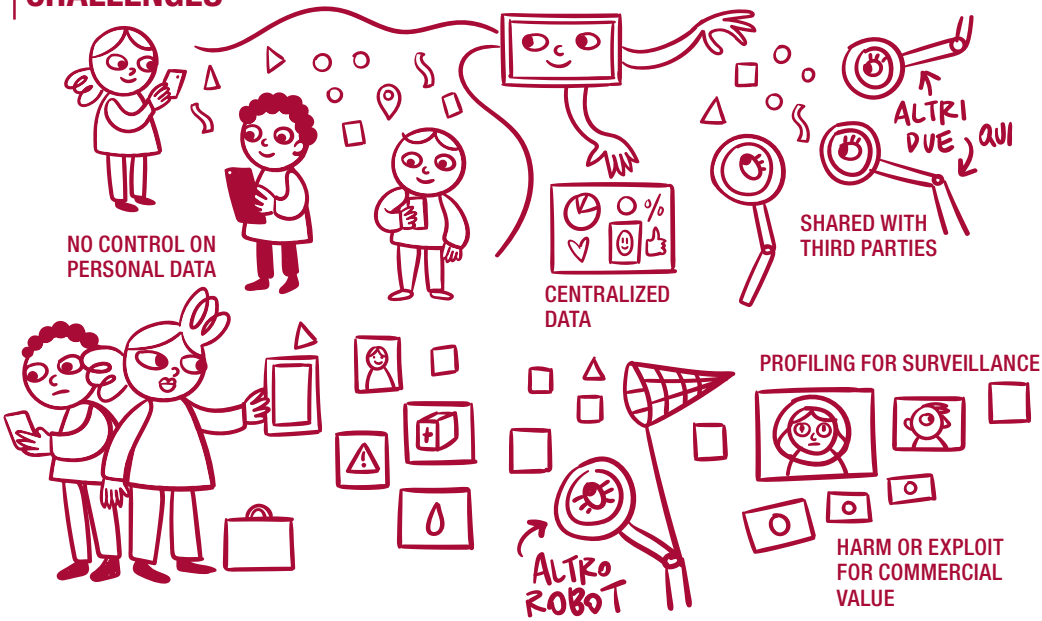
SOCIAL MEDIA

POSSIBLE USE

CHALLENGES



CHAPTER 14

SOCIAL MEDIA

Júlia Zomignani Barboza and Lina Jasmontaite-Zaniewicz*

* The authors would like to thank Nicolas de Bouville (Facebook), John Warnes (UNHCR), and Camila Graham Wood, Antonella Napolitano and Ed Geraghty (Privacy International) for their contributions to this chapter.

14.1 INTRODUCTION[1]

14.1.1 SOCIAL MEDIA IN THE HUMANITARIAN SECTOR

Humanitarian Organizations often use social media in their work both to engage with those in need and for campaigning and fundraising purposes. While this chapter focuses on the former use case, it will sometimes refer to the latter, as usually the social media "profile" used is the same for both purposes and thus a completely separate analysis is not possible.

Humanitarian Organizations interact with beneficiaries via social media in a variety of ways. In emergencies, for instance, they may use social media to inform people about safe places and the delivery of aid. They may also use social media to raise awareness (such as addressing humanitarian needs arising in the framework of migration), to encourage beneficiaries to share information with each other in an emergency or to provide information about health and medical care.

Engaging with beneficiaries in this way carries a number of risks. When individuals view or reply to public or private social media posts by Humanitarian Organizations, or when they join public or private groups hosted by such organizations, they share a rich variety of data with the platform in question. Both Humanitarian Organizations and beneficiaries may engage with each other on social media without necessarily being fully aware that they are generating both data and metadata (a set of data that describes and gives information about other data)[2] that can be collected by social media platforms, then used to profile an individual to determine characteristics such as key aspects of their identity, their networks, views and opinions, preferences and affiliations. Likewise, organizations and beneficiaries may be unaware of the consequences and risks of such Processing.

Although individuals may engage with Humanitarian Organizations informally, in a manner akin to a private conversation, the way social media platforms are designed and operate means that Third Parties may be able to monitor, collect, retain and analyse their exchanges. These Third Parties include not only social media providers, but also corporate entities, law enforcement agencies, immigration and border authorities,[3] and governments, who use open-source intelligence techniques and

1 This chapter focuses on the use of social media by Humanitarian Organizations to communicate and engage with affected communities. For information related to the use of social media to identify crises and improve the humanitarian response, please refer to Chapter 17: Artificial Intelligence. For messaging apps, please refer to Chapter 12: Mobile messaging apps.

2 For more on metadata, see: ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018.

3 See for example: Lina Jasmontaite-Zaniewicz and Júlia Zomignani Barboza, "Disproportionate surveillance: Technology-assisted and automated decisions in asylum applications in the EU?",

sophisticated social media monitoring tools. Data, including images shared on social media, can be analysed in a range of ways – from image and facial recognition, to sentiment and emotion recognition[4] – often using opaque algorithms and Machine Learning.[5] This type of profiling adds to the opacity of how individuals can be exposed through their interactions with, and use of, social media. When decisions are made based on such profiling, it can have serious consequences for an individual, because this opacity brings added risks that come from unequal access to data and to justice, such as the inability to challenge incorrect assumptions that influence or determine decision-making processes and outcomes.

While social media can help Humanitarian Organizations provide services, using these platforms can cause organizations to lose control of the data generated and shared, and pose medium- or longer-term risks. These must be assessed through clear procedures and risk assessments (see Section 15.2 – Data Protection Impact Assessments, below).

Below are some examples of cases where Humanitarian Organizations have used social media to engage with beneficiaries:[6]

- **Facilitating emergency management by contributing to the mitigation, preparedness, response, and recovery of disasters and emergency situations.** In Bangladesh, the creation of a national coordination platform allowed Humanitarian Organizations, in coordination with the government, to broadcast easily understandable disaster-preparedness messages through social media during emergencies to facilitate the disaster-preparedness stage of emergencies.
- **Improving the quality of aid delivery.** In 2016, the ICRC doubled the amount of food contained in food parcels delivered in Syria, as the security situation led to longer periods between food distribution. Beneficiaries were informed of this change in a short video shared on ICRC's institutional Facebook page. Through the comments feature, beneficiaries also had the opportunity to reply to the video and explain their needs (e.g. requesting better cardboard boxes so the food inside would not be damaged in transit). The ICRC then replied to the comments, explaining what it was doing to fulfil the requests or why it could not do so.
- **Improving the efficiency of services.** The Kenyan Red Cross Society (KRCS) actively monitors social media platforms to find out about road accidents and

International Journal of Refugee Law, Vol. 33, No. 1, 27 October 2021, pp. 89–110: www.icrc.org/en/document/social-media-to-engage-with-affected-people.

4 See for example: Flor Miriam Plaza-del-Arco et al., "Improved emotion recognition in Spanish social media through incorporation of lexical knowledge", *Future Generation Computer Systems*, No. 110, 1 September 2020, pp. 1000–1008: https://doi.org/10.1016/j.future.2019.09.034.

5 See Chapter 17: Artificial Intelligence.

6 The first four examples were taken from: Timo Lüge, "How to Use Social Media to Engage with People Affected by Crisis", News release, ICRC, IFRC, UN OCHA, September 2017: www.icrc.org/en/document/social-media-to-engage-with-affected-people.

dispatch ambulances to those locations. Knowing this, Kenyans frequently flag road-traffic accidents to the KRCS through social media.

- **"Information as aid" and health promotion.** MSF and other NGOs use social media to provide health information and advice to beneficiaries.
- **Combatting misinformation.** In the early days of the COVID-19 pandemic, the International Organization for Migration (IOM) noted that TikTok was a powerful tool to combat misinformation about the pandemic, including falsehoods that migrants were responsible for the crisis, which could lead to xenophobia, stigma and discrimination.[7]

Although social media platforms offer a wide range of opportunities, using them can also pose risks to beneficiaries and raise important responsibility questions for Humanitarian Organizations. This chapter will discuss how data are generated on social media before addressing core data protection concerns.

14.1.2 SOCIAL MEDIA AND DATA

14.1.2.1 WHAT DATA ARE GENERATED ON SOCIAL MEDIA AND HOW?

Social media platforms receive, capture, generate and process large amounts of data from users, including metadata, user location, images, contacts, "likes", and attention and interest indicators, using them for various purposes. Despite this large-scale Processing, there may often be little transparency as to what specific data are being created, and how the platform and other Third Parties are accessing and using these data for profiling and other purposes.

Some of the data collected by social media platforms come directly from the individual (this is known as "declared data"), such as when they sign up for an account (a name or username, sometimes a copy of an identity document, a phone number, an email address and a physical address), or when they post photographs or comments on their profile.[8]

Furthermore, the declared data may include not only data provided directly by the user, but also data about the user coming from other apps or platforms,[9] which sometimes automatically transfer Personal Data to social media platforms when a user opens the app or accesses its services, even before obtaining Consent.[10] This

7 IOM-UN Migration, "Humanitarians on TikTok", Medium, 15 May 2020: https://medium.com/digital-diplomacy/humanitarians-on-tiktok-246651af74d.

8 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 34.

9 In its guidelines on targeting of social media users, the European Data Protection Board called this type of data "observed data". See: European Data Protection Board (EDPB), *Guidelines 8/2020 on the targeting of social media users*, 13 April 2021, 13: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

10 Privacy International, "Investigating Apps Interactions with Facebook on Android", March 2019: https://privacyinternational.org/appdata.

happens, for example, when an online store notifies a social media platform that a user has accessed its website so that the platform can use their shopping preferences to offer them targeted advertisements.

Social media platforms also process so-called "inferred data" – additional data not provided directly by users themselves but inferred from their declared data. In this regard, social media platforms usually combine data obtained from different sources and, applying Data Analytics,[11] create a user profile that monitors the user's activities and behaviour.[12] For example, providers can infer who someone's close friends are from how often they communicate and interact on social media.[13] Similarly, social media platforms "might infer that an individual is likely to be interested in a certain activity or product on the basis of his or her web browsing behaviour and/or network connections".[14] Understanding someone's routine and behaviour allows platforms to offer targeted services and individualized content to their users.[15]

Evidence shows that it is possible to build a profile-type identity from someone's digital behavioural attributes, i.e. their online activity.[16] Consequently, a person's digital traces can be used to create a digital profile even without their knowledge[17] and infer information about them including their gender, sexual orientation, religion, location, interpersonal relationships and anticipated behaviour.[18] This type of profile is then used for targeted advertising, but has also been used in the past for political campaigning, as well as predictive policing.[19] This means that if Humanitarian Organizations encourage beneficiaries to engage with them on social media, they may be facilitating this kind of targeting. Furthermore, Humanitarian Organizations frequently use the same social media page or profile both for their humanitarian work and for campaigning and fundraising and thus may also benefit from such targeting in other activities, while at the same time contributing to generation of data and user profiles.

11 See Chapter 17: Artificial Intelligence.

12 Article 29 Data Protection Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 Rev.01)*, Guideline (Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 22 August 2018), 12: https://ec.europa.eu/newsroom/article29/items/612053.

13 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 35.

14 European Data Protection Board (EDPB), *Guidelines 8/2020*, 14.

15 For more on target advertising, see Privacy International, "AdTech", accessed 15 February 2022: https://privacyinternational.org/learn/adtech.

16 Beduschi et al., "Building Digital Identities", 8.

17 For example, Facebook shadow accounts. See: Brandom, "Facebook Has a Shadow Profile for You".

18 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 90.

19 See for example: Albert Meijer and Martijn Wessels, "Predictive policing: Review of benefits and drawbacks", *International Journal of Public Administration*, Vol. 42, No. 12, 10 September 2019, pp. 1031–1039: https://doi.org/10.1080/01900692.2019.1575664. Predictive policing is considered to be part of law enforcement practices.

EXAMPLES OF DATA THAT MAY BE COLLECTED:

Facebook divides the data it collects into three categories: things that users do and provide, device information and information from partners.[20] Under each category, there is a long list of data that the platform collects, including:

> *communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created.*[21]

The list also includes "information about operations and behaviours performed on the device, such as whether a window is in the foreground or background, or mouse movements"[22] as well as Bluetooth signals, and information about nearby Wi-Fi access points, beacons and cell towers.

Similarly, TikTok also divides the data it collects into three categories: information users provide, automatically collected information and information from other sources.[23] The automatically collected information includes inferred information, explained by the platform as follows:

> *We infer your attributes (such as age-range and gender) and interests based on the information we have about you. We use inferences to, for example, keep our Platform safe, content moderation, and, where permitted, to serve you personalised ads based on your interests.*

X (former Twitter), in turn, collects data related to a user's basic information (such as declared name, username and email address), profile information, contact information and public information (tweets as well as metadata generated by tweets such as time and location).[24]

14.1.2.2 WHAT DATA CAN BE SHARED WITH THIRD PARTIES?

Some social media platforms may share the information they collect with other service providers for purposes such as targeted advertising of individuals with specific profiles. Given the exponential growth of social media platforms, the number of people and advertising companies that have access to personal information has vastly increased in recent years, thereby increasing the possibility that individuals could be tracked through different methods. Moreover, social media platforms receive data from other parties and organizations through partnership arrangements,

20 Facebook, "Data Policy", Facebook, accessed 15 February 2022: www.facebook.com/about/privacy.

21 Ibid.

22 Ibid.

23 TikTok, "Privacy Policy", TikTok, accessed 15 February 2022: www.tiktok.com/legal/privacy-policy-eea?lang = en.

24 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 96.

and these additional data are used to further develop a user's profile for various purposes, including advertising.

EXAMPLES OF HOW SOCIAL MEDIA DATA MAY BE SHARED:

Facebook shares aggregated information it collects from users and non-users of the network with other Meta companies (including Instagram, WhatsApp and Messenger) and Third Party partners. It also allows users to share data they store on Facebook with Third Party apps, websites or other services that use or are integrated with Facebook.[25] This means that users may (knowingly or otherwise) share data that are not related solely to them, such as their friends list. Consequently, "even when a user 'locks down' their profile, their data could still be collected by a third-party app being used by one of their friends".[26]

Facebook also offers a variety of options for advertisers to benefit from users' profiles. For instance, advertisers may upload an email or phone list of registered customers and ask Facebook to find their social media profiles in order to target them for marketing purposes (known as a "custom audience").[27] This way, advertisers benefit from aggregated information provided by Facebook, while the social media platform also gathers data from the advertiser. Companies may also ask Facebook to find profiles that are similar to existing customers in order to increase their range of advertising, to focus on specific locations, demographics or genders, or even to install pixels[28] on their websites, so that when a Facebook user visits their website, they receive ads from the company on their Facebook page.[29] Since December 2019, however, Facebook no longer allows phone numbers provided by users when signing up for two-factor authentication to be used to make friend suggestions.[30] This change in company practice reflects increased recognition of the implications of data-sharing between platforms and Third Parties.[31] This is further demonstrated by the new

25 Facebook, "Data Policy".

26 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 96.

27 Facebook, "About Customer List Custom Audiences", Facebook Business Help Center, accessed 15 February 2022: www.facebook.com/business/help/341425252616329.

28 Facebook pixel is a Facebook analytics tool that allows businesses to better target their advertisements by measuring their effectiveness and understanding the actions people take when visiting the business' website. See: Facebook, "About MetaPixel", Facebook Business Help Center, accessed 15 February 2022: www.facebook.com/business/help/742478679120153.

29 Brendan Van Alsenoy et al., *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms*, Belgian Privacy Commission, 2015, 55–64.

30 Katie Paul, "Facebook Separates Security Tool from Friend Suggestions, Citing Privacy Overhaul", Reuters, 19 December 2019, sec. Internet News: www.reuters.com/article/us-facebook-privacyidUSKBN1YN26Q.

31 In 2020, the platform also removed some of its target audience categories related to race and ethnicity to prevent misuse; however, some have questioned the fact that the platform still uses categories that could be considered as racial proxy categories. See: Meta, "Simplifying Targeting Categories", Meta for Business, 11 August 2020: www.facebook.com/business/news/update-to-facebook-ads-targeting-categories; see

Off-Facebook Activity tool,[32] which allows users to segregate information obtained by Third Parties from their Facebook profile. In the same manner, in recent versions of its mobile operational system, Apple limited the tracking options between mobile applications, including social media applications, with the goal of increasing transparency and control of such activities by mobile users.[33]

With regard to advertising, TikTok shares and receives data from partners in a similar way to Facebook. According to the platform's privacy policy

> *Advertisers and measurement and data partners share information with us such as mobile identifiers for advertising, hashed email addresses, and event information about the actions you've taken on a website or app. Some of our advertisers and other partners enable us to collect similar information directly from their website or app by integrating our TikTok Advertiser Tools (such as TikTok Pixel).*

X (former Twitter), in turn, allows users to opt out of much of its Processing activities. By default, however, everything shared and published on the platform is public unless the user specifies otherwise. In practice, this means X (former Twitter):

> *is allowed to share or disclose a user's public information (such as profile information, public tweets, or followers) to a wide range of users, services and organizations. Twitter further maintains the right to infer, from these data, which topics might be of interest to the user.*[34]

14.1.2.3 WHAT DATA CAN LAW ENFORCEMENT AND GOVERNMENT AUTHORITIES OBTAIN?

National law may require social media platforms to store users' Personal Data so that public authorities can access them to identify an individual or obtain information about their online activity for law enforcement purposes.[35] In some – but not all – jurisdictions, a warrant may be needed to access such information. In this regard, a

also: Jon Keegan, "Facebook Got Rid of Racial Ad Categories. Or Did It?", The Markup, 9 July 2021: https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it.

32 Erin Egan and David Baser, "Now You Can See and Control the Data That Apps and Websites Share With Facebook", Meta (blog), 20 August 2019: about.fb.com/news/2019/08/off-facebook-activity/.

33 Apple Inc, "User Privacy and Data Use – App Store", Apple Developer, accessed 15 February 2022: https://developer.apple.com/app-store/user-privacy-and-data-use; see also: "How the Apple IOS 14 Release May Affect Your Ads and Reporting", Facebook Business Help Center, accessed 15 February 2022: www.facebook.com/business/help/331612538028890.

34 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 97.

35 Ibid., 34.

few social media companies publish transparency reports containing information on government access requests.[36]

Using various tools, including those provided by the platforms themselves (the so-called "firehose"), law enforcement agencies and other Third Parties can directly access social media through what is known as open-source intelligence (OSINT), i.e. intelligence gathered from publicly available data. They can also use social media intelligence (SOCMINT), which involves monitoring and gathering both publicly available and private information on social media platforms.[37] These practices are unregulated in many jurisdictions, and the law is often unclear as to whether such monitoring is legal. Further invasive techniques also enable data and information physically stored on a device[38] or in cloud-based applications[39] to be extracted. As with SOCMINT, mobile phone and cloud extraction technologies are used with little transparency and remain unregulated in a number of jurisdictions. In practice, as social media storage is often cloud-based, the volume of Personal Data that can be obtained through these methods is very large.

14.2 DATA PROTECTION IMPACT ASSESSMENTS

Humanitarian Organizations cannot fully control how social media platforms operate, or how they generate and process data. But they can – and should – conduct risk assessments to understand the consequences of using social media to interact with beneficiaries before deciding whether to use such platforms, how to use them and for what purpose.

Humanitarian Organizations use social media with the expectation that beneficiaries have already signed up and consented or otherwise agreed to the platform's terms and conditions. This expectation does not relieve organizations of their duty to carry out a Data Protection Impact Assessment (DPIA).[40] The purpose of a DPIA is to identify how

36 Meta, "Government Requests for User Data | Transparency Center"; Twitter, "Twitter Transparency Center", Twitter, accessed 15 February 2022: https://transparency.twitter.com/en.html; TikTok; "Reports", TikTok, accessed 15 February 2022: www.tiktok.com/transparency/en-us/reports.

37 Privacy International, "Social Media Intelligence", Privacy International, 23 October 2017: http://privacyinternational.org/explainer/55/social-media-intelligence.

38 See, for example: Privacy International, "Push This Button For Evidence: Digital Forensics", Privacy International, 24 June 2019: http://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics; Privacy International, "Can the Police Limit What They Extract from Your Phone?", Privacy International, 14 November 2019: http://privacyinternational.org/node/3281.

39 Privacy International, "Cloud Extraction Technology: The Secret Tech That Lets Government Agencies Collect Masses of Data from Your Apps", Privacy International, 7 January 2020: http://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data.

40 See Chapter 5: Data Protection Impact Assessments (DPIAs).

social media use will affect beneficiaries and which measures the organization can take to mitigate potential risks. In particular, a DPIA should not only look at data protection risks, but also evaluate whether social media use in a particular context could lead to human rights violations or otherwise harm the individuals in question. These risks should then be weighed against the potential benefits.

It is worth stressing again that, aside from the content users generate and provide when they sign up for their account(s), the use of social media also generates a large amount of data and metadata that platforms do not proactively declare. Consequently, users may not even be aware these data are being generated and processed.[41] For example, merely clicking "like" buttons or links that redirect the user to other websites generates metadata.

In recent years, many governments have gained access to, and made use of, large amounts of social media data and metadata, as well as powerful analysis tools that help them identify patterns in such data and profile individuals and groups.[42] The DPIA must therefore go beyond merely analysing compliance with data protection requirements. It should also address how the use of a certain application or platform could positively or negatively impact a variety of fundamental rights, as well as the ethical and social implications of Processing by Humanitarian Organizations.[43] This does not mean that the DPIA should replace other forms of impact assessment that may take place within a Humanitarian Organization before implementing their programmes, but it should consider the implications that come from the Processing of Personal Data in a holistic way, which may involve including stakeholders from fields other than data protection.

This is because the Processing of Personal Data and especially metadata can carry significant risks. In 2014, for instance, a former director of the US National Security Agency (NSA) said that they would take the decision to kill people based on information acquired via metadata.[44] Fintech and advertising companies are also employing numerous techniques to make use of such data.[45] That is why it is important for Humanitarian Organizations to take the non-humanitarian purposes and consequences of using social media into account when conducting a DPIA and developing their social media use strategy.

Likewise, the DPIA should consider the fact that social media providers' business models rely on monetizing user data (e.g. for ad targeting). This means that data

41 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 17.

42 Ibid., 29.

43 Alessandro Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", *Computer Law & Security Review*, Vol. 34, Issue 4, 2018, pp. 754–772: https://doi.org/10.1016/j.clsr.2018.05.017.

44 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 22.

45 Ibid., 23–24.

gathered for humanitarian purposes through such platforms might be vulnerable to commercial exploitation and surveillance.

Humanitarian Organizations should also assess whether social media platforms are the safest and most reliable way to communicate with beneficiaries. In places where physical access to Humanitarian Organizations is difficult, for example, social media may provide an effective means of communication between organizations and beneficiaries who cannot reach them in person.[46] In emergencies, however, governments can shut down social media to avoid the spread of fear or false information,[47] meaning Humanitarian Organizations will need to consider alternative means of communication.

14.3 ETHICAL ISSUES AND OTHER CHALLENGES

For Humanitarian Organizations, involving social media platforms in their work inevitably raises ethical issues because the organization does not have control over Third Parties' privacy and data protection policies. Many of these platforms rely on exploiting and monetizing users' data[48] – both declared data and inferred data, which can reveal sensitive information such as a person's sexual orientation, religion, political opinion and ethnicity.[49] Indeed, not only social media platforms but also other entities can make such inferences based on publicly available information from these platforms. An example of this is a 2022 case in which the Belgian and French data protection authorities sanctioned an NGO for publishing a study in which it created a political profile of over 3,300 Twitter accounts without anonymizing the Personal Data of account holders.[50] By engaging with beneficiaries on social media, Humanitarian Organizations contribute to the generation of the data and metadata

46 Adapting to current technological changes affecting the humanitarian landscape, social media and other connected means have been suggested as a possible alternative to physical contact by the ICRC. The ICRC's guidelines on how to organize such communication and other actions responsibly are summarized in: ICRC, *Accountability to Affected People Institutional Framework*, Publication, ICRC, Geneva, 15 February 2019: www.icrc.org/en/publication/accountability-affected-people-institutional-framework.

47 See for example: Jane Wakefield, "Sri Lanka Attacks: The Ban on Social Media", *BBC News*, 23 April 2019, Online edition, sec. Technology: www.bbc.com/news/technology-48022530.

48 See for example: Privacy International, "Guess What? Facebook Still Tracks You on Android Apps (Even If You Don't Have a Facebook Account)", Privacy International, 7 October 2020: https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report; Privacy International, "How Apps on Android Share Data with Facebook – Report", Privacy International, 29 December 2018: http://privacyinternational.org/report/2647.

49 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 89–90.

50 Autorité belge de Protection des Données, *Décision quand au fond 13/2022 du 27 janvier 2022*, 27 January 2022.

from which these inferences are made.[51] Furthermore, it should be noted that not only can these inferences be used to target and even discriminate against social media users, but may also be used to manipulate them. In this regard,

> *Targeting mechanisms are, by definition, used in order to influence the behaviour and choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens engaged in civic life. Certain targeting approaches may however go so far as to undermine individual autonomy and freedom (e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values, or concerns).*[52]

It is also important to consider that social media platforms change their terms and conditions, privacy policies and Processing activities very frequently, without always requesting users' Consent. In addition, although users may understand that the platform processes declared data, platforms may not be transparent about what they infer from such data – and, more importantly, from information obtained from other sources (such as online activity, other users and Third Parties), as well as from data generated by design and default because of the way the platform is designed and operates.[53] The information gathered – and, ultimately, the decisions made on the basis of these data – can severely and adversely affect a user's life, as the example below shows:

> Social media data are being increasingly used to assess the credibility of users requesting loans and to monitor those who have already been given a loan. These assessments are based on a selection of indicators that categorize people as either a "reliable, trustworthy borrower" or an "unreliable, risky borrower".[54]

Aside from the risks associated with the sharing of data by beneficiaries on social media platforms, Humanitarian Organizations must also be mindful about the content they themselves share. Some content, such as public photographs or videos including beneficiaries, can have negative consequences for the individuals in question, from profiling and targeting by companies, to persecution, intimidation and blackmail, discrimination, identity theft and loss of control over their data.

Organizations should also remember that social media may not always be the most useful or effective way to reach a given audience. Social media use is often limited in rural and remote areas, and not all members of a target population may have equal access to technology. Likewise, in some contexts, most social media users will be male, so using platforms for women's health initiatives is unlikely to be effective.

51 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 91.

52 European Data Protection Board (EDPB), *Guidelines 8/2020*, 7.

53 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 102.

54 Ibid., 106. See also: Privacy International, "Fintech", Privacy International, accessed 21 February 2022, https://privacyinternational.org/learn/fintech.

14.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

When Humanitarian Organizations use social media for communication purposes, their role in relation to the Processing of beneficiaries' Personal Data is often not entirely clear. When organizations set up an institutional page or profile on a social media platform, for instance, the platform's terms and conditions might allow the provider to process more data through that page, or to profile users for advertising purposes. Here, the organization could arguably be considered a joint controller with the platform, and therefore bears part of the responsibility for the Processing. However, when an organization simply uses the platform to interact with beneficiaries through a page, profile or group created by beneficiaries themselves, it is harder to establish the organization's role and the extent of its responsibility.

EXAMPLE OF JOINT CONTROLLERSHIP:

In 2018, the Court of Justice of the European Union (CJEU) ruled, in case C-210/16, that administrators of Facebook pages are Data Controllers in relation to the Personal Data collected and processed by Facebook through their fan pages (a fan page is an institutional page, created by the company or organization on the Facebook platform, to communicate with Facebook users and share content about their work).[55] As fan pages are hosted on the Facebook platform, Facebook gathers information about those who access or interact with them, regardless of whether they have a Facebook account. Facebook uses this information to produce statistics about fan page visitors, which are shared with the page's administrator.

According to the Court, the administrators of such pages (i.e. the organizations that create and manage them) are Data Controllers because creating the fan page "gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account" (para. 35). Furthermore, where administrators define specific parameters to be collected by Facebook to benefit from statistics about the page's visitors, they are considered to be taking part in the determination of the means and purposes of the Processing.

Although this ruling relates to the European Union regulatory context and only concerns Facebook,[56] the influence of EU data protection law means that this broad

55 Court of Justice of the European Union (CJEU), Case 210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Judgement ECLI: EU:C:2018:3885, June 2018.

56 The European Data Protection Board interpreted that joint controllership in activities involving targeting social media users would apply to all social media platforms offering such services. See their analysis of the roles and responsibilities of joint controllers in multiple targeting activities in: European Data Protection Board (EDPB), *Guidelines 8/2020*.

(albeit controversial) definition of controllership may also be adopted in other regions. Should that be the case, Humanitarian Organizations might be considered Data Controllers in relation to the Processing of Personal Data by the social media platforms they use in relation to their page. In practice, this means that, where the platform processes Personal Data collected through the organization's page for non-humanitarian purposes, the organization in question could be responsible for such Processing.

Humanitarian Organizations must therefore do everything they can to fully understand the business models, privacy policies and security protocols of the social media platforms they use, since they could be held liable for misuses by the platform and other Third Parties. If there are any doubts regarding compliance with data protection, human rights and humanitarian principles, organizations should always choose a safer communication option. It is important to note, however, that in some cases Humanitarian Organizations may have no other alternative to reach certain populations, due to their predominant use of a specific social media platform and possible reluctance to use other means of communication. Regardless of choice limitations, however, Humanitarian Organizations should do everything in their capacity to mitigate possible risks arising from their use of such tools.

14.5 BASIC DATA PROTECTION PRINCIPLES

14.5.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

While Humanitarian Organizations cannot control how social media platforms operate and process data, they should still determine the legal basis for Processing data that they may request and/or receive through social media.

Consequently, Humanitarian Organizations must identify a legal basis for each Processing activity.[57] As mentioned above, organizations frequently use the same social media page or profile both for their humanitarian work, and for campaigning[58] and fundraising, which may make it difficult to differentiate each purpose in practice. For instance, Humanitarian Organizations may sometimes use images of beneficiaries in public relations campaigns. Where Consent is relied upon, an individual must be able to withdraw Consent. Yet once an image or video is published online, the

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

58 For example, in 2019, the IFRC chose to use its institutional TikTok account as the main tool to promote a global flagship campaign to foster climate action. See: Dante Licona and Melis M. Figanmeşe, "We Were the First Global Humanitarian Organization to Partner with TikTok", Medium, 22 October 2019: https://medium.com/digital-diplomacy/we-were-the-first-global-humanitarian-organization-to-partner-with-tiktok-ea16b280d51.

organization may lose control of its copies and reproductions and, should a beneficiary withdraw Consent, the organization may not be able to remove the content entirely. In such cases, it is important to consider the purpose of each element of a Processing activity and to document it accordingly.[59]

14.5.2 INFORMATION

Individuals should be given clear and timely information regarding the Processing of their data by the Data Controller,[60] explaining what data are collected (in order to provide a service, for instance), what data are generated by the use of the service, what the purposes of the collection are and who can access, share and/or use the individual's Personal Data. This information allows Data Subjects to make informed decisions about whether to use a specific service, and to understand how to exercise their rights. Yet when Humanitarian Organizations interact with beneficiaries through social media, the data are primarily generated and processed directly through the platforms themselves, leaving Humanitarian Organizations with little control over the actions mentioned above. Organizations should nevertheless take responsibility for providing relevant information as far as possible.

Again, it should be stressed that platforms regularly change and update their privacy and data protection policies, which can make it very difficult for users to understand what data are being generated and processed (i.e. how they are used and with whom they are shared).[61] It is therefore challenging for Humanitarian Organizations to understand the risks that using social media platforms presents, and it is unclear what information organizations should provide to Data Subjects. Humanitarian Organizations are advised, at the very least, to inform beneficiaries about the Processing activities for which they are responsible – for instance, explaining why they are communicating through social media, and how the information beneficiaries share with the organization will be used and for what purposes.

Although Humanitarian Organizations have no control over what social media platforms do with the data they collect, some organizations have carried out online awareness-raising campaigns to explain the risks associated with social media and what actions beneficiaries should take to protect their data. In Mexico, for instance, UNHCR uses the El Jaguar page to communicate with beneficiaries. The organization produced a video, shared via the page, warning beneficiaries about the risks associated with using Facebook and how to minimize them.[62]

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

60 See Section 2.10 – Information.

61 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 17.

62 See the campaign video (in Spanish) at: El Jaguar, "Privacidad En Facebook", Facebook, 27 October 2018: www.facebook.com/ConfiaEnElJaguar/videos/874221649451680.

Campaigns like these help beneficiaries understand the chain of parties and organizations that may have access to the data they produce on social media, and the risk of harm that might come from these platforms. Yet informing beneficiaries about social media data and privacy policies may not prove helpful if they cannot find an alternative to their current platform. Instead, Humanitarian Organizations should focus on informing beneficiaries about the potential and most likely risks they will encounter when, for instance, they join their groups or follow their pages on social media, and on explaining whether membership of such communities may be visible to others or may be used against them in any way. This is particularly important since, data protection concerns aside, social media use poses other risks such as surveillance and consequent identification (and potential location) of vulnerable people and groups by ill-intentioned parties.

14.5.3 DATA RETENTION

According to the data retention principle, data should be retained for a defined period necessary for the purposes for which they were processed. This period can be three months, a year, the duration of a crisis or some other time frame.[63] When it is not possible to determine the retention period at the time of collection, a review should be conducted at the end of an initial predefined period.

When Humanitarian Organizations interact with beneficiaries through social media, the platforms themselves collect and retain their data. The retention period will therefore vary from one platform to the next.

EXAMPLE OF FACEBOOK'S DATA RETENTION POLICY:

Facebook's data policy stipulates that data are retained until they are no longer necessary to provide the services or until the account is deleted, although there is evidence that the platform keeps some data even after deletion of the account.[64] The policy explains further:

> *This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after review, unless otherwise stated.*[65]

63 See Section 2.7 – Data retention.

64 Aimee Picchi, "OK, You've Deleted Facebook, but Is Your Data Still out There?", *CBS News*, 23 March 2018, Online edition, sec. Moneywatch: www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there.

65 Facebook, "Data Policy".

Some social media platforms may share data or information with Third Parties. These parties may also have different data retention rules in place. The fact that social media users have to agree to the terms and conditions in order to use these services raises questions about accepting Third Parties' retention policies. Humanitarian Organizations should therefore analyse these policies, assess whether they pose risks to beneficiaries or to the organization itself, and make an informed decision as to whether it is appropriate for the organization to use the platform for its intended objective.

Humanitarian Organizations are also responsible for setting retention periods and/or policies for the data they collect from beneficiaries through social media interactions, groups and pages. They should explain these periods and/or policies to both their staff and beneficiaries.

14.5.4 DATA SECURITY

Humanitarian Organizations should carry out a DPIA (see Section 14.2 – Data Protection Impact Assessment, above), taking into account the platform's business model, policies, and terms and conditions, the wider ecosystem, and whatever security measures the platform takes to protect the data it processes. While the platform may not share this information openly, analysing previous Data Breaches, the platform's response and other known vulnerabilities may be a useful starting point. It is also important to understand how the platform processes users' data and what measures it has in place to guarantee those data are kept safe.

Internally, Humanitarian Organizations are advised to ensure they take appropriate measures to protect the data they collect from beneficiaries, such as protecting data with login and a strong password, granting access on a need-only basis, and training their staff to handle data correctly.

14.6 INTERNATIONAL DATA SHARING

Data processed through social media platforms routinely flow and are accessed across national borders, which raises Personal Data protection concerns. Although recognized contractual mechanisms exist, it can be difficult for Humanitarian Organizations to implement them effectively, especially since social media platforms are often outside their control. That said, organizations must do whatever they can to ensure that the provider has implemented the necessary data transfer arrangements.[66] Determining applicable law and jurisdiction can also present challenges, since a proper and targeted risk analysis is impossible unless choice of jurisdiction and choice of law are clearly embedded in social media governance.

66 See Chapter 4: International Data Sharing.