CHAPTER 12

MOBILE MESSAGING APPS

Lina Jasmontaite-Zaniewicz*

* This chapter is based on: The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*, January 2017: https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

12.1 INTRODUCTION

In their daily work, Humanitarian Organizations rely on multiple communication channels, including formal (e.g. radio and television), informal, unofficial and direct means of exchanging information. To employ the most appropriate communication channels in a given situation, Humanitarian Organizations have to understand the cultural background and needs of a particular society affected by a crisis and their means of communication.

In this respect, where mobile messaging apps are widely used, their deployment by Humanitarian Organizations is particularly attractive, because it allows immediate communication with people affected by crisis or conflict, and helps to coordinate internal tasks and actions efficiently. This type of technology can enhance the effectiveness and efficiency of Humanitarian Actions and reach populations in remote or inaccessible locations. However, mobile messaging apps are often employed without due consideration of the risks relating to Personal Data protection.

Despite the great functionality offered by mobile messaging apps, their use may entail significant risks ranging from data protection issues to disinformation. It seems that in practice, Humanitarian Organizations sometimes deploy them ad hoc, without following any formal procedures underpinned by risk analysis or considerations of long-term sustainability and management. Rather, the focus is on the Humanitarian Organizations' pressing information and communications needs. Insofar as this approach fails to include a comprehensive risk analysis, it runs counter to the guiding principles of Humanitarian Organizations, such as accountability, appropriateness, "do no harm" and due diligence.[1] As is the case with any other communication channel, the adoption of mobile messaging apps requires careful consideration of their benefits and risks. Questions to be included in such an analysis depend on the specific circumstances of a particular situation. For example, security concerns about Personal Data of individuals in a situation of political violence may differ greatly from security concerns in a natural disaster.

Mobile messaging apps installed on cellular phones or other smart devices may pose risks to individuals' right to Personal Data protection. This is because apps provide not only the possibility to exchange data between users, but also to process, aggregate and generate huge amounts of data (e.g. metadata, location data and contacts). Some data protection regulators consider that risks to Personal Data protection result from a combination of the following factors: (1) users' lack of awareness of the types

1 For an example of the operationalization of these principles, see ICRC, *Accountability to Affected People Institutional Framework*, January 2019: www.icrc.org/en/publication/accountability-affected-people-institutional-framework.

of data they actually process on a smart device; (2) absence of user's Consent; (3) poor security measures; and (4) the possibility of Further Processing.[2]

In line with the "digital proximity" imperative, i.e. Humanitarian Organizations seeking to be digitally where the beneficiaries are (just as they try to be physically), Humanitarian Organizations tend to use mobile messaging apps that are popular in a particular society at the time of a Humanitarian Emergency, such as WhatsApp, Facebook Messenger, Snapchat, Viber, Telegram and LINE. These proprietary cross-platforms are established by service providers which are usually not willing to customize their applications to meet the needs of Humanitarian Organizations. At the same time, deploying a less popular communication platform may exclude the people the organization is seeking to help. Therefore, it is imperative to know not only which communication channels exist in a particular place, but also which ones affected individuals trust and can use.[3]

The adoption of mobile messaging apps may also result in the Further Processing of collected data, including Personal Data. Mobile messaging apps make it possible to collect information online and may also provide new ways of analysing the available data. In other words, data and metadata collected via mobile messaging apps can help to triangulate information in new ways. In light of this and the probability of Further Processing of Personal Data, it is important to consider that in practice it is going to be challenging to limit the purpose for using a messaging application (e.g. affected individuals may decide to use it for providing feedback or reporting sensitive personal information, although the channel is designed for sharing public health information), and the number of entities with whom the collected data will be shared. Humanitarian Organizations may then find they are unable to state confidently that users can destroy or remove data already submitted, because this could entail multiple negotiations with multiple parties.

Mobile messaging apps were primarily designed to allow private communication between individuals or small groups. This type of functionality could be used by Humanitarian Organizations to provide basic counselling or to obtain information from beneficiaries about incidents, ongoing conflicts or particular needs. However, these apps may also be used in Humanitarian Action to "broadcast" content to large numbers of personal contacts or followers. In particular, in situations where the number of users is very large, mobile messaging apps may work as a one-way broadcasting channel (e.g. to announce the time and place for delivery of humanitarian aid, changed opening hours of a local clinic, or secure routes for transfer and evacuation of people). However, it is

2 Article 29 Data Protection Working Party, *Opinion 02/2013 on Apps on Smart Devices (WP 202)*, 27 February 2013: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

3 ICRC, *Accountability to Affected People Institutional Framework*, January 2019, 5.

challenging to ensure that messaging apps are used for one-way communication with beneficiaries as these apps are designed with two-way communication features. It should be highlighted that the latter often carry much higher risks for affected individuals (potentially more Personal Data may be transferred) and it also raises issues of long-term management/sustainability against expectation.

12.1.1 MOBILE MESSAGING APPS IN HUMANITARIAN ACTION

A messaging application (or app) is a software program that allows users to send and receive information using their mobile phones or other smart portable devices. The ease with which apps work has had a great impact on their popularity, public acceptance and continuously increasing demand. There are three key differences between communication through mobile messaging apps and communication through mobile phone networks:[4]

- Mobile messaging apps transmit and receive data using a Wi-Fi Internet connection or a mobile data connection (unlike SMS messages, which are transmitted over conventional telephone networks).
- Mobile messaging apps can transmit or receive a much wider range of data types than is possible using SMS or even its multimedia-enabled successor, MMS. Mobile messaging apps have developed more similarities than differences over time and, in addition to voice calls and text, messaging app users can also send and receive the following types of information: files, including photos, images and (in some cases) documents; 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; live video calls (in some apps); and emojis (pictographic representations of emotions or specific objects).
- Mobile messaging apps can transmit end-to-end encrypted content. They may, however, also generate and keep large amounts of – unencrypted – metadata.
- Humanitarian Organizations have been adopting mobile messaging apps for reasons such as the following:[5]
  - to target audiences (staff or beneficiaries) already using messaging apps;
  - to reduce communications costs;
  - to maintain reliable contact with people (whether staff or beneficiaries) in transit;
  - to enable communication with people in environments where other communications methods are unavailable;
  - to increase the speed of communications;
  - to improve the security of digital communications as compared with existing methods of communication (where such apps offer end-to-end encryption of content);

4 ICRC, The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*.

5 For a more detailed explanation of the reasons to adopt mobile messaging apps in Humanitarian Action, see ibid.

- to facilitate information collection from or dissemination to hard-to-reach, remote or inaccessible areas;
- to speed up data collection or increase efficiency;
- to improve inter-office coordination.

The use of mobile messaging apps can benefit affected individuals as such communication tools can enhance community engagement and acceptance, and can lead to a more people-centred, coordinated, accountable and effective response.[6] There is, however, little high-quality, disaggregated data available regarding which apps affected individuals are using and how they are being used.[7] The following usages of digital communications technologies have been identified by people migrating to Europe:[8]

- finding data on the intended country of destination (including legal information);
- 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.

Certainly, the reasons for individuals to use messaging apps in the humanitarian context may be diverse and range from meeting basic communication needs to the possibility of sharing documented atrocities.

Based on the considerations above, there are two separate areas of analysis to be distinguished from a data protection point of view:

- Personal Data Processing through the mobile messaging apps themselves;
- Personal Data Processing by Humanitarian Organizations, of data collected through mobile messaging apps.

These are addressed, in turn, below.

12.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

6 OCHA, "From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action – World | ReliefWeb", United Nations Office for the Coordination for Humanitarian Affairs (OCHA), Policy Branch, New York, 19 April 2021: https://reliefweb.int/report/world/digital-promise-frontline-practice-new-and-emerging-technologies-humanitarian-action.

7 ICRC, The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*, 32.

8 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", SSRN Scholarly Paper, Social Science Research Network, Rochester, NY, 1 June 2016: https://papers.ssrn.com/abstract=2862592; John Warnes, *Update: 10 CwC Challenges in the New Face of the European Refugee Crisis*, UNHCR, 2016: www.unhcr.org/innovation/update-10-cwc-challenges-new-face-european-refugee-crisis.

12.2.1 PROCESSING OF PERSONAL DATA THROUGH MOBILE MESSAGING APPS

Communicating with individuals affected by Humanitarian Emergencies through mobile apps requires Humanitarian Organizations, in most cases, to install and use applications already used by the majority of the population. Individuals, or in other words, beneficiaries in most cases have already downloaded and installed such applications and consented to their data protection terms.

By communicating with beneficiaries through mobile messaging apps, however, Humanitarian Organizations may suggest, whether directly or indirectly, that such means of communication are secure and that no harm is likely to arise for the beneficiaries in engaging with the Humanitarian Organization. It is important therefore that, irrespective of the initial Consent given by the beneficiaries to the app provider to process their Personal Data, a clear analysis of the implications of such use is made by the Humanitarian Organization to ensure that no unexpected negative consequences are generated by their engagement. It is recommended to do this with a DPIA, which would take into account the considerations set out below. The outcome of the DPIA may be that only certain types of data can be collected or communicated through a particular app, or that a particular app may be used only in certain circumstances and not others. It may also be that the use of a particularly popular app may be inappropriate for the Humanitarian Organization, and that the Humanitarian Organization may want to use such an app only to notify individuals of its intention to communicate through another, more secure, app. In carrying out the assessment it is also important to note that messaging apps develop and change features fast, and there is no guarantee that a feature offered by an app will be available indefinitely, or that users are running up-to-date software, particularly in countries where encryption is restricted by law. Similarly, companies' policies and statements about data usage, security and privacy may be revised at a later stage. Organizations will often be unable to view technical details of the underlying code, so they may be unable to make a comprehensive assessment of how any such changes affect users' security or privacy. Organizations that use Third Party providers to manage or process information should also prepare to engage with these risks. Changes in app features may require revision of the DPIA.

12.2.1.1 POTENTIAL THREATS

Data protection and privacy concerns arise in every area of a Humanitarian Organization's work, therefore organizations should evaluate particular risks when considering whether to deploy a messaging app or not. 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 (e.g. access by local authorities, law enforcement authorities, groups driven by various interests or private entities).

These Third Parties could include:

- entities in refugees' countries of origin, including armed groups and authorities, who may wish to identify groups or individuals for the purpose of harming and/or targeting them;
- entities with migration policy or security interests, who wish to understand and predict displacement trends and flows;
- entities with an interest in surveillance for national security purposes;
- hostile parties who wish to target Humanitarian Organizations and the people that they support and carry out violent attacks against them;
- commercial entities that wish to conduct behavioural profiling of particular groups, which can lead to discrimination.[9]

Concerns in this area have been acknowledged and supported by the International Conference of Data Protection and Privacy Commissioners, in its 2015 Resolution on Privacy and International Humanitarian Action:

> *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.*[10]

12.2.2 WHAT KIND OF DATA DO MESSAGING APPS COLLECT OR STORE?

There are three main protocols in the mobile messaging and encryption world: the Signal Protocol, MTProto and iMessage:[11]

- The Signal Protocol (previously known as both Axolotl and TextSecure) is used by Open Whisper Systems' Signal Messenger, Meta's WhatsApp, Facebook Messenger (in secret conversations), Google Allo (in incognito mode), Skype (since mid-2018, in private conversations) and Viber (proprietary, modified implementation).
- MTProto was developed and is used by Telegram (in secret chats).
- The iMessage protocol was developed by Apple and is used in iMessage.

These messaging protocols generate and process different kinds of data, and also protect message contents and metadata to various degrees.

9 Maria Xynou and Chris Walker, "Why We Still Recommend Signal over WhatsApp . . . Even Though They Both Use End-to-End Encryption", Security in a Box, 23 May 2016: https://securityinabox.org/my/blog/why-we-still-recommend-signal-over-whatsapp/.

10 International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action.

11 ICRC and Privacy International, *The Humanitarian Metadata Problem*, 50.

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 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 (such as Telegram, LINE and Facebook Messenger). This means that unless users are aware of the need to enable this feature in their settings, all message data may still be sent unencrypted. Communication with most bots on services such as Telegram is not end-to-end encrypted. It is important to note that although the content may be protected, metadata may not enjoy the same kinds of safeguards (see "Metadata" below.)[12]

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 images, 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.[13] Many apps automatically access a user's list of phone number contacts during sign-up to find other contacts that already have the app. In some cases, apps may store these data separately (WhatsApp, for example, confirmed in June 2016 that it stores contact list information).[14] Details of any groups to which the user belongs may also be stored in some cases.

Metadata: according to their terms of service, apps collect varying quantities of metadata, including sites and information accessed from within the app. Examples of metadata that could be obtained from a message include IMEI/IMSI (device and SIM identifiers), sender phone number, recipient phone number, message size, location data, time data, IP addresses, hardware model and web browser information.[15] Many app companies state that such data are retained on their servers, although they rarely clarify the length of time that data are retained, or if and how metadata are encrypted (even among apps that claim to have implemented end-to-end encryption). Although some messaging applications on personal computers offer to obscure users' metadata using Tor hidden services (software that enables

12 Lucy Handley, "Sheryl Sandberg: WhatsApp Metadata Informs Governments about Terrorism in Spite of Encryption", Yahoo! Finance, 31 July 2017: https://finance.yahoo.com/news/sheryl-sandberg-whatsapp-metadata-informs-112540721.html.

13 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.

14 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.

15 ICRC and Privacy International, *The Humanitarian Metadata Problem*, 60.

anonymous browsing),[16] this is not an option on the major messaging apps currently available. Instead, even the most privacy-conscious apps, such as Signal,[17] simply aim to collect as little metadata as possible.

Inferred data: even with end-to-end encryption of content, a lot can be inferred from the metadata around messaging.

EXAMPLE:
Researchers at MIT and the Université Catholique de Louvain, in Belgium, analyzed data on 1.5 million cellphone users in a small European country over a span of 15 months and found that just four points of reference, with fairly low spatial and temporal resolution, was enough to uniquely identify 95 percent of them.

In other words, to extract the complete location information for a single person from an "anonymized" data set of more than a million people, all you would need to do is place him or her within a couple of hundred yards of a cellphone transmitter, sometime over the course of an hour, four times in one year. A few Twitter posts would probably provide all the information you needed, if they contained specific information about the person's whereabouts.[18]

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 the data are processed and stored.[19] Twilio, a Third Party provider that works with some messaging app companies, provides limited transparency reports which indicate that it received 376 requests for data from international agencies in the first half of 2016 compared with 46 over the same period in 2015.[20]

16 For example, Orbot uses Tor hidden services: "Orbot: Proxy with Tor", Guardian Project, accessed 20 January 2022: https://guardianproject.info/apps/org.torproject.android; Joseph Cox, "'Ricochet', the Messenger That Beats Metadata, Passes Security Audit", Vice, 17 February 2016: www.vice.com/en/article/mg7v3a/ricochet-encrypted-messenger-tackles-metadata-problem-head-on.

17 Signal Messenger, "Grand Jury Subpoena for Signal User Data, Eastern District of Virginia", Signal Messenger, 4 October 2016: https://signal.org/bigbrother/eastern-virginia-grand-jury.

18 Hardesty, "How Hard Is It to 'de-Anonymize' Cellphone Data?"

19 For example, the EDPB's Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR noted that the reference to "other business services" by WhatsApp in its Legal Basis notice is unclear as it neither provides a relation to the specific legitimate interest nor specifies businesses or partners WhatsApp IE refers to, paragraph 63. See: European Data Protection Board (EDPB), Binding Decision 1/2021 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding WhatsApp Ireland under Article 65(1)(a) GDPR, 28 July 2021: https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf.

20 See Twilio, "Transparency Reporting", Twilio, accessed 20 January 2022: www.twilio.com/legal/transparency.

Evidence that a user has installed an app on their phone: by accessing an individual's physical device, authorities could find physical evidence that a user has installed a particular messaging app. This could also potentially be accessed through other means – for example, in most cases 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.

12.2.3 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 that it stores on its servers, in response to a disclosure request from an authority in the jurisdiction where such data are 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 actors (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.[21]
- When a device (e.g. a mobile phone or computer) is seized, forensic tools can be used to access its metadata, including content and data that the user believed to be deleted.[22] Extraction tools can be used to download data from mobile phones, including:
  - contacts;
  - call data (who we call, when and for how long);
  - text messages;
  - stored files (photos, videos, audio files, documents, etc.);
  - app data (what apps we use and the data stored on them);
  - location information;
  - Wi-Fi network connections (which can reveal the locations of any place where the users connected to Wi-Fi, such as workplace and properties they have visited).

21 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. Masashi Crete-Nishihata et al., "Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications", The Citizen Lab, 14 November 2013, https://citizenlab.ca/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", TechCrunch (blog), 23 December 2014: https://social.techcrunch.com/2014/12/23/thailand-line-monitoring-claim.

22 ICRC and Privacy International, *The Humanitarian Metadata Problem*, sec. 5.3.

Some mobile phone extraction tools may also access data stored in the cloud instead of directly on phones, or data that cannot be confirmed to exist or be accessed, i.e. deleted data.[23]

- **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,[24] or inducing users to install "malware" (short for malicious software) onto their phone which enables others to remotely gain access to that phone and data stored on it.[25]
- **An individual is forced to hand over their physical device.** End-to-end encryption only encrypts data 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 apps account (such as by compelling the user to unlock it), they may be able to access message content as well as details of apps that are installed on the device. In some countries, authorities consider merely installing apps such as WhatsApp as an indicator of subversive behaviour.[26] In view of this, messaging apps allowing "self-destructing" or "disappearing" messages, which can automatically be destructed after a short or predefined period of time and in this way make messages sent untraceable, offer more secure options for affected individuals.
- **A messaging app company allows an authority to directly access content or data transmitted over the app by building a secret feature into its code (known as a "backdoor").** For example, certain countries have reportedly threatened to fine messaging app companies that did not introduce backdoors into their code, specifically citing WhatsApp, Telegram and Viber.[27] Other companies have publicly stated that they have refused requests from government agencies to create backdoors.[28] There have also

23 Mobile Phone Extraction, explainer produced by Privacy International and Liberty as part of the joint campaign "Neighbourhood Watched: How policing surveillance technology impacts your rights", available at: Privacy International, "Mobile Phone Extraction" (Neighbourhood Watched: How policing surveillance technology impacts your rights), February 2019: https://privacyinternational.org/sites/default/files/2019-02/Explainers-MPE.pdf.

24 Frederic Jacobs, "How Russia Works on Intercepting Messaging Apps", bellingcat, 30 April 2016: www.bellingcat.com/news/2016/04/30/russia-telegram-hack; thaddeus t grugq, "Operational Telegram", Medium, 5 July 2016: https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a.

25 See for example: "Malware Posing As Human Rights Organizations and Commercial Software Targeting Iranians, Foreign Policy Institutions and Middle Eastern Countries", Iran Threats: Documenting Iranian State Sponsored Hacking, 1 September 2016: https://iranthreats.github.io/resources/human-rights-impersonation-malware; Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, Amnesty International, 18 July 2021: www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus.

26 Danny O'Brien, "Your Apps, Please? China Shows How Surveillance Leads to Intimidation and Software Censorship", Electronic Frontier Foundation, 8 January 2016: www.eff.org/deeplinks/2016/01/china-shows-how-backdoors-lead-software-censorship; Xynou and Walker, "Why We Still Recommend Signal over WhatsApp ... Even Though They Both Use End-to-End Encryption".

27 Patrick Howell O'Neill, "Russian Bill Requires Encryption Backdoors in All Messenger Apps", Daily Dot, 20 June 2016: www.dailydot.com/debug/encryption-backdoor-russia-fsb.

28 Jon Russell, "Apple Won't Create Universal IPhone 'Back Door' to Aid FBI", TechCrunch (blog), 17 February 2016: https://social.techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-

been ongoing attempts by intelligence agencies to enable them to access encrypted content.[29]

- **If the group is set as "public"** (i.e. anyone can join without being invited), these data could be accessed. Also, in a messaging group such as on WhatsApp, every member of the group can extract the declared names of other members, their phone numbers and the messages they have sent.[30]
- **The protections used in messaging apps have also been compromised by flaws in SS7, the underlying telecoms protocols.**[31] These flaws allow individuals to impersonate a phone number, create a duplicate account on a messaging app, and send and receive all messages destined for this number without the user's knowledge.[32]

12.2.4 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 situations.

12.2.4.1 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.

---

to-unlock-san-bernardino-attackers-iphone; Max Eddy, "What It's Like When the FBI Asks You to Backdoor Your Software", PCMag UK, 8 January2014: https://uk.pcmag.com/opinion/11141/what-its-like-when-the-fbi-asks-you-to-backdoor-your-software.

29 For reference see: Privacy International, "Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages", 29 May 2019: http://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages.

30 Vivek Wadhwa, "WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping", VentureBeat (blog), 3 April 2018: https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping.

31 Today's public switched telephone network (PSTN, i.e. the sum of all nationally, regionally or locally operated circuit-switched telephone networks) uses a signalling system called Signalling System No. 7 ("SS7"). SS7 is also the foundation of mobile telephony, used to route calls, SMS and other mobile services. For more details see: ICRC and Privacy International, *The Humanitarian Metadata Problem*" sec. 5.

32 vijay, "How to Hack Facebook Using SS7 Flaw", TechWorm (blog), 16 June 2016: www.techworm.net/2016/06/hack-facebook-using-ss7-flaw.html; John Leyden, "SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers", The Register, 10 May 2016: www.theregister.com/2016/05/10/ss7_mobile_chat_hack.

12.2.4.2 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 do not routinely store messages and that they delete messages from their servers immediately after they have been delivered to their intended recipient(s). However, companies such as Skype 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.

12.2.4.3 END-TO-END ENCRYPTION

End-to-end encryption restricts the ability of Third Parties such as governments or adversaries to intercept communications between Humanitarian Organizations and their beneficiaries in a way that allows the message contents to be viewed. In this case, even if a company does retain content data, this will be in an encrypted form and thus not legible to the company or to any Third Party seeking access to the data. 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. There are online resources which assess the levels of security offered by specific apps.[33]

12.2.4.4 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 purposes 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.

12.2.4.5 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, although Telegram's claim is contested,[34] whereas most major apps under consideration state that they collect contact numbers, logs of activity on the app and location information.

33 "Secure Messaging Apps Comparison | Privacy Matters", accessed 8 April 2022: www.securemessagingapps.com.

34 Jeremy Seth Davis, "Telegram Metadata Allows for 'Stalking Anyone'", SC Media, 30 November 2015, Online edition, sec. Security News, www.scmagazine.com/news/security-news/telegram-metadata-allows-for-stalking-anyone.

12.2.4.6 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. Ideally, an app will publish its entire codebase openly: messaging apps such Signal and Wire are entirely open source, while apps such as Telegram and Threema publish only part of their code.[35]

12.2.4.7 COMPANY 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, Microsoft[36] and Meta[37] publish regular transparency reports that detail how many requests they receive and how much data they hand over to law-enforcement agencies, while Signal provides more detailed descriptions of the small number of requests they receive.[38]

Additionally, it is important to consider whether an entity providing a messaging app is located in a country where the government has broad surveillance powers or a record of regularly flouting legal restraints on surveillance.[39]

12.2.4.8 LIMITED PERSONAL DATA SHARING WITH THIRD PARTIES

Although messaging apps will need to share some data with Third Parties (typically those playing some technical role in the data Processing) in order to facilitate the delivery of their services, it is critical that companies do not share Personal Data, and only share minimal, de-identified data when this is strictly necessary. Organizations should choose a messaging app that does not share any data with Third Parties other

35 For more on this topic, see Lorenzo Franceschi-Bicchierai, "Wickr: Can the Snapchat for Grown-Ups Save You From Spies?", Mashable, 4 March 2013: https://mashable.com/archive/wickr.

36 Microsoft, *Law Enforcement Request Report*, Microsoft Corporate Social Responsibility, accessed 21 February 2022: www.microsoft.com/en-us/corporate-responsibility/lerr.

37 Meta, "Government Requests for User Data | Transparency Center", Meta, accessed 15 February 2022: https://transparency.facebook.com/government-data-requests.

38 Signal Messenger, "Government Requests", Signal Messenger, accessed 21 February 2022: https://signal.org/bigbrother.

39 Useful sources for further research include: Electronic Frontier Foundation, "Digital Citizen", Electronic Frontier Foundation, 4 November 2019: www.eff.org/digital-citizen; Privacy International, "We Demand Change and Litigate | Advocacy", Privacy International, accessed 21 February 2022: https://privacyinternational.org/advocacy; Global Voices Advox, *Defending Free Speech Online*, Global Voices Advox, accessed 21 February 2022: https://advox.globalvoices.org; Electronic Frontier Foundation, "Deeplinks Blog", Electronic Frontier Foundation, accessed 21 February 2022, www.eff.org/deeplinks.

than those which are strictly necessary for the technical operation of the service – and seek to confirm this explicitly with companies before proceeding.

12.2.4.9 RESTRICTING ACCESS THROUGH THE DEVICE'S OPERATING SYSTEM, SOFTWARE OR SPECIFIC SECURITY PATCHES

Newer versions of mobile phone operating systems also include additional security features that, for instance, prevent apps from accessing data elsewhere on the device. Users can also choose to grant individual permissions or enable full-device encryption. However, these newer devices and operating systems are unlikely to be found in the areas in which Humanitarian Organizations operate. This means that unauthorized Third Parties may be able to access the data shared, as well as the metadata generated through the use of messaging apps, using the various means outlined above (Section 12.2.3 – How could other parties access data shared on messaging apps?).[40]

12.2.5 PROCESSING OF PERSONAL DATA COLLECTED THROUGH MOBILE MESSAGING APPS

Once the beneficiaries engage in communications with Humanitarian Organizations through mobile messaging apps, Humanitarian Organizations will need to collect, most likely store on other platforms, aggregate and analyse the information provided.

It is key that this Processing also takes place in line with the data protection principles set out in Part I of this Handbook. A few selected principles, specific to the collection of data through mobile messaging apps, are considered below.

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

- 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 their Personal Data are 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?

40 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 61–62.

Working with messaging apps adds a new layer of complexity to all these issues.

In their DPIAs, Humanitarian Organizations should include details of the various protocols and the degree to which each protocol protects content and metadata. Doing so will allow them to assess which option is best for a given purpose (i.e. sharing sensitive information), and also the context in which it will be used (i.e. legal and political), as well as the profile of beneficiaries.

12.3 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data collected through mobile messaging apps using one or more of the following legal bases:[41]

- the vital interest of the Data Subject or of another person;
- the public interest, in particular based on an organization's mandate under national or international law;
- Consent;
- a legitimate interest of the organization;
- the performance of a contract;
- compliance with a legal obligation.

In most cases, the Processing of Personal Data collected through mobile messaging apps may be based on Consent, vital interest or the public interest. If individuals have already communicated with a Humanitarian Organization by messaging app, or have given their telephone numbers to them, it can be assumed individuals consented to the privacy policy of the messaging application they use. This Consent, however, should not be confused with the legal ground for Processing Personal Data by Humanitarian Organizations. Consent obtained by Humanitarian Organizations must be informed, and it is key that Humanitarian Organizations provide relevant, clear, transparent and intelligible information concerning the purpose, retention or further sharing of collected data, as discussed in this Handbook.[42]

Otherwise, messages concerning Humanitarian Emergencies can be assumed to fall within the vital interest of Data Subjects or to be in the public interest. These legal bases also require that information be given to individuals, which can be done by sending them a link to the relevant information notice in a message via the mobile messaging application used. The quality, accessibility and comprehensibility of the information is as important as the actual content of the notice concerning the Processing.[43]

41 See Chapter 3: Legal bases for Personal Data Processing.

42 See Chapter 2: Basic principles of data protection.

43 Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679 (WP260 Rev.01)*, 11 April 2018, para. 4: https://ec.europa.eu/newsroom/article29/redirection/

12.4 DATA RETENTION

Humanitarian Organizations need to set out in their information notices and data protection policies how long they envisage holding the data collected.

Some of the data entered into most messaging apps are retained and stored by Third Parties (messaging-app companies), which in turn share some of those data with other parties – whether service providers that enable an app to function, or parent companies (as with Meta and WhatsApp). It is therefore also worth pointing out in the Humanitarian Organization's information notice that the data provided through the app will also be retained by the app provider and any Third Parties involved, under the responsibility of the app provider and governed by their data protection policies.

Humanitarian Organizations should also consider having a retention policy concerning the exchanges of information or "chats" themselves and delete the chat history at regular intervals to ensure data minimization.

12.5 DATA SUBJECT'S RIGHTS TO RECTIFICATION AND DELETION

As per Part I of this Handbook, Humanitarian Organizations should provide for mechanisms to facilitate the effective exercise of Data Subjects' rights, and inform Data Subjects thereof, in their data protection policies. Such policies should be concise, transparent, intelligible and easily accessible, and written in clear and plain language.[44]

Individuals should be informed that these policies differ from the data protection policy of a particular app, in order to be able to approach the relevant Data Controller. Individuals that seek to exercise their Data Subjects' rights will have to follow different procedures depending on whether they seek to exercise their rights within the communication channel of a Humanitarian Organization or within the scope of an app.

While it may not be problematic to erase or rectify Personal Data extracted from the messaging apps by the Humanitarian Organizations, it may be difficult to state

document/51025; European Data Protection Board (EDPB), Binding Decision 1/2021 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding WhatsApp Ireland under Article 65(1)(a) GDPR, para. 51.

44 Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679 (WP260 Rev.01)*, 11 April 2018, para. 7.

confidently that messaging apps allow users to destroy or remove data that they have already submitted, because this could entail negotiations with multiple parties (not all of whom are transparent about the data that they hold). It is recommended that this factor also be specified in the data protection policies of Humanitarian Organizations.

12.6 DATA MINIMIZATION

Considering the limited control Humanitarian Organizations have with regard to data collection by mobile messaging apps, organizations seeking to use messaging apps should aim to minimize the amount of information submitted to them. Academic research focused on the United States has also found that users of messaging apps are usually unaware of the privacy implications of installing and sharing data on messaging apps.[45] Therefore, it is suggested that Humanitarian Organizations should provide incentives for crisis-affected individuals to share only Personal Data that are strictly necessary to provide humanitarian aid.

EXAMPLE:

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.[46]

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 sociocultural 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," Claudia Abreu Lopes, Head of Research and Innovation, said. "It was problematic

45 Patrick Gage Kelley et al., "A conundrum of permissions: Installing applications on an Android smartphone", in *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Springer, Berlin/Heidelberg, 2012, 68–79: https://link.springer.com/chapter/10.1007/978-3-642-34638-5_6.

46 Africa's Voices Foundation, "Youth Priorities for 2016 Municipal Elections in South Africa (Livity Africa)", Africa's Voices Foundation (blog), 2016: www.africasvoices.org/case-studies/youth-priorities-for-2016-municipal-elections-in-south-africa-livity-africa.

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."

As suggested above, it is recommended that Humanitarian Organizations also consider having clear policies on deleting chats at regular intervals, for example, once the necessary data have been extracted.

12.7 PURPOSE LIMITATION AND FURTHER PROCESSING

In most cases data collected through mobile messaging apps will be extracted and analysed by Humanitarian Organizations on other platforms. As part of the Humanitarian Organizations' data protection policies to be communicated to the Data Subjects, Humanitarian Organizations should also clearly specify the purpose of Processing.

This can be particularly challenging considering the flexibility of use and immediacy of communication offered by such solutions, as it is likely that in any one chat numerous issues will be raised by a Data Subject, with each issue requiring one or more follow-up actions. With this in mind, and considering the compatibility of humanitarian purposes, it is suggested that a general humanitarian assistance and protection purpose specification should suffice.

Again, as Processing by mobile messaging applications is beyond the control of Humanitarian Organizations, the fact that such applications may process data for different purposes, according to their own data protection policies, should also be clarified in the Humanitarian Organization's data protection policy.

12.8 MANAGING, ANALYSING AND VERIFYING DATA

Making use of data processed through messaging apps in Humanitarian Action is 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 manage, analyse and verify collected data.

Difficulties can arise in creating an effective workflow to manage and analyse the information received. The systems used by messaging apps are not always interoperable with existing information-management systems or databases used by

Humanitarian Organizations. Manual transcription of individual messages into spreadsheets is often used by Humanitarian Organizations to analyse data in a way that would allow for effective decision making.

Challenges also arise with regard to verifying information received through messaging apps. While this is an issue in many online channels,[47] 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 defenders have attempted to respond to these challenges through collaboration and efforts to produce resources and guidance on the issue. Some messaging apps (e.g. WhatsApp) have developed features aiding the verification and fact-checking process.[48] Some of these resources may also be useful to Humanitarian Organizations.[49]

Humanitarian Organizations engage in Further Processing in cases where the Personal Data collected via apps are managed, analysed or verified. Consequently, Humanitarian Organizations have to ensure that Further Processing of Personal Data operations is compatible with the initial purpose for which data were collected.

12.9 DATA PROTECTION BY DESIGN

Prior to launching a communication channel through a messaging app, Humanitarian Organizations, in addition to the guiding principles of humanitarian work,[50] should consider whether the app implements appropriate technical and organizational measures and whether it is designed in such a way that it implements the core data protection principles (e.g. lawfulness, fairness and transparency, purpose limitation and data minimization).

47 The Engine Room, "Verification of Social Media: The Case of UNHCR on Twitter", Responsible Data (blog), 2016: https://responsibledata.io/rd-reflection-stories/social-media-verification.

48 Mark Sweney, "WhatsApp launches factcheck feature aimed at viral messages", *The Guardian*, 4 August 2020, Online edition, sec. Digital Media: www.theguardian.com/technology/2020/aug/04/whatsapp-launches-factcheck-feature-aimed-at-viral-messages.

49 See for example: Craig Silverman, ed., *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, 1. ed., European Journalism Centre, Maastricht, 2014: http://verificationhandbook.com; AAVV, *DatNav: New Guide to Navigate and Integrate Digital Data in Human Rights Research*, Guide, The Engine Room; Benetech; Amnesty International, June 2016: www.theengineroom.org/datnav-digital-data-in-human-rights-research; First Draft News Partner Network, "Mission Statement", First Draft, accessed 22 February 2022: https://firstdraftnews.org/about.

50 ICRC, *Accountability to Affected People Institutional Framework*, January 2019.

If Humanitarian Organizations intend to develop a messaging app, they should consider implementing the principle of data protection by design and by default, which requires the development of privacy-friendly systems and services through a set of both technical solutions and organizational measures. The client-server architecture used to store data should give effect to the principle of data protection by design. For more guidance on the topic of data protection by design and by default, see Chapter 6: Designing for Data Protection.

When deciding to develop its own app or platform, there are a few practical considerations for a Humanitarian Organization to keep in mind. First, the organization needs to understand the context, needs and local community communication channels (e.g. what messaging apps are popular in a particular society and how a new app would complement or replace it).[51] Second, promoting the use of a new app among the organization's beneficiaries may prove challenging. It is likely that the local community is going to prefer the established communication platform (i.e. messaging app) over a new app. And finally, app maintenance and security involves ongoing costs. All software, once it has been developed, requires regular updates as new vulnerabilities emerge. A Humanitarian Organization will need to consider whether it has the in-house skills and expertise to develop and maintain such an app or platform.[52]

12.10 INTERNATIONAL DATA SHARING

It is also important to be aware that some services intersect, and they may overlap in terms of the entities and operating methods involved. In practice, this means that the Data Processing activities of social media networks and messaging apps must not, and cannot, be viewed as separate. Often, messaging apps are linked to social media networks directly (e.g. Facebook Messenger), or indirectly because they are owned by the same business group (e.g. WhatsApp is owned by Meta, which also owns Facebook). Here, services may share data for a variety of purposes.[53]

51 Ibid.

52 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, sec. 5.4.

53 Ibid., sec. 4.1.