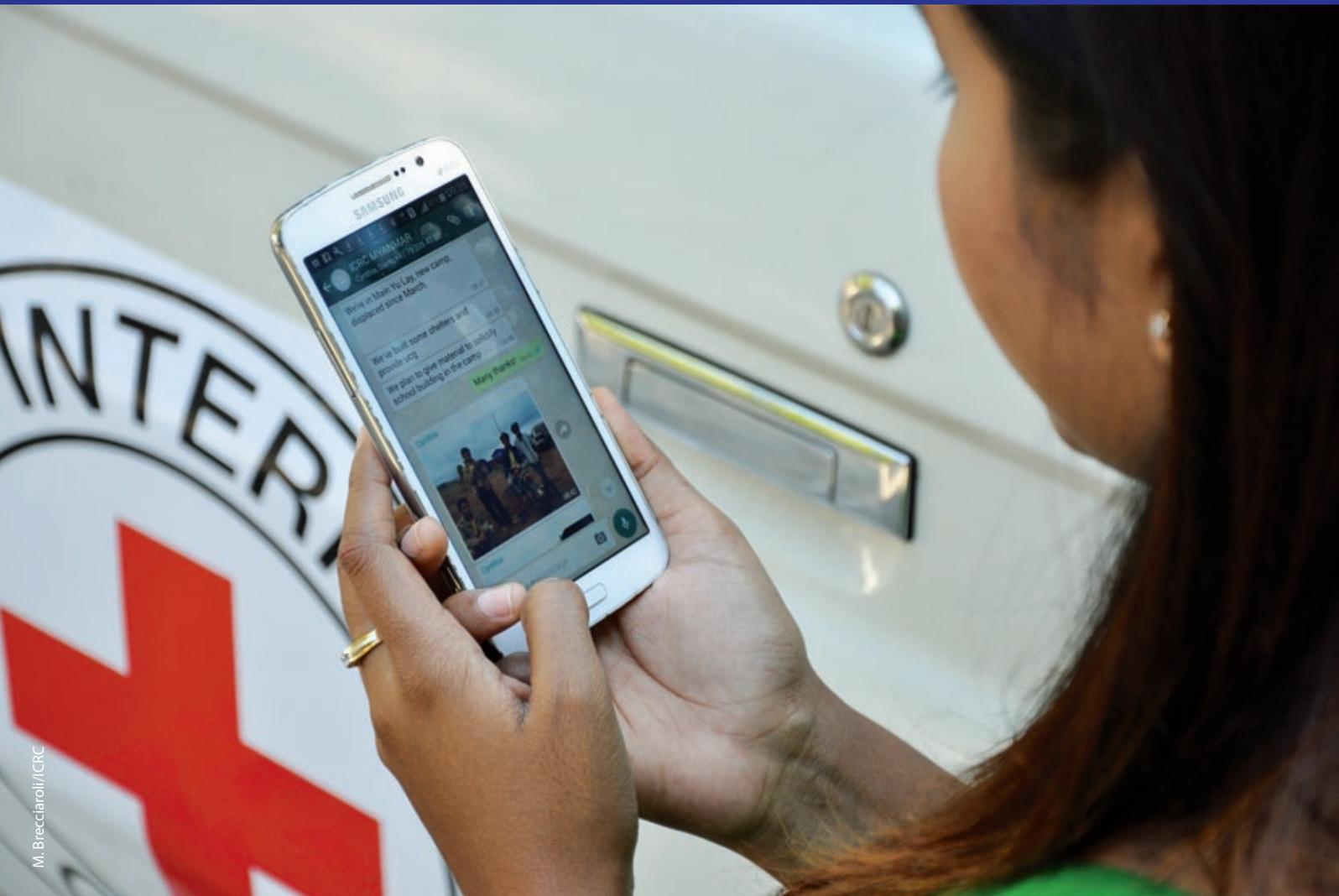
Interviewees involved in developing bots repeatedly emphasised the importance of human-centred design processes that devote substantial time to understanding users' needs, responsible data concerns (see Section 4 below) and ways of relating to bots and apps more generally.

Bots pose important questions about the way in which humanitarian agencies engage with people. If a bot is unable to 'understand' or answer a user's questions, it may simply increase levels of frustration and decrease trust in the humanitarian organization as a whole.

116 <https://chatfuel.com/>.

117 <http://chatsuite.net/>; <http://www.massively.ai/>; <https://www.onsequel.com/>.

118 <http://imperson.com/>; <http://msg.ai/>; <http://pandorabots.com/>.



An ICRC staff member uses a WhatsApp group to communicate with colleagues, Yangon, Myanmar.

4. CONSIDERATIONS WHEN USING MESSAGING APPS IN HUMANITARIAN SITUATIONS

Systems for using messaging apps are currently both new and largely untested, and humanitarian organizations currently have no agreed codes of conduct, standards or ethical frameworks for deploying them. Organizations need to address this “doctrine gap” in order to use messaging apps responsibly.

As the 2014 report *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies* recommends, humanitarian organizations should “support ethical innovation, ensuring that projects using new or untested systems are held to a higher standard of oversight and codes of conduct are regularly updated and enforced.”¹¹⁹

Systems for using messaging apps are currently both new and largely untested, and humanitarian organizations currently have no agreed codes of conduct, standards or ethical frameworks for deploying them. Organizations need to address this “doctrine gap” in order to use messaging apps responsibly.¹²⁰

When a humanitarian organization communicates or exchanges information with local communities, it also has a responsibility to ensure that this generates no harm for those people. The technical characteristics of messaging apps, and the way in which they share and process data, introduce new risks to users’ security and privacy.

This section describes a set of issues for organizations to consider when assessing whether messaging apps can be used responsibly and effectively in a given situation.

WORKING WITH MESSAGING APP PROVIDERS: CHALLENGES AND RISKS

Humanitarian organizations interviewed for this report said that they were attracted to using messaging apps because it would allow them to communicate with people using channels that those people already knew and used on a daily basis. Perhaps as a result, many interviewees said that they decided which apps to use on the basis of popularity - assessing which were most widely used in that context and then working out how to use them.

However, this approach may encourage organizations to adopt apps whose features do not comply with established good practice for security, introduce uncertainties into existing workflows, or run counter to existing data protection policies or laws.

Messaging apps also develop and change features fast, and there is no guarantee that a feature offered by an app will be available indefinitely. Similarly, companies’ policies and statements about data usage, security and privacy may be revised later, as highlighted by WhatsApp’s August 2016 announcement that it would share users’ phone numbers and times of usage with Facebook, despite previous statements to the contrary.¹²¹ In most cases, companies are unlikely to consult users (including humanitarian organizations) or provide advance notification about such changes. Several interviewees described instances where an app that they were using to communicate with groups of people altered or removed features at short notice, forcing the organization to dramatically change its strategy.

Consequently, organizations may be unable to view the technical details of the underlying code, and therefore unable to make a comprehensive assessment of how changes affect users’ security or privacy. Organizations that use third-party providers to manage or process information should also consider these risks and make adequate provisions to mitigate them.

119 UNOCHA, *Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*, OCHA Policy and Studies Series, October 2014: <http://www.unocha.org/node/107049>.

120 Nathaniel A. Raymond and Casey S. Harrity, “Addressing the ‘doctrine gap’: professionalising the use of Information Communication Technologies in humanitarian action”, April 2016: <http://odihpn.org/magazine/addressing-the-doctrine-gap-professionalising-the-use-of-information-communication-technologies-in-humanitarian-action/>.

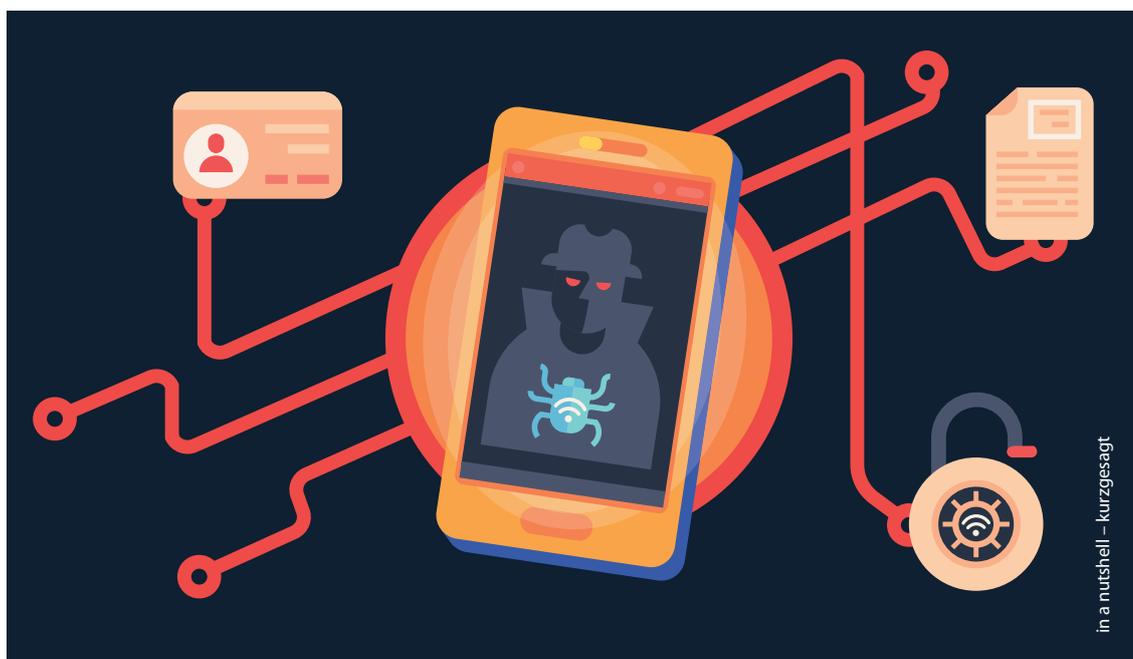
121 BBC, “WhatsApp users to receive adverts”, 25 August 2016: <http://www.bbc.co.uk/news/technology-37184651>; Sean McDonald, “WhatsApp, Trust, & Trusts”, 27 August 2016: <https://medium.com/@McDapper/whatsapp-trust-trusts-980ec18d71b2#.cs9pv6hxp>.

THREATS TO MESSAGING APP USERS' SECURITY AND PRIVACY

Adopting messaging apps introduces a range of additional challenges for humanitarian organizations. This is partly because the companies behind most major apps process and store data using proprietary, opaque systems that external organizations cannot independently scrutinize.

Most major messaging app companies process and store data using proprietary, opaque systems that external organizations cannot independently scrutinize.

This section discusses key areas where more work is needed to establish standards and assess threats associated with messaging apps.



Messaging apps also introduce risks for security, data protection and privacy.

TYPES OF DATA TO CONSIDER

There is continuing discussion over how information can best be shared among humanitarian organizations while protecting individuals' privacy and security. Here, it is important to consider three main types of data:

- **Personally identifiable information (PII)** is data that allows an individual to be identified. It can include information such as an individual's name, age, email address, telephone number or identification number. The use of personal data is also covered by a range of international agreements. The parameters of what constitutes personally identifiable data are continually expanding, as technological advancements make it easier to derive an individual's identity using disparate pieces of information from the wide range of datasets that are now accessible (also known as the "mosaic effect").
- **Community identifiable information (CII)** is data that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic or political.¹²² While this may be helpful for organizations directing their support towards particular groups, it can also help other people or organizations who may wish to target a particular group for political or other reasons.
- **Metadata**, in the present context, is data about the transmission of information on messaging apps. This can include the date and time at which messages or files were sent, the user's location, the identity of the person to whom data was sent, and in some

¹²² As defined in UNOCHA, *Humanitarianism in the Age of Cyber-warfare*: <http://www.unocha.org/node/107049>, p. 6.

cases even the phone's manufacturer and operating system.¹²³ (Note that even where messaging apps use end-to-end encryption for message content, metadata itself is not encrypted in the same way).¹²⁴ Metadata can be used to link an individual with other individuals or groups, or be combined with other datasets to infer details about an individual; studies demonstrate that it is possible to extrapolate information such as health conditions, gun ownership and even literacy from mobile phone metadata.¹²⁵

Moreover, governments or security forces may use metadata to identify and follow individuals or groups: as a former director of the US Central Intelligence Agency (CIA) put it in 2014, "We kill people based on metadata."¹²⁶ In some countries, app companies are required to store metadata for longer time periods than for other forms of content.

POTENTIAL THREATS

Data protection and privacy concerns will arise in every area of a humanitarian organization's work, but humanitarian organizations should consider particular risks when considering whether to deploy a messaging app. Of these, the primary concern is the prospect that unintended third parties access data collected by humanitarian organizations, for purposes that run counter to the neutral, impartial and independent nature of humanitarian work.

These groups could include:

- **Entities in refugees' countries of origin**, who wish to identify groups or individuals for political reasons.
- **Entities with interests in migration or security policy**, who wish to understand and predict migration flows.
- **Governments hosting refugees or IDPs** who wish to identify groups or individuals.
- **Hostile parties** who wish to target or discriminate against some groups of people and the humanitarian organizations supporting them.
- **Business concerns** who wish to profile the behaviour of particular groups, which can lead to discrimination.¹²⁷

In its 2015 Resolution on Privacy and International Humanitarian Action, the International Conference of Privacy and Data Protection Commissioners acknowledged concerns in this regard:

"Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally."¹²⁸

123 For an example of the information that can be gathered about an individual using metadata, see Kai Biermann, "Betrayed by our own data", 20 March 2011, *Die Zeit*: <http://www.zeit.de/datenschutz/malte-spitz-data-retention>.

124 Annex contains detailed breakdowns of metadata collected by a selection of major messaging apps, including information about who users have spoken to at specific times and places.

125 Pål Sundsøy, "Can mobile usage predict illiteracy in a developing country?", *Telenor Group Research*, June 2016: <https://arxiv.org/pdf/1607.01337v1.pdf>; Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, "Evaluating the privacy properties of telephone metadata", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 113 no. 20, pages 5536–5541: <https://doi.org/10.1073/pnas.1508081113>; Yves-Alexandre de Montjoye, Alex "Sandy" Pentland, Laura Radaelli, and Vivek K. Singh, "Unique in the Shopping Mall: Reidentifying credit card data", *Science*, vol. 347, no. 6221, 2015, pages 536–539: <https://doi.org/10.1126/science.1256297>.

126 David Cole, "We Kill People Based on Metadata", *New York Review of Books*, 10 May 2014: <http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/>.

127 Maria Xynou and Chris Walker, "Why we still recommend Signal over WhatsApp," 23 May 2016, <https://securityinabox.org/en/blog/23-05-2016/why-we-still-recommend-signal-over-whatsapp>.

128 International Conference of Data Protection and Privacy Commissioners, *Adopted Resolutions*, 2015: <https://icdppc.org/document-archive/adopted-resolutions/>.

WHAT KIND OF DATA DO MESSAGING APPS COLLECT OR STORE?

Message content: Although some major messaging app companies state that their apps offer end-to-end encryption, meaning that they are unable to decrypt or read the contents of messages, other widely-used apps such as imo and Facebook Messenger store all message content on their servers.

Note that some apps offering end-to-end encryption include it only as an opt-in feature (notably Telegram, LINE and Facebook Messenger). This requires users to be aware of the need to manually enable this feature in their settings, increasing the risk that message content may unwittingly be sent unencrypted. Communication with most bots or bulk messaging features on messaging apps is not end-to-end encrypted.

User information: When users sign up for an app, they are asked to submit information about themselves (ranging from a phone number, in the case of most apps, to full names and email addresses in the case of apps such as WeChat and Facebook Messenger).

Mandatory SIM card registration is enforced in many countries worldwide. In these countries, an app's requirement to submit a phone number may in effect prevent individuals from using messaging apps anonymously. In parts of Latin America, users may also be required to register their handset number.¹²⁹ During sign-up many apps automatically access a user's contacts list to find other contacts who already have the app. In some cases, apps may store this data separately. WhatsApp, for example, confirmed in June 2016 that it stores contact list information.¹³⁰ Details of any messaging groups to which the user belongs may also be stored. Information about a user's network of contacts could be used as evidence against them.

Metadata: Apps collect varying quantities of metadata (see examples in the box below), including sites and information accessed from within the app. Many app companies state that this data is retained on their servers, but rarely explain the length of time that data is retained, or if and how metadata is encrypted. This is the case even among apps which claim to have implemented end-to-end encryption. Although some messaging applications on personal computers offer to hide users' metadata using Tor hidden services (software that enables anonymous browsing),¹³¹ this is not an option on the major messaging apps currently available. Instead, the most privacy-conscious apps currently available simply aim to collect as little metadata as possible.

Messaging apps - user and metadata collection compared¹³²

imo: A user's account creation data, profile information, posted content, contacts, device information, logs of messages, aggregated online activities, location, and chat history.¹³³

Snapchat: A user's Snapchat username, email address, phone number, Snapchat account creation date, "timestamp" and Internet Protocol (IP) address of account logins and logouts, and logs of previous messages sent and received.

Signal: A user's phone number, the time they signed up, and the last time they connected to Signal's server (with the precision of this time limited to the day, rather than the hour, minute and second).¹³⁵

129 GSMA, "Mandatory registration of prepaid SIM cards: Addressing challenges through best practice", April 2016: www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf.

130 Micah Lee, "Battle of the secure messaging apps: How Signal beats WhatsApp", *The Intercept*, 22 June 2016: <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>.

131 All the following options use Tor hidden services (software that is designed to allow anonymous communication): Guardian Project, "What is Orbot?": <https://guardianproject.info/apps/orbot/>; Security in a Box, "Guide to Orbot": <https://securityinabox.org/en/guide/orbot/android/>; Tor Project, "Tor Messenger Beta: Chat over Tor, Easily", 29 October 2015: <https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily/>; Joseph Cox, "Ricochet: the Messenger That Beats Metadata, Passes Security Audit", 17 February 2016: <http://motherboard.vice.com/read/ricochet-encrypted-messenger-tackles-metadata-problem-head-on>.

132 Based on publicly available information from the apps' terms of service at the time of writing.

133 "Aggregated online activities" is likely to denote external internet sites accessed from within the app.

134 Signal, "Grand jury subpoena for Signal user data, Eastern District of Virginia", 4 October 2016: <https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/>.

Data shared with third-party providers: Messaging app companies frequently state that they share users' personal data with other companies which provide services to enable the app to operate. However, they rarely state which companies they work with, what services they provide, what data they have access to, or how that data is processed and stored (see Annex for details).

One interviewee reported starting a project with a third-party provider to send content over a messaging app, but later terminated the agreement after the provider could not produce a privacy policy or explain how they stored data securely.

Evidence that a user has installed an app on their phone: By accessing an individual's physical device or viewing metadata shared by an internet service provider, authorities may find physical evidence that a user has installed a particular messaging app. This could also potentially be accessed through other means: for example, users must associate an email address with their smartphone to download an app, creating a potentially traceable link between the app and other online activity.

HOW COULD OTHER PARTIES ACCESS DATA SHARED ON MESSAGING APPS?

Other parties may be able to access data transmitted through messaging apps in a number of ways, including:

- **A messaging app company (or a third-party provider that accesses app users' personal information) discloses message content or metadata** stored on its servers, in response to a disclosure request from an authority in the jurisdiction where that data is stored.
- **Another party gains unlawful or covert access to message content or metadata** stored on a messaging app company's servers (through hacking), or accesses that information while it is travelling between the two parties (known as a 'man-in-the-middle' attack). For example, tests by the University of Toronto's Citizen Lab in late 2013 indicated that the messaging app LINE was not encrypting content sent over 3G connections despite the fact that content sent over Wi-Fi was encrypted and pointed to speculation that LINE may have done so intentionally to allow the authorities to access message content.¹³⁵
- **Parties access messaging app content through other covert methods.** These include accessing the SMS login codes sent to users when they sign up for an app by redirecting traffic on conventional mobile phone networks, or inducing users to install 'malware' (short for malicious software) onto their phone which enables others to remotely gain access to that phone or data stored on it. To limit the risk of the former type of attack, security experts generally advocate enabling two-factor authentication in the app's settings (see Annex for details on where this feature is available).¹³⁶ It may also be possible for parties to manipulate individuals into disclosing information through "social engineering," often by impersonating a person or organization that the individual trusts.
- **An individual is forced to hand over their physical device.** End-to-end encryption only encrypts data while it is in transit, not on the user's device. If a party gains physical access to a phone or computer with access to a user's messaging app account (such as by compelling the user to unlock it), they may be able to access message content, contacts as well as details of apps that are installed on the device. This could potentially

¹³⁵ 3G networks are encrypted by default, but only at the level of the network provider, meaning that internet service providers (ISPs) and telecommunications companies can decrypt information sent over them. Citizen Lab, *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*, November 2013: <https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/>; Jon Russell, "Thailand's Government Claims It Can Monitor The Country's 30M Line Users": <https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/>.

¹³⁶ Two Factor Auth provides a list of websites and whether or not they support 2FA: <https://twofactorauth.org>.

compromise others' privacy and security. In some countries, the authorities consider merely installing apps such as WhatsApp as an indicator of subversive behaviour.¹³⁷

Governments are reported to have made efforts to unlock access phones in several countries. Signal, Telegram and SnapChat all offer "self-destructing messages," which are only visible on the sender and recipients' phones for a limited time before being automatically deleted. Viber, Signal, LINE and Telegram allow users to set a password that must be submitted in order to view message contents. Note that screenshots of a recipient's conversation can also be collected and shared, irrespective of whether end-to-end encryption is enabled.

- **A messaging app company allows a government to directly access content or data transmitted over the app by building a secret feature into its code (known as a "backdoor").** Other companies have publicly stated that they have refused requests from government agencies to create backdoors,¹³⁸ while many major app companies have publicly stated that they will not include backdoors in their apps' code.¹³⁹

CONSENT

Communicating with communities in humanitarian situations always involves negotiating a range of complex questions, including the following:

- Do individuals need to give a humanitarian organization "permission" to add their details to a group or channel?
- How can an individual opt out of receiving the content? Is this made clear to them at the outset?
- How can people be made aware of who PII or other information is shared with?
- If requests for support that fall outside the humanitarian organization's mandate are shared with another humanitarian agency, are there clear data-sharing protocols to cover this?
- How do people know how long their data will be kept, and for what purposes?
- How can all these issues be communicated in a way that is easy to understand, including for people with limited experience of technology?

Working with messaging apps adds an additional layer of complexity to all these issues.

Some of the data entered into most messaging apps is retained and stored by third parties (messaging app companies), which in turn share some of that data with other parties - whether service providers that enable an app to function, or parent companies (as with Facebook and WhatsApp).

To maintain fully informed consent, humanitarian organizations will need to constantly monitor changes in messaging app companies' terms and conditions, and communicate any changes to the people they are seeking to support.

To maintain fully informed consent, humanitarian organizations will need to constantly monitor changes in messaging app companies' terms and conditions and communicate any changes to the people they are seeking to support.

137 Maria Xynou and Chris Walker, "Why we still recommend Signal over WhatsApp", 23 May 2016: <https://securityinabox.org/en/blog/23-05-2016/why-we-still-recommend-signal-over-whatsapp>.

138 Jon Russell, "Tim Cook Says Apple Won't Create Universal iPhone Backdoor For FBI", 17 February 2016: <https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/>; Max Eddy, "What It's Like When The FBI Asks You To Backdoor Your Software", 8 January 2014: <http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software>.

139 Amnesty International, "For your eyes only: ranking 11 technology companies on encryption and human rights", 17 October 2016: <https://www.amnesty.org/en/documents/POL40/4985/2016/en/>.

Humanitarian organizations may also be unable to confidently state that users can destroy or remove data that they have already submitted because this could entail multiple negotiations with multiple parties (not all of whom are transparent about what data they hold). In these circumstances, organizations seeking to use messaging apps should aim to minimize the amount of information that is submitted to them.

Academic research focused on the US has also found that users of messaging apps are usually unaware of the privacy implications of installing and sharing data on messaging apps.¹⁴⁰ Interviewees frequently said that people regularly provided them with more information over messaging apps than their organization had requested, including names, addresses and contact details. This has also been an issue for news media, as Trushar Barot, (Mobile Editor, BBC World Service) explained:

“There have been some examples where people have sent us content [...] and have said ‘I’m happy for you to use my name’, but we said we’re not going to or we’d anonymize it by just using the first name because we felt that was important, even if they were fine with it. We overrode the safety considerations they may have themselves and made our own judgement.”¹⁴¹

Humanitarian organizations need to conduct detailed research into what data is necessary for their operations, and what risks collecting it might entail.

However, this varied from situation to situation: several interviewees noted that in conflict-affected areas, refugees and IDPs were often cautious about surveillance and careful about what data they disclosed. For example, Refugee Text’s Ciarán Duffy said that individuals were only prepared to submit data about their country of origin after the organization explained exactly why it was necessary to answer their questions about asylum regulations.

Again, this highlights the need for humanitarian organizations to conduct detailed research into what data is necessary for their operations, and what risks collecting it might entail.

Interviewees regularly said that they were looking for clear ways to explain to users how their data would be used, with some expressing particular concerns over potential uses of data for other purposes by organizations such as Facebook.

More work is needed to identify common approaches for communicating this information in an easily comprehensible way. Organizations may also have an opportunity to promote practices among users that help to reduce the amount of data an app collects, such as altering the app’s default settings or communicating clearly what kinds of information should not be shared on the app.¹⁴²

140 Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh and David Wetherall, “A Conundrum of Permissions: Installing Applications on an Android Smartphone”, *Financial Cryptography and Data Security*, Vol. 7398, pp 68-79: http://dx.doi.org/10.1007%2F978-3-642-34638-5_6.

141 Alastair Reid, “How newsrooms can use chat apps and private networks for newsgathering”, 15 November 2015: <https://firstdraftnews.com/how-newsrooms-can-use-chat-apps-and-private-networks-for-newsgathering/>.

142 See, for example, the grugq, “Operational WhatsApp”, 15 April 2016: <https://medium.com/@thegrugq/operational-whatsapp-on-ios-ce9a4231a034#.rsft0ye56>; or Security in a Box, “Guide to Signal”, 23 May 2016: <https://securityinbox.org/en/guide/signal/android>.

Responsible data considerations when using WhatsApp and Facebook Messenger to collect data

Ahead of South Africa's municipal elections in August 2016, the non-profit Africa's Voices Foundation partnered with Livity Africa to evaluate the impact of Voting is Power, a campaign to encourage young people to vote and highlight issues that mattered to them.¹⁴³

To do so, they used online surveys of young people (conducted via email and through WhatsApp and Facebook Messenger) and posts published on social media. WhatsApp and Messenger were selected as channels because of their popularity with young people (476 people were engaged through Facebook Messenger and 46 through WhatsApp).

Africa's Voices Foundation felt that their use of WhatsApp groups encouraged conversations that would yield particularly useful feedback. Impact and Communications Officer Rainbow Wilcox said: "the data that can be gathered [through WhatsApp] is rich, authentic, and provides insights into socio-cultural beliefs and behaviours."

However, Africa's Voices had concerns about privacy when using both Facebook Messenger and WhatsApp. "We sought informed consent and stored the data securely, but we cannot control how the data will be used in these platforms," Lopes said. "It was problematic because we asked for personal information such as voting and demographics. We have decided not to embark on a [similar] project again if the privacy risks are not well understood before it starts."

MESSAGING APP FEATURES RELATED TO PRIVACY AND SECURITY

The following are relevant features to look for when choosing a messaging app to exchange information in humanitarian crises:

1. Anonymity permitted/no requirement for authenticated identity

Enabling users to communicate anonymously via a messaging app enhances their privacy, whereas requiring the use of real names, email addresses and authenticated identities increases the risk that individuals will be monitored or targeted. The less information a user is required to provide in order to use an app, the less information about them other parties may be able to access. Because most apps require a user's account to be linked to a telephone number, users' anonymity could be enhanced by creating an account using a SIM card that is then disposed of.

2. No retention of message content

User privacy is better served when the contents of messages are delivered to a user's device and deleted from the app company's servers after they are read. Apps such as Telegram, WhatsApp, Viber and Signal state that they delete message content from their servers immediately after the intended recipient has accessed it. However, humanitarian organizations should be aware that they may not be able to independently verify these claims. Companies such as Skype and Facebook Messenger retain message content on their servers after the user has read the message, without stating a maximum time limit after which they will delete the data.

3. End-to-end encryption

End-to-end encryption restricts the ability of third parties to intercept communications between humanitarian organizations and their beneficiaries in a way that allows the message contents to be viewed. Even if a company does retain content data, it will be in encrypted form and thus not legible to the company or to any third party seeking access

143 Africa's Voices, "Case Study: Livity South Africa": <http://www.africasvoices.org/case-studies/livity-south-africa/>.

to it. Encryption thus restricts the type and amount of legible data that messaging-app companies can be compelled to disclose. Ideally, it should be deployed by default in both one-to-one and group chats.

Some encryption protocols are considered by security experts to be stronger than others: for example, Telegram has been criticized for developing its own protocol rather than using the existing Signal protocol, which experts generally regard as among the strongest currently available.

At the time of writing the Electronic Frontier Foundation was updating its Secure Messaging Scorecard, which assesses levels of security offered by specific apps. The Scorecard and media sources should be monitored for updates.¹⁴⁴

4. User ownership of data

It is essential that messaging-app users be regarded as the lawful owners of their personally identifiable data as well as the contents of their messages. This prevents messaging-app companies from using such data for commercial or other initiatives without the explicit consent of the user. This issue is addressed by national law in some countries, and the topic may also be included in the messaging apps' terms-of-service agreements.

5. No or minimal retention of metadata

The less metadata messaging apps retain on their servers, the less data they can be compelled to disclose to governments or sell to commercial interests. Messaging apps such as Signal and Telegram claim not to retain any metadata on their users, though Telegram's claim has been contested¹⁴⁵, whereas most major apps under consideration state that they collect contact numbers, logs of activity on the app and location information (see Annex for details).

6. Messaging-app code is open source

When the code which underpins a messaging app is open source, the app can be independently scrutinized to verify that it has no vulnerabilities to security threats or hidden surveillance functions such as backdoors.¹⁴⁶ Ideally, an app will publish its entire codebase openly. Messaging apps such as Signal and Wire are entirely open source, while apps such as Telegram and Threema publish only part of their code.¹⁴⁷

7. The app company rigorously vets disclosure requests from law enforcement

It is critical that the company producing the messaging app rigorously vets and responds in a restrained manner to law-enforcement requests for user data. Ideally, they will provide information on their own behaviour in this regard, publishing regularly updated transparency reports that provide details about what requests they have received from which jurisdictions, and what types of information they have provided.

At the time of writing, Microsoft¹⁴⁸ and Facebook¹⁴⁹ publish regular transparency reports that detail how many requests they receive and how much data they hand over to law-enforcement agencies, while Open Whisper Systems (the company behind Signal) provides more detailed descriptions of the requests they receive.¹⁵⁰

144 Electronic Frontier Foundation, "Secure Messaging Scorecard": <https://www.eff.org/secure-messaging-scorecard>. See Annex for basic details on the encryption protocols used by the various messaging apps.

145 Jeremy Seth Davis, "Telegram metadata allows for 'stalking anyone'", 30 July 2015: <http://www.scmagazine.com/telegram-metadata-allows-for-stalking-anyone/article/456484/>.

146 See, for example, Darren Pauli, "'Trust it': Results of Signal's first formal crypto analysis are in", 8 November 2016: http://www.theregister.co.uk/2016/11/08/trust_it_results_of_signals_first_formal_crypto_analysis_are_in/?mt=1478607335044.

147 <https://wire.com/>; <https://threema.ch/en/>; For more on this topic, see Lorenzo Franceschi-Bicchieri, "Wickr: Can the Snapchat for Grown-Ups Save You From Spies?", 4 March 2013: <http://mashable.com/2013/03/04/wickr/#3EwYsDKZ5kqh>.

148 Microsoft Transparency Hub: <https://www.microsoft.com/about/csr/transparencyhub/>.

149 Facebook, Government Requests to Facebook: <https://govtrequests.facebook.com/about/>.

150 Open Whisper Systems, "Big Brother": <https://whispersystems.org/bigbrother>.

8. No sharing of personally identifiable information or community identifiable information with third parties

Although messaging apps will need to share some data with third parties (typically information playing a technical role in data processing) to facilitate the delivery of their services, it is critical that companies do not share personally identifiable or community identifiable data and only share data that has been minimally de-identified when this is strictly necessary. Organizations should choose a messaging app that does not share any data with third parties other than that which is strictly necessary for the technical operation of the service - and seek to confirm this explicitly with companies before proceeding.

9. Companies not domiciled in a country with broad surveillance powers

A final critical feature of a privacy-protecting messaging app is that data collected by the app is stored in a country where the government does not have broad surveillance powers or a record of regularly flouting legal restraints on surveillance.¹⁵¹ Note that a company may also store the data that it collects in a data centre outside the country in which it is domiciled.

The table below provides a brief overview of the extent to which a subset of the most popular messaging apps claim to embody the privacy-friendly features listed above.¹⁵² It is based on publicly available statements and the apps' terms of service (TOS) documents, and has not been independently verified. Annex contains more details on the information in these categories.

151 Useful sources for further research include: <https://www.digcit.org/>; <https://privacyinternational.org/global-advocacy>; <https://advox.globalvoices.org/>; and <https://www.eff.org/deeplinks>.

152 The inclusion of specific messaging apps in this list does not imply an endorsement of these apps, or suggest that they are the only apps suitable for use in humanitarian situations. They are included here because publicly available usage data indicates that they are the most frequently used in countries in which the ICRC works. See Annex for more details.

PRIVACY-FRIENDLY FEATURES OF MESSAGING APPS

WhatsApp	Viber	Signal	Telegram	LINE	Facebook Messenger	Snapchat	FireChat	Skype	imo	WeChat
Does the app ask the user to submit their real name to use the service?										
YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	NO
Is message content retained by the app company after a message has been delivered?										
NO	NO	NO	NO	NO	YES	NO	NO	YES	YES	Partially*
Does the app offer claim to offer end-to-end encryption for group chats?*										
YES by default	YES by default	YES by default	YES opt-in	YES opt-in	NO	NO	YES by default	NO	NO	NO
Does the app claim to offer end-to-end encryption for one-to-one chats?*										
YES by default	YES by default	YES by default	YES opt-in	YES by default	YES opt-in	NO	YES by default	NO	NO	NO
Does the user have ownership rights over data they submit using the app?***										
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Does the app retain metadata collected while the app is used?										
YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES
Is the app's code open source?										
NO	NO	YES	Partially****	NO	NO	NO	NO	NO	NO	NO
Does the company publish reports on requests from law enforcement for user data?										
YES	NO	YES	NO	NO	YES	YES	Unknown	YES	Unknown	Unknown
Does the app share data with any third parties?										
YES	YES	NO	NO	YES	YES	YES	YES	YES	YES	YES
Where is the app company domiciled?										
US	Israel	US	Germany	Japan	US	US	US	US	US	China

HEIGHTENED LEVEL OF RISK.

* Shared message content is retained.

** Note: this report has not independently audited the implementation of end-to-end encryption. The Electronic Frontier Foundation's Secure Messaging Scorecard (currently under revision) aims to provide a more detailed assessment of these claims: <https://www.eff.org/secure-messaging-scorecard>.

*** This row is based on statements in the apps' terms of service. Some apps, such as Facebook Messenger, state that user data may be analysed or shared with others for advertising purposes.

**** Telegram's code for its clients (such as its Android and iOS apps) is open source, but its "server-side" code is not. Telegram states that it may publish this code openly in future, but has not provided a more detailed timeline.

OPERATIONAL CONSIDERATIONS

GOVERNMENT RESTRICTIONS ON MESSAGING APP USAGE

Content transmitted on messaging apps is increasingly becoming subject to government controls or censorship, limiting the extent to which individuals can communicate freely and openly (including with humanitarian organizations).

Freedom House's *Freedom on the Net 2016* report indicates that in 2016, messaging apps became the communications tools most routinely targeted by governments in the 65 countries they assessed.¹⁵³

Content transmitted on messaging apps is increasingly becoming subject to government controls or censorship, limiting the extent to which individuals can communicate freely and openly, including with humanitarian organizations.

BLOCKING OF APPS OR MOBILE INTERNET

Governments across the world have demonstrated that they are prepared to ban specific apps or shut down mobile-internet connections¹⁵⁴. If a humanitarian organization relies on a specific app, it will be exposed to the risk that that app could become unusable at a crucial point during a crisis.

Governments across the world have demonstrated that they are prepared to ban specific apps or shut down mobile-internet connections.

MANAGING AND ANALYSING DATA

Some interviewees indicated that processing the data collected through messaging apps was a challenge. Greater numbers of people can now collect and share larger volumes of data with organizations, but this means the organizations need to ensure they have the capacity to deal with it.

Processing the data collected through messaging apps can be challenging. Organizations need to ensure they have the capacity to deal with this data, and to integrate it within existing information management systems.

Interviewees frequently described difficulties in creating a workflow to manage and analyse the information received. Several noted that the systems used by messaging apps were not interoperable with existing information management systems or databases; three interviewees described manually transcribing individual messages into spreadsheets to allow them to analyse data in a way that would allow for effective decision-making.

For example, when working with WhatsApp, Africa's Voices Foundation (AVF) had to extract data in an unstructured format, with staff then linking users' answers to the questions AVF had initially asked using a set of heuristic rules. Claudia Abreu Lopes, Head of Research and Innovation, noted: "We had to do exhaustive manual checks and creative data wrangling to be confident about the quality of the dataset [on users' views]."

Because interactions over messaging apps may be more conversational in tone (see Section 3), interviewees noted that humanitarian organizations may also receive information that is in a different format to what has been requested. For example, the spontaneous nature of the WhatsApp group set up by Africa's Voices Foundation meant that people also responded with other information, such as questions about the organization, or photos of polling stations, to which staff responded on an ad hoc basis where possible.

¹⁵³ Sanja Kelly, Mai Truong, Adrian Shahbaz and Madeline Earp, "Freedom on the Net 2016: Silencing the Messenger - Messaging apps under pressure", November 2016: <https://freedomhouse.org/report/freedom-net/freedom-net-2016>.

¹⁵⁴ Recent reports have identified 81 short-term internet shutdowns in 19 different countries over the last year - see Darrell M. West, "Internet shutdowns cost countries \$2.4 billion last year", 6 October 2016: <https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/>; Thomas Carothers, *Closing Space: Democracy and Human Rights Support Under Fire*, Carnegie Endowment, 2014: <http://carnegieendowment.org/2014/02/20/closing-space-democracy-and-human-rights-support-under-fire-pub-54503>.

Although this may be achievable in smaller groups (Africa's Voices' WhatsApp group contained 56 users), it entails a significant investment in staff time. As Rainbow Wilcox of Africa's Voices cautioned: "It can be difficult to curate conversations - they can take on a life of their own." From the outset, organizations which allow spontaneous conversations through apps should prepare to manage users' expectations about the level of response that they can provide. In cases where organizations used messaging apps for internal communication, interviewees often said that it was crucial to give at least one person in each group responsibility for moderating conversations, to ensure that they remained focused.

Verifying data

Interviewees also described challenges with regard to verifying information received through messaging apps. While this is an issue in many online channels,¹⁵⁵ verifying content from messaging apps is made more challenging by the speed at which information can be sent, as well as by message volume and the range of data types that can be sent.

News media and human rights bodies have attempted to respond to these challenges through collaboration and efforts to produce resources and guidance. Some of these resources may also be useful to humanitarian organizations.¹⁵⁶ Nonetheless, verification requires substantial time and effort, and as a result is likely to become a core activity for any humanitarian organization that chooses to adopt messaging apps.

Rumours and misinformation can spread rapidly on messaging apps, in part because information is usually shared in closed groups that are based on peer-to-peer trust.¹⁵⁷ This poses a challenge to humanitarian organizations. However, there is increasing recognition that monitoring rumours and misinformation can help organizations direct their efforts more effectively. For example, Internews' Anahi Ayala suggests that it could help to predict trends such as the displacement of large numbers of people in response to rumours or threats, and increase understanding of popular perceptions of humanitarian agencies' activities.

Some humanitarian organizations invest time and effort in debunking rumours.¹⁵⁸ For example, during the Ebola crisis in Liberia, the Health Communication Capacity Collaborative initiative created a weekly newsletter to debunk rumours collected from sources including radio stations and health workers, and then trained journalists on how to respond to these claims.¹⁵⁹

Messaging apps are another potential channel that may need to be monitored in these circumstances. However, if humanitarian organizations distribute information collected through messaging apps without also ensuring that they have the capacity to validate and verify it, they could risk losing the trust of the communities they work with. In conflict-affected areas, this is an ever-present risk.¹⁶⁰

In some cases, messaging apps introduce specific technical challenges for verification efforts. As one interviewee put it, describing the situation in a conflict-affected area: "The way that sources favour transferring information is often through [messaging apps] that by default strip out some of the [metadata] that's helpful for verification, and obviously that complicates things substantially." For example, while not collecting geolocation data with

Verifying content is already an issue in many online channels; using information from messaging apps is made even more challenging by the speed at which information can be sent, by the volumes of messages and the range of data types that can be sent.

155 The Engine Room, "Verification of social media: The case of UNHCR on Twitter": <https://responsibledata.io/reflection-stories/social-media-verification/>.

156 See, for example, Craig Silverman (ed.), *The Verification Handbook*, European Journalism Centre: <http://verificationhandbook.com/>; Various authors, *DatNav: New Guide to navigate and integrate digital data in human rights research*, Amnesty International, The Engine Room and Benetech, 2016: <https://www.theengineroom.org/datnav-digital-data-in-human-rights-research/>; First Draft News Partner Network: <https://firstdraftnews.com/partners-network/>.

157 Anahi Ayala, "The Dichotomy of Technology in Conflict: Beauty and the Beast", in Raquel Vazquez Llorente and Imogen Wall (eds.) "Communications technology and humanitarian delivery: challenges and opportunities for security risk management", 2014, European Interagency Security Forum (EISF): <https://www.eisf.eu/library/communications-technology-and-security-risk-management/>.

158 See Internews' "News that Moves" project: <https://newsthatmoves.org/>.

159 Beatrice M. Spadacini, "Tracking Rumors to Contain Disease: The Case of DeySay in Liberia's Ebola Outbreak", 22 September 2016: <https://blog.usaid.gov/2016/09/tracking-rumors-to-contain-disease-the-case-of-deysay-in-liberias-ebola-outbreak/>.

160 Jacobo Quintanilla, "Ten lessons on communicating with communities in complex emergencies", 23 October 2015: <http://odihpn.org/blog/ten-lessons-on-communicating-with-communities-in-complex-emergencies>.

incident reports may help protect users' privacy, it may also make those reports considerably more difficult for organizations to verify.¹⁶¹

Organizations will have to balance the imperatives of protecting individuals' privacy and collecting data that is accurate and actionable, on the basis of an assessment of the risks that apply in that context.

Bias in data collected through messaging apps

Relying on data gathered solely through one app risks introducing statistical bias into analyses of a particular issue. Differences in individuals' access to the internet or to mobile phones could affect the way that different populations are represented, with conclusions based on this skewed data potentially reinforcing inequalities.

This phenomenon could also exacerbate blind spots: for example, incident reports collected through messaging-app data might give the impression that violence was concentrated in a particular part of a country, without taking account of network outages or limited internet access in other parts of the country.

Decisions taken during the design of interactions with messaging apps can also exacerbate biases - for example, by failing to account for the fact that in some situations, women may not be able to access or submit data over a messaging app without the approval of a man in their household. For this reason, some interviewees described deliberate decisions to avoid messaging apps, instead using bespoke apps that included elements such as a requirement to sign in every time they used the service.

A comprehensive breakdown of similar challenges and processes for mitigating them is beyond the scope of this report; for an introduction, see the Human Rights Data Analysis Group's outline of the key elements that can lead to inaccuracies when using data (including data collected in conflict-affected environments).¹⁶²

Differences in individuals' access to the internet or to mobile phones could affect the way that different populations are represented, with conclusions based on this skewed data potentially reinforcing inequalities.

161 Timo Luege, *Lessons Learned: Social Media Monitoring during Humanitarian Crises*, Assessment Capacities Project, 2015: <http://www.alnap.org/resource/21232>.

162 Human Rights Data Analysis Group, "Core Concepts": <https://hrdag.org/coreconcepts/>.



A. Zavalllis/UNHCR

A group of Syrian refugees takes a selfie moments after crossing the Aegean sea from Turkey in an inflatable plastic boat.

5. RECOMMENDATIONS

Messaging apps are likely to continue to pose responsible data challenges related to privacy, data protection, digital security and consent as companies add new features and more people begin to use them. The onus will be on humanitarian organizations to take active steps to recognize their duty of care towards the people they seek to protect and assist.

Messaging apps are becoming the primary mode of communication for many people around the world, including many members of communities facing humanitarian crises. As such, these apps deserve to be considered along with other communications channels by humanitarian organizations. Given rising rates of smartphone ownership and messaging-app usage, it is abundantly clear that messaging apps are here to stay.

Messaging apps will not be appropriate in every humanitarian situation. As with any technology, they can exacerbate inequalities associated with gender, age, literacy and experience with technology, as well as access to energy, mobile phones and network connectivity. Humanitarian organizations should therefore consider who messaging apps do not reach. Nonetheless, in some situations they offer a way of contacting individuals who might otherwise be impossible to reach, and a means of sharing information that would otherwise be inaccessible.

Messaging apps are a new, rapidly evolving technology. More work is needed in order to understand their potential effects, and establish community standards for using them effectively and responsibly. Humanitarian organizations must ask questions such as if and how data transmitted by the apps can be responsibly retained or analysed; what consent procedures are both appropriate and practical; and how to assess threats that arise from use of the apps.

Fundamentally, it is crucial that humanitarian organizations start from a clear understanding of the local information ecosystem in order to know, specifically, why a messaging app may be useful in that particular context and why information exchanged through a messaging app may be a safe and effective way of collecting or sharing that information.¹⁶³

Messaging apps are likely to continue to pose responsible data challenges related to privacy, data protection, digital security and consent as they add new features and more people start to use them.¹⁶⁴ The onus will be on humanitarian organizations to take active steps to recognize their duty of care towards the people they seek to protect and assist. They must also ensure that the approaches they adopt when using and engaging with messaging apps respect users' rights to consent, privacy, security and ownership.

GENERAL PRINCIPLES

Research for this project has shown that some organizations already deem the benefits associated with messaging apps to outweigh the potential concerns. Those organizations, and others considering whether to integrate these apps into their own communications strategies, should keep the following recommendations in mind:

- **Invest the time and effort needed to understand the local information ecosystem.** Before adopting any new technology, organizations should learn how the people they want to reach communicate and which channels they use and trust. The way in which people communicate may also vary significantly across different environments and cultures; moreover, there may be changes in people's information needs and the channels they have access to over time. Organizations should consult with local communities regularly and take time to learn from them before making any project design decisions – local residents are the true communication experts.
- **At a minimum, humanitarian organizations need to systematically include questions on access to and use of mobile telephony into humanitarian needs assessments.** Historically, humanitarian organizations have asked affected people what they need, but

¹⁶³ Nathaniel A. Raymond and Casey S. Harrity, "Addressing the 'doctrine gap': professionalising the use of Information Communication Technologies in humanitarian action", April 2016: <http://odihpn.org/magazine/addressing-the-doctrine-gap-professionalising-the-use-of-information-communication-technologies-in-humanitarian-action/>.

¹⁶⁴ For more information and resources, see the Responsible Data Forum, a collaborative effort to develop useful tools and strategies for dealing with the ethical, security and privacy challenges that includes an active mailing list of practitioners discussing these questions: <https://responsibledata.io>.

rarely what they need and want to *know*, how they access information, and what channels they use and trust. Although this is starting to change, failing to ask such questions can result in assumptions that can significantly limit organizations' effectiveness and overall accountability to people affected by crises.

- **Use a range of communications channels rather than relying exclusively on a messaging app.** Organizations should ensure that messaging apps are part of a multi-platform, multi-channel communications strategy rooted in a deep understanding of the local information ecosystem. Efforts should be made to craft this strategy to enable vulnerable groups to access information in ways appropriate to their skills or resources, ensuring that individuals are not discriminated against as a result of their gender, age or abilities.
- **Remember that technology is only the start - building trust with the community is hard.** When it comes to messaging apps and other communication platforms, simply deploying and learning how to use the technology itself can be the easy part. It is much more difficult to build a relationship of trust that translates into a strong relationship with local communities. People will judge humanitarian organizations on the basis of the quality of their engagement, as well as their ability to listen, deliver what is needed and (when necessary) change the way they operate.
- **Don't let the technology distract from the need for appropriate local content.** Technology and connectivity alone are not enough to produce beneficial change in people's lives. Humanitarian organizations using messaging apps will have very limited impact if they don't also invest in providing timely, actionable and useful content tailored for people locally. Moreover, managing and analysing the data received through the apps is necessary to ensure that the information provided by target communities genuinely helps to guide an organization's future activities.
- **Establish feedback mechanisms with all key stakeholders.** Humanitarian organizations should build in flexibility to allow for corrections following feedback from respondents to improve the use of messaging apps; they should also prioritize higher levels of local content and relevance. Suggestions from users on how the app can best serve their needs should be built into implementation on an ongoing and iterative basis.
- **Plan well in advance:** as far as possible, put in place strategies and processes for using messaging apps well before they are actually needed in a humanitarian situation. This might mean building up systems for managing data or developing policies and training field staff in how to implement these policies.

PRIVACY, SECURITY AND DATA PROTECTION

- **Prioritize the privacy rights of respondents when choosing a messaging app.** Organizations should investigate the privacy risks associated with using messaging apps to communicate with vulnerable individuals and communities, and should take all possible steps to mitigate those risks. This includes choosing messaging apps with end-to-end encryption enabled by default, run by companies which collect and retain minimal amounts of data, and which have a strong record of resisting unlawful demands for private data from law-enforcement and other agencies.
- **Collect as little data as needed to conduct essential operations (both message content and message metadata), and emphasize to users that any data they submit remains insecure.** Even apps that include end-to-end encryption collect other data about their users that could expose individuals to risks in some contexts. Organizations should conduct a risk assessment to gain a better understanding of what data is being collected, and what the worst-case scenarios could be as a result. As a general principle, organizations should encourage individuals to remember that any information submitted over a communications network may be viewed by an adversary at some point in the future.

- **Ensure that your organization has and complies with a data protection or responsible data policy.** All data collected, generated and stored by humanitarian agencies is incredibly sensitive and should be given the strongest possible protection. As organizations adopt new technologies and adjust their working practices accordingly, taking a broader look at the challenges this brings through establishing a Responsible Data Policy may also help to proactively address the related issues of consent, data protection, ethical obligations and privacy rights. On the data protection front, the ICRC and UNHCR are examples of organizations which are currently in the process of shoring up their data-protection policies and systems and can provide guidance to smaller organizations wishing to do the same. Organizations like Oxfam¹⁶⁵, Mercy Corps¹⁶⁶ and Médecins Sans Frontières¹⁶⁷ have all taken a rights-based, Responsible Data approach to dealing with these challenges.

IMPLEMENTATION

- **Test, test and test again.** Interviewees repeatedly emphasized that approaches which are effective in some regions will fail in others. One organization described communications initiatives which had been launched with usage assumptions taken from a Western context, but without any of the funding needed to adapt the initiatives when they proved inappropriate for the intended local situation. Organizations should thus conduct thorough research into key factors that affect accessibility and the use of the app among local people before introducing it. Following the launch, organizations should use analytics tools to monitor usage patterns, support local dialects wherever possible, consider ways to promote usage among women and older people, and factor in the needs of those who may be inexperienced with these tools.
- **In urban areas, consider network connectivity as a basic urban service that needs to be restored.** Network connectivity certainly cannot solve all problems in conflict areas or urban settings damaged by conflicts or disasters. When first responders help to restore connectivity, this can enable people to reconnect with community members, diaspora groups, their government, the media and humanitarian organizations. Moreover, this can allow local communities to start organizing their own responses to a crisis in a faster and better way. The specifics of re-establishing or providing connectivity and sufficient electric power to charge mobile phones will inevitably differ between situations, but mobile-network operators and the private sector will almost inevitably play an important role.¹⁶⁸

COLLABORATION WITH LOCAL MEDIA AND OTHER PARTNERS

- **Work with local media to promote humanitarian services and tailor messages through and beyond messaging apps.** Local media have enormous potential to provide people with relevant, trusted and timely information, particularly when people need such information most urgently. Moreover, media organizations can demand accountability from local governments and humanitarian organizations. Representatives of initiatives seeking to communicate with communities in crisis situations have reported that people

165 Oxfam, "Responsible Program Data Policy": <http://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950>.

166 Electronic Cash Transfer Learning Action Network, "A Data Starter Kit for Humanitarian Field Staff": <http://elan.cashlearning.org/>.

167 The Engine Room, "Médecins Sans Frontières case study": <https://www.theengineroom.org/projects/msf-responsible-data/>.

168 Following two years of industry consultation, the GSM Association (GSMA, a trade association representing mobile-network operators around the world) launched the Humanitarian Connectivity Charter in March 2015 to support mobile-network operators in improving network preparedness and resilience. The Charter consists of a set of shared principles adopted by key players in the mobile industry to support improved access to communication and information for those affected by crisis, with the aim of reducing loss of life and positively contributing to humanitarian responses. The Charter is supported by the UN Office for the Coordination of Humanitarian Affairs (UNOCHA), the UN Emergency Telecommunications Cluster (ETC), the IFRC and the ICRC: www.gsma.com/mobilefordevelopment/programmes/disaster-response/humanitarian-connectivity-charter.

become frustrated when communication efforts fail to provide locally relevant, actionable information.¹⁶⁹

Organizations should thus consider collaborating with local media to promote their humanitarian services, including through the publication of relevant messaging-app numbers.¹⁷⁰

Additionally – and crucially – local media can help organizations tailor their messaging to be more effective and establish two-way communication and dialogue through participating in interactive programming (not just facilitating the broadcasting of messages), while also providing links to existing on-the-ground networks that may be able to provide in-person support.¹⁷¹

PRACTICAL CONSIDERATIONS

- **Develop a workflow and an information-management system.** Consider carefully how the information gathered through a messaging app will be used to inform operational decision-making. More data does not necessarily lead to better decisions. Messaging apps can introduce large quantities of new information and data from many different sources. Without proper planning, this could overwhelm organizations, increase the risk that organizations fail to respect users' privacy,¹⁷² and frustrate members of local communities who may not find their questions, feedback or complaints addressed. Third-party providers offering applications which can access an app's features and data may be able to assist with data analysis or management, but introduce a further set of risks around data protection and users' privacy that organizations should consider carefully before proceeding.
- **Consider how the organization will verify and validate information received.** The speed of peer-to-peer information exchange exacerbates the danger of spreading misinformation. However, information verification requires time and resources, and can end up being a core function for any humanitarian organization choosing to utilize messaging apps. Organizations will thus need to offset the time spent in verifying information against the potential benefits associated with rapid communication or, indeed, invest more resources in verification than initially planned.
- **Consider collaborating directly with messaging-app companies.** As more research findings and pilot projects demonstrate the potential of messaging apps to support humanitarian initiatives, the humanitarian community should consider approaching selected messaging-app companies to propose practical collaborations or partnerships. It is important to bear in mind that for-profit companies who develop messaging apps may have different priorities to those of humanitarian organizations. These need to be discussed and clearly communicated at the outset to develop strong working relationships. If humanitarian organizations seek to work collectively, rather than individually and separately, direct collaboration with the app developers could be of greater benefit to all the parties.

169 BBC Media Action, *Humanitarian Broadcasting in Emergencies: A Synthesis of Evaluation Findings*, 2015: www.cdacnetwork.org/tools-and-resources/i/20151006113456-dir49.

170 See Internews, *Reporting on Humanitarian Crises: A Manual for Trainers & Journalists and an Introduction for Humanitarian Workers*, 2014: <http://www.internews.org/research-publications/reporting-humanitarian-crises-manual-trainers-journalists-and-introduction>, and BBC Media Action iLearn website, containing resources related to "Lifeline programming", 2016, or its special broadcasting for audiences in emergencies. Among those resources, there is a Guide with tips for aid workers on working with media to save lives: <https://www.bbcmediaactionilearn.com/course/view.php?id=187>.

171 Rose Foran, "The refugee crisis will not be hacked", 29 July 2016: <http://news.trust.org/item/20160729132618-0oczq/>.

172 For an excellent overview of roles and strategies to mitigate this (in the context of SMS campaigns, see Frontline SMS's section on Human Participation in their "User Guide on Data Integrity", p.51: <http://www.frontlinesms.com/impact-of-frontline/guides-tools-and-case-studies/>).



G. Makkas/Panos

Ramia Sabbagh from Aleppo, Syria, checks her phone at the disused freight platform of Idomeni railway station, Greece.

ANNEX

**WHAT KIND OF
MESSAGING APPS
ARE AVAILABLE,
AND WHAT ARE
THE KEY DIFFERENCES
BETWEEN THEM?**

This annex examines features offered by ten messaging apps: Facebook Messenger, imo, LINE, Skype, Snapchat, Telegram, Viber, WhatsApp, Signal and FireChat.

Selection of apps

The inclusion of specific messaging apps in this list does not imply an endorsement of these apps or suggest that they are the only apps suitable for use in humanitarian situations. Rather, they were included because publicly available usage data indicates that they are the most frequently used in countries where the International Committee of the Red Cross's most important operations were underway at the time of writing: Afghanistan, Iraq, the Lake Chad region, Somalia, South Sudan, Syria, Ukraine and Yemen.

Two others (Signal and FireChat) were included because they offer specific features of interest to the ICRC that were not available elsewhere. Various other messaging apps also offer similar features,¹⁷³ but are not included here for reasons of time and space.

The information in this annex is based on information that was publicly available at the time of writing. Wherever possible, it was shared with app companies for comment before publication.

The list here does not attempt to rank apps against each other or recommend specific apps as appropriate in all situations. An organization should decide which app is appropriate on the basis of a practical assessment of its needs, and (if possible) in conversation with the app company itself.¹⁷⁴

N.B. It is important that humanitarian organizations understand that messaging apps evolve rapidly. Please note that the information contained in the tables below was accurate at the time of writing, but some apps' key functionalities and other features may have changed since then.

173 For example, see Wire (<https://wire.com>), KakaoTalk (<http://www.kakao.com/talk>), YikYak (<http://yikyak.com>), Zalo (<http://zalo.me>) and Threema (<https://threema.ch>).

174 Sean McDonald, "Ranking the 6 Problems with ICT4D Product Rankings", 6 October 2016: <http://www.ictworks.org/2016/10/06/ranking-6-problems-with-ict4d-product-rankings/>.

Key functionalities

	Voice calls	Voice messages	Photo messages	Bots	Location sharing	Video messages	File sharing	Video calls
WhatsApp	YES	YES	YES	NO	YES	YES	Up to 160 MB	NO
Viber	YES	YES	YES	NO	YES	YES	YES	YES
Signal	YES	YES	YES	NO	YES	NO	NO	NO
Telegram	NO	YES	YES	YES	YES	YES	files of up to 1.5 GB	NO
LINE	YES	NO	NO	YES	NO	NO	NO	NO
Facebook Messenger	YES	YES	YES	YES	YES	YES	Through an integration with Dropbox	YES
Snapchat	YES	NO	YES	NO	NO	YES	NO	YES
FireChat	NO	YES	YES	NO	YES	YES	Yes (limits unknown)	NO
Skype	YES	YES	YES	YES	NO	YES	300MB size limit	YES
imo	YES	NO	YES	NO	NO	YES	NO	YES
WeChat	YES	YES	YES	YES	YES	NO	NO	YES

OPERATIONAL CONSIDERATIONS

REGISTRATION

All apps require users to download and install them from an online store. To use these stores, users must have an email address registered either with Google (for phones using the Android operating system) or Apple (for phones using iOS).

CONNECTING WITH USERS

All apps discussed in this report require both participants in an exchange or conversation to have downloaded and installed the same app. For most of these apps, the phone number serves as the user's identifier. Most apps then automatically add contacts using the mobile-phone numbers stored in the user's phone book.

Many apps, including WeChat, LINE, Viber, Facebook Messenger, Skype, imo, Snapchat and FireChat, also allow users to set up an account with a username (which can be a pseudonym) that others can then add as a contact. WhatsApp and Signal are exceptions to this and require use of the account holder's phone number. By contrast, Skype and Facebook Messenger do not require a phone number to participate (though they do encourage users to provide a phone number in the setup process). WeChat is starting to offer multi-platform accounts without reference to a phone number.

SENDING MESSAGES TO LARGE NUMBERS OF PEOPLE

Apps typically allow a user to communicate with large numbers of people in two ways:

- **By setting up a group based on users' phone numbers.** This method either uses existing contacts from the group creator's phone book, or numbers that are submitted directly by potential group members.

In most cases, numbers need to be added manually, with the user then consenting to be added to the group. WhatsApp and Signal only allow groups to be created in this way. Most apps place limits on the number of participants in a group, with upper bounds ranging from 20 to 500 (see table below). WhatsApp currently has a maximum group size of 256 members; many interviewees described setting up multiple groups to get around this restriction.

- **By setting up a channel, account or page that users actively subscribe to.** In this case, there is no need to use phone-book contacts or a phone number. Users cannot be added by the humanitarian organization itself - they have to actively initiate the connection.

This is possible through various methods. For example, they can visit a specific URL, scan a quick response (QR) code with their phone, or respond to an invite via email, SMS or the app itself. App services offering this capability include WhatsApp's Broadcast Lists, Telegram's Channels and Viber's Public Chats; Snapchat only allows broadcast or bulk communication (through its "Stories" feature) to be initiated in this way. In most cases, conversations with bots require a user to initiate an interaction (for example, by sending a message to the bot's "account").

Viber, Telegram, WeChat, FireChat, LINE and imo all allow groups to be set up using either of these methods.

Operational features for connecting with groups

Requirements for users communicating using the app	Method of adding contact	Communication with large numbers of people	Maximum number in group	Alternative platforms for non-mobile use available?
WhatsApp				
All users must have the app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	Add user's phone number to the mobile phone's address book. If the contact has WhatsApp installed, they will appear in the contacts tab in the app (if not, they will be invited to download the app).	<p>The Broadcast List feature can be used to contact a large group of people without letting them see who else has been contacted. Replies to Broadcast List messages will only be received by the list administrator. To receive a message from a Broadcast List, the list owner must have the sender's phone number saved in their address book.</p> <p>Group chats can be used where individuals wish to permit other group members to see information that they have submitted. This requires an invitation to the group chat by a group administrator (users' phone numbers must be in the group admin's contacts.)</p>	256 for both groups and broadcast lists	Windows 8 and up, OS X 10.9 and higher, or a browser app for browsers such as Chrome.
Viber				
All users have to create an account and have the app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	Add a phone number to the mobile phone's address book or through the app, it is also possible to add people by having them scan a QR code that the app generates.	Public chats allows users to set up a group chat with up to 200 people; the message content of that group is public for any Viber user to see.	200	Windows 10 and Windows phone, OS X, Linux
Signal				
Signal can be used to send SMS messages to any phone number. For end-to-end encrypted messages, all participants must have the Signal app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	In order to add contacts to Signal you have to add the contact to the mobile phone's address book. For SMS messages just input phone number to the message screen and send a text.	<p>Signal can be used as both an online messaging app and an SMS app, so there are two ways to have group chats.</p> <p>Using Signal as an SMS app you can have a group chat with up to 10 users: these users don't have to be in the mobile phone's address book and can be added manually. It is also possible to send bulk messages using Signal SMS by selecting all the users in the phone book and sending a message. This chat will not be encrypted and SMS fees apply.</p> <p>Using Signal as an online messaging app, group chats can include an unlimited number of members. Everyone in the group must have the latest version of Signal and be in the mobile phone's address book.</p>	No limit for secure group chat, 10 users for non-secure group chat.	Google Chrome app, Linux, Mac OS X, Chromium
Telegram				
All users have to create an account and have the app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	It is possible to add contacts to Telegram from the mobile phone's address book or searching for the Telegram user name.	<p>In group chats, an administrator creates the group but any group member can add others by sending invite links or searching for usernames.</p> <p>In "supergroups", an administrator can contact groups of up to 5,000 people and send updates to the whole group: these groups can also be public so anyone can view the whole chat and join. Any group can be converted into a supergroup. A message that is deleted by a user will be deleted from the whole group.</p> <p>Users can also subscribe to a channel to receive notifications. All notifications are public. Users can join by clicking a shareable URL or by subscribing to the group.</p>	<p>Groups - 200</p> <p>Supergroups - 5000</p> <p>Channels - No limit</p>	Windows, OS X, and Linux

Requirements for users communicating using the app	Method of adding contact	Communication with large numbers of people	Maximum number in group	Alternative platforms for non-mobile use available?
LINE				
All users have to create an account and have the app installed. Users are asked to create a username, and can create an account using their Facebook account or a phone number.	It is possible to add people to Line by adding a number to the mobile phone book, search by Line user ID, scan a QR code, or two users can shake their phones simultaneously.	Line manages group chats with up to 500 people. They have also created another app just for broadcasting messages. Line@ was created for businesses to broadcast to Line users who friend their account. You can chat or update a timeline, post documents etc. for people who have friended the account. There is no limit on the Line@ account.	500 for groups, no limit for Line@	Windows, IOS, iPad, Chrome browser version.
Facebook Messenger				
All users must have the app installed and a Facebook account. It is not necessary to be “friends” with the contact if the user’s mobile number is set to be searchable in the app. In some regions (and only on Android devices), it is possible to use the app to send SMS messages.	To start a group chat you can go to the group chat tab in the app, create a new group, and add people from your friend’s list or contacts to the group. You need to have a Facebook account and be in the contacts of the group admin.	The Facebook Messenger Platform is integrated into Messenger, and allows developers to create bots to communicate with an unlimited number of people.	Group chats - unclear. Bots - .	Version that works within browsers.
Snapchat				
All users have to create an account and have the app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	It is possible to add contacts from the mobile phone’s address book, as well as a “nearby” function which finds people near the user and adds them as a contact.	It is possible to use Snap to send stories, etc. to multiple people, but they have to be in the contact list and be individually selected. There doesn’t appear to be a limit on the number of people that can be selected. It is also possible to send stories to an unlimited number of followers. There is apparently no group chat function, only private one-to-one chat. The Discover option for broadcasting involves using a channel to contact subscribers; it is a paid service.	No limit	No
FireChat				
In order to use FireChat for messaging, all users have to install the app.	It is possible to add people by sending an individualized invite link to share via any sharing app, email, or SMS. Once clicked, the user is added to the group.	In FireChat, it is possible to have public chats that are on a broadcast channel; anyone with the app can join and the group can include thousands of people; you send messages by creating an invite link.	No limit	No
Skype				
In order to use Skype all users must have a Skype ID and the app installed.	It is possible to add contacts by searching for Skype usernames, email addresses or phone numbers.	Bots can be created that users can subscribe to, allowing them to receive messages from them. There is a business broadcast feature designed for communicating about meetings: all recipients must be on a list of attendees.	N/A	Browser, Windows, OS X, Linux, iPad, Android Tablets, Kindle, PC tablets, Xbox One, Apple and Android watch, Skype for TV

Requirements for users communicating using the app	Method of adding contact	Communication with large numbers of people	Maximum number in group	Alternative platforms for non-mobile use available?
imo				
All users have to create an account and have the app installed. A user must enter a code (sent to their phone number by SMS) when signing up.	It is possible to add a contact from the mobile phone book or by searching for their imo username.	imo offers group chats and a broadcast message feature. Broadcast feature allows the user to send messages to all their contacts.	No stated limit	Windows desktop, OS X
WeChat				
All parties need to have the app installed. Users are asked to submit their full name, country/region, phone number and a password. A user must enter a code (sent to their phone number by SMS) when signing up.	It is possible to find WeChat users in the mobile phone book, adding people close by with the WeChat nearby feature, adding their number manually, mass adding contacts with the 'friend radar' feature. Users can also send messages to a virtual space where people can see and add users by liking the message.	WeChat offers group chats that include an announcement feature that sends a notification for a message to all members of a group: only the administrator of the group can use this feature. The broadcast feature can send a mass message to all a user's contacts in WeChat.	500	OSX, Windows, browser

ENCRYPTION

Viber, Signal and WhatsApp all include end-to-end encryption that is turned on by default in one-to-one and group chats. End-to-end encryption is not enabled on WhatsApp's Broadcast Lists or Telegram's Channels. Facebook Messenger includes end-to-end encryption through its Secret Chats function, although users must actively opt in to be able to access this feature. LINE uses end-to-end encryption for one-to-one chats by default, though users must actively turn on encryption for group chats. Snapchat, Skype and WeChat do not currently provide any form of end-to-end encryption. Although imo has stated that its service is encrypted, it provides no further information that this report was able to verify.

Different apps use different encryption protocols. For example, Signal, WhatsApp and Facebook Messenger all use Open Whisper Systems' Signal protocol, an open standard that many cryptography specialists consider to be strong and well-designed. Telegram and Viber have developed their own protocols: Telegram uses the MTProto protocol, while Viber uses a protocol built from scratch that its developers describe as being similar to the Signal protocol. LINE uses the ECDH protocol.¹⁷⁵ Several apps, including LINE and Facebook Messenger, do not extend end-to-end encryption to their desktop platforms by default.

¹⁷⁵ The elliptic curve Diffie-Hellman (ECDH) protocol, like a number of other encryption protocols, is based on a public-private key system. Users' public keys are widely distributed, while private keys are not shared. Messages are encrypted using the intended recipient's public key, but can only be decrypted and read using the paired private key. A message can be authenticated by referencing the sender's public key.

Encryption features

	End-to-end encryption available?	Details of encryption	Other security features		
			Self-destructing messages?	Optional passcode protection for message content?	Two-factor authentication
WhatsApp	End-to-end encryption is available by default in one-to-one and group chats. All users must have the most recent version of the app in order for encryption to work.	Open Whisper Systems' Signal protocol.			No ¹⁷⁶
Viber	End-to-end encryption is available by default in one-to-one chats and group chats. End-to-end encryption is not available for Windows Phone 8 users.	Encryption protocol developed by Viber.		Yes	
Signal	End-to-end encryption is available by default for one-to-one and group chats for all users who have the most recent version of the app installed.	Open Whisper Systems' Signal protocol.	Yes	Yes	
Telegram	End-to-end encryption is available for one-to-one and group chats to all users with the updated Telegram app, and who opt in to using "Secret chats." Note that end-to-end encryption does not currently apply to conversations with bots or channels.	Encryption protocol developed from scratch by Telegram known as the MTproto protocol.	Yes	Yes	Yes
LINE	End-to-end encryption is available by default for one-to-one conversations and as an opt-in feature for group chats; all users must have the most recent version of the app in order for encryption to work.	Encryption protocol developed by Line using the ECDH protocol.		Yes	
Facebook Messenger	End-to-end encryption is not available by default, but only available for the "secret conversations" feature.	Open Whisper Systems' Signal protocol.			Yes
Snapchat	No end-to-end encryption available.	No end-to-end encryption	Yes		Yes
FireChat	End-to-end encryption is available for one-to-one communication. Encryption is also offered for offline peer-to-peer private messages.	FireChat states that it uses "state-of-the-art elliptic curve cryptography comparable to the Signal protocol, which works offline over the mesh network."			
Skype	No	No end-to-end encryption.			
imo	No, there is no information on the website or in imo's Privacy Policy that indicates whether end-to-end encryption is available or not.	No encryption information available.			
WeChat	No	No end-to-end encryption			

176 At the time of writing, WhatsApp's beta version included two-factor authentication: <https://www.whatsapp.com/faq/en/general/26000021>

OTHER FUNCTIONALITIES

Apps allow different types of media to be shared in the context of a chat conversation. All apps except FireChat and Snapchat offer a desktop computer version of their software, thus making it easier to send messages and share files between a conventional computer and a mobile phone. These desktop versions are usually linked directly to the mobile app via a phone number and use either a QR code or the submission of a short numeric code sent via SMS to confirm the user's identity.

DATA PROTECTION

App companies' jurisdictions and approaches towards data-sharing

Privacy policy/ legal usage policy URL	Company owner	Location of company	Terms of Service - Company jurisdiction	Does the app share information with third parties?
WhatsApp				
https://www.whatsapp.com/legal/	Facebook	US	California	The Terms of Service and Privacy Policies state that WhatsApp shares data with third parties. The data they share includes anonymous user usage data, referring / exit pages and URLs, platform types, asset views, number of clicks, etc. to understand the usage patterns for certain content, services, advertisements, promotions, and/or functionality on the WhatsApp site. In mid-2016, WhatsApp announced that they would start sharing users' phone numbers and time of usage data with Facebook.
Viber				
http://www.viber.com/en/terms	Viber Media	Israel	New York State	The Terms of Service states that Viber shares some data with third parties for technical needs, analytics or analysis of services, but does not specify what data.
Signal				
https://whispersystems.org/signal/privacy/	Open Whisper Systems	US	US	No.
Telegram				
https://telegram.org/privacy	Telegram Messenger LLP	Germany	Stated that servers are kept in different jurisdictions	The Terms of Service and Privacy Policies does not mention Telegram sharing data with third parties or outside servers being used.
LINE				
https://terms.line.me/line_rules/	Line Corporation / Naver Corporation	Japan	Japan	The Terms of Service state that Line does provide information to third-party partners and service providers, but do not specify what data is shared.
Facebook Messenger				
https://www.facebook.com/privacy/explanation	Facebook	US	California	The Data Policy states that Facebook Messenger uses third parties for technical infrastructure and analysis of services, but does not specify what data is shared.
Snapchat				
https://www.snapchat.com/privacy	Snap Inc.	US	California	The Privacy Policy states that Snapchat shares data with third parties for services, including sellers that provide goods through Snapchat, and business partners that provide services and functionality. It does not specify what data is shared.

Privacy policy/ legal usage policy URL	Company owner	Location of company	TOS - Company jurisdiction	Does the app share information with third parties?
FireChat				
https://www.snapchat.com/privacy	Open Garden	US	California	The Privacy Policy states that FireChat shares information with third-party vendors who provide services in connection with the app, i.e. vendors who send emails on behalf of FireChat. It does not specify what data is shared.
Skype				
https://www.skype.com/en/legal/	Microsoft	US	Washington	The Data Policy states that Skype shares personal data with third parties who provide services for them (i.e. vendors that provide customer service support or assist in protecting and securing systems) which may need access to personal data to function. It does not specify what kind of personal data is shared.
imo				
https://imo.im/policies/terms_of_service	PageBites Inc.	US	California	The Terms of Service state that imo shares data with third parties, but does not specify what data is shared.
WeChat				
https://www.wechat.com/en/privacy_policy.html	Tencent	China	Hong Kong	The Privacy Policy states that WeChat shares personal information with third parties. It does not specify what personal data is shared.

Metadata and content collected by app companies

App name	What user data and metadata does the app collect and retain?	How long does the app company retain metadata?	Does message content remain on the app company's servers?
WhatsApp	Phone number, mobile device information, log file information, IP address, browser language, referring/exit pages, URLs, platform type, number of clicks, domain names, landing pages, pages viewed, amount of time spent on pages, info of when a message is sent or received, if you update or request status information, time and date stamps, mobile phone numbers the messages were sent from and to.	No maximum retention period stated.	Content is kept on WhatsApp's servers until it is read; if the message is not read, it is deleted after 30 days. WhatsApp says it doesn't store messages on its servers and can't recover them for you.
Viber	Phone numbers and names from your address book on their servers, IP address, location, call detail records, numbers of messages and calls made by users, typical destinations, call lengths, network type.	Personal data is kept for "as long as needed", which means that it will be retained until an account is deactivated or the app is uninstalled.	Viber claims not to store content from messages once the message has been read. If a message is not read within two weeks, Viber says that the message will be deleted from their servers.
Signal	Signal states that it does not keep any user data or metadata beyond the user's phone number, the date that the user signed up for the service and the last time that the app communicated with the Signal server.	Signal states they do not keep any data and can't access any information.	No
Telegram	Telegram claims only to keep phone numbers and names of contacts, but no metadata on usage. There is a way to access the "last seen" data for each user in your contacts.	Telegram claims to delete all information when the account is deactivated, and if the account is not active for six months. When a message is deleted, it is deleted from their servers.	Telegram claims not to keep message information on their servers, only personal information needed for basic app functioning.
LINE	Line states that it retains user data that includes: operating system type, IP address, and browser information including type and language settings, device identifier, advertising identifier or mobile application identifier, telephone number. The user can also submit information to them including: email address, location, contacts, payment information, and information from integrated websites.	Line may retain personal information even after the account is closed if retention is reasonably necessary; in order to comply with applicable laws, regulations or legal obligations; to provide and complete customer support service; to resolve disputes between or with LINE users; or to detect and deter unauthorized or fraudulent use of or abuse of the Service.	According to Line's Privacy Policy User generated content is considered "optional" data that Line collects. It does not state in the policy how long the messages are stored in their servers and when/if they delete them. The app will keep metadata and personal data for basic functioning. They also offer "Keep" a storage solution for content to be stored on Line servers, but they say that they only keep it for 30 days.
Facebook Messenger	Facebook states that it retains user data that includes: phone number, message content, device information (operating system, location, connection information), network information and information about payments.	According to the Facebook Data Policy they store data for as long as they need to, they will keep data for law enforcement regulations for 90 days	Facebook does not store the messages from the secret conversations features, for all other conversations they store the message information and metadata for "as long as they need."
Snapchat	Snapchat username, Email address, Phone number, Snapchat account creation date, Time stamp and IP address of account logins and logouts, logs of previous messages sent and received	The Law enforcement document states that different information has different retention policies. Account information when creating the account is retained and when changed the old information is overwritten. If there is a law enforcement request then information will be kept. Logs of account activity are also kept until the user deletes the account.	Once the message is read Snapchat deletes it. If the message is not acknowledged it stays on their servers then is deleted after an expiration period (not specified how long), metadata is kept. If the content is shared on "public features such as Live, Local, or any other crowd-sourced service, we may retain the content indefinitely."

App name	What metadata does the app collect and retain?	How long does the app retain data?	Does message content remain on the app's servers?
FireChat	Contacts, when you use the app, logs of activity, third-party apps, websites visited, photo information, location, cellular network location, Wi-Fi networks, bluetooth services, browser services,	Terms of Service states FireChat will retain data as long as they have to.	FireChat keeps messages, metadata and user information "for as long as they need."
Skype	Name and contact data. Credentials. Demographic data. Payment data. Usage data. Product use data. Device data. Error reports and performance data. Support Data. Interests and favourites. Contacts and relationships. Location data. Content. Subject line and body of an email, text or other content of an instant message, audio and video recording of a video message, and audio recording and transcript of a voice message you receive or a text message you dictate.	No official retention policy is listed in its privacy policy.	Microsoft's Privacy Policy indicates that Skype keeps message content. The company does not specify a maximum retention time.
imo	Account creation data, profile info, posted content, contacts, device information, logs, online activities aggregated, location, chat history	No official data retention policy is listed in its privacy policy.	According to imo's Terms of Service they keep "anonymous and aggregated data" as well as metadata. The company does not specify a maximum retention time.
WeChat	Name, phone number, email, address, credit card, profile info, contact list, biometrics, location data, log data, date, time, and posts you make.	WeChat keeps data for law enforcement purposes. Personal information is kept for as long as the account is active.	WeChat states that it keeps content from group and public messages as well as metadata, but not private chat messages.

MISSION

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

#CommlsAid



ICRC