unicef INNOVATION

unicef Office of Research-Innocenti

Ethical Considerations When Using Social Media for Evidence Generation

Gabrielle Berman, James Powell and Manuel Garcia Herranz

Office of Research - Innocenti Discussion Paper
DP-2018-01 | June 2018

unicef | for every child

THE UNICEF OFFICE OF RESEARCH – INNOCENTI

The Office of Research – Innocenti is UNICEF's dedicated research centre. It undertakes research on emerging or current issues in order to inform the strategic directions, policies and programmes of UNICEF and its partners, shape global debates on child rights and development, and inform the global research and policy agenda for all children, and particularly for the most vulnerable.

Publications produced by the Office are contributions to a global debate on children and may not necessarily reflect UNICEF policies or approaches. The views expressed are those of the authors.

The Office of Research – Innocenti receives financial support from the Government of Italy, while funding for specific projects is also provided by other governments, international institutions and private sources, including UNICEF National Committees.

INNOCENTI WORKING PAPERS

The findings, interpretations and conclusions expressed in this are those of the authors and do not necessarily reflect the policies or views of UNICEF.

The text has been reviewed both externally and within UNICEF. The text has not been edited to official publications standards and UNICEF accepts no responsibility for errors.

For readers wishing to cite this document, we suggest the following form: Berman, G., Powell, J., and Garcia Harranz, M. Ethical Considerations When Using Social Media for Evidence Generation, Innocenti Discussion Paper 2018-01, UNICEF Office of Research - Innocenti, Florence.

Correspondence should be addressed to:
UNICEF Office of Research - Innocenti
Piazza SS. Annunziata, 12
50122 Florence, Italy
Tel: (+39) 055 20 330
Fax: (+39) 055 2033 220
florence@unicef.org
www.unicef-irc.org
twitter: @UNICEFInnocenti
facebook.com/UnicefOfficeofResearchInnocenti

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals for their useful insights and review of this paper: Tanya Accone, Kerry Albright, Tamima Boutel, Mads Olsen, Christian Larsson, Katarzyna Pawelczyk, Toby Wicks, Emily Garin and Hye Jung Han. We would also like to thank Stuart Campo from the Harvard Humanitarian Initiative for his valuable input.

TABLE OF CONTENTS

Introduction: Social media ... **6**

Section 1: Evidence generation through social media-based programmes ... **7**
1.1 Benefits of evidence generation using social media platforms ... **7**
Benefits to children engaging with social media programmes that involve evidence generation ... 7
Benefits in using social media for evidence generation in organizational programmes ... 8
1.2 Risks of evidence generation using social media platforms ... **10**
Age-based concerns ... 10
Privacy, confidentiality and security ... 11
Risk aversion leading to lost opportunities ... 13
Risks relating to data quality and use of data ... 13
1.3 Ethical considerations for evidence generation using social media ... **16**
Determining the value of the data and obligations to those providing it ... 16
Ensuring the confidentiality of data ... 17

Section 2: Using third party data collected and analysed by social media services ... **20**
2.1 The benefits of using third party data and/or analysis from social media services ... **20**
2.2 The risks of using third party data and/or analysis from social media services ... **21**
Silencing children's voices ... 22
Privacy, confidentiality and security ... 22
Risk aversion leading to lost opportunities ... 22
Informed consent ... 22
Risks relating to data quality and applications ... 23
2.3 Ethical considerations when using third party data collected and analysed by social media services ... **25**
The value and timeliness of the data ... 25
National and organizational privacy frameworks ... 25
Consent and transparency ... 26
Use of a risk assessment framework ... 26
Aggregation of findings to avoid or limit identification of groups or individuals ... 27
Understanding the data and limitations ... 27
Understanding the implications of algorithmic based findings ... 28

Conclusion: Reflections on the longer term ... **29**

Bibliography ... **30**

Annexes
Annex 1: Checklist of ethical issues for consideration when using social media for evidence generation ... 33
Annex 2: Checklist for partnerships with social media providers ... 35
Annex 3: Social media privacy settings ... 38
Annex 4: Privacy-friendly features of messaging apps ... 39
Annex 5: Example of social media safety tips ... 40
Annex 6: Data privacy and data protection principles (United Nations Global Pulse (2016) ... 41

GLOSSARY

Algorithm: A step-by-step procedure for solving a problem or accomplishing an end, especially by a computer.

Big data: Data sets that are so large or complex that traditional data processing applications are inadequate to deal with them (Canavillas et al., 2016).

Bot or 'chatbot': A piece of code or software that performs specific automated functions within an app. For example, it may provide information when a user requests it (often in natural language that makes it resemble a human operator – hence 'chatbot'), request information from another user, or provide a means of linking to other web services.

Crowdsource: Obtain (information or input into a particular task or project) by enlisting the services of a large number of people, either paid or unpaid, typically via the Internet.

End-to-end encryption: A system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation (Greenberg, 2014).

Evidence generation: Evidence generation at UNICEF includes all research, evaluations and data collection and analysis activities.

Messaging app: A mobile-phone-based software programme that allows users to send and receive information from and to their phones over an Internet connection (either via Wi-Fi or mobile data networks).

Metadata: Metadata provides descriptors on content and related activities, in relation to web-based content and visual and alphanumerical databases. Within social media platforms, this can include data on when the account was created, by whom, the number of logins, number of posts and links, the technology on which the service is accessed and where etc. The presence of metadata enables data and sites to be searched.

Social media: Forms of electronic communication through which users create online communities to share information, ideas, personal messages and other content.

Smartphone: A mobile phone offering advanced features, typically including a GPS sensor, the ability to access the Internet over mobile-phone networks and Wi-Fi connections and the capacity to download apps from the Internet.

Feature phone: A mobile phone that has very basic multimedia and Internet capabilities.

SMS (Short Message Service): A service for sending short messages of up to 160 characters to mobile devices, including mobile (cellular) phones and smartphones, digital phones and web-based applications within a web browser.

Webscraping (also known as screen scraping, web data extraction, web harvesting): A technique that uses specialized software to extract large amounts of data from websites.

ACRONYMS

API	Application Programming Interface
DII	Demographically identifiable information
ICT	Information and communication technologies
PII	Personally identifiable information
SDGs	Sustainable Development Goals
SMS	Short Message Service
SNS	Social Network Service
WAGGS	World Association of Girl Guides and Scouts

INTRODUCTION: SOCIAL MEDIA

As of January 2017, 2.78 billion people worldwide were classified as active social media users. Of these users, 1.87 billion use Facebook. In turn, 39 per cent of these users are between the ages of 13 and 24 (approximately 729 million young people). Available data also shows that in 2014, approximately 31 per cent of users of the top five social media platforms were aged between 16 and 24 years. With the enormity of this coverage as well as over 40 per cent growth in usage from the previous year in countries like India, UNICEF has and continues to look at ways to use these platforms and the data generated to connect with and understand the reality of children today and to ensure more child-centred/user-centred policies and services.

However, while recognizing the influence and power of these networks, it is also necessary to acknowledge the ethical issues presented by these platforms and services in terms of both risks and benefits. Ethical issues arise not only with respect to the privacy settings and confidentiality of data amassed by these applications and platforms, but also in relation to the use of the 'big data' that is produced via social media for predictive modelling, trend analysis and consequently for decision making and influence.[1]

There are significant ethical implications in the adoption of technologies and the production and use of the resulting data for evidence generation. The potential benefits and opportunities need to be understood in conjunction with the potential risks and challenges. In the past, understanding the technologies, data and data analytics was, primarily the domain of experts. However, as noted by Berman and Albright (2017), this is an area where it is no longer sufficient for users of data and technologies to leave ethical reflection to subject matter experts. Rather, data providers (i.e. the social media users that indirectly provide data through their interaction with the social media platform), child advocates who use social media data, need to be brought into the conversation and to understand and reflect on the ethical implications of the use and potential outcomes of adopting these technologies and the data they generate. For the reasons noted above, understanding the ethical implications of using social media platforms for programming involving evidence generation and/or of using third party data provided by social media services is critical, if we are to ensure that the rights of children are secured and respected.[2]

A couple of caveats should be noted. In light of the complexity and diversity of the legal frameworks for social media, legal considerations are largely beyond the scope of this paper and are not explored in detail beyond basic considerations and guidance on when to approach an organization's legal office.

Further, it should be noted that this paper does not explore issues related to social media, evidence generation and ethics in humanitarian contexts extensively. This is premised on the belief that while several ethical issues pertaining to social media and evidence generation apply to humanitarian contexts, the ethics of social media use within these circumstances are more complex, particularly considering the requisite contextualization within the suite of humanitarian standards. Hence, this paper cannot and does not attempt to cover the wide scope of ethical issues in these difficult contexts and within their frequently highly prescribed response planning and systems. This is, however, an area that will require explicit focus and research in the future.

1 For the purposes of this paper, big data is defined as data sets that are so large or complex that traditional data processing applications are inadequate to deal with them (Canavillas et al., 2016).

2 It should be noted that the ethical concerns raised by social media platforms and the data they generate also apply to the adoption of Information and Communication Technologies more generally. This, however, is beyond the scope of this paper.

Finally, it should be noted that while several risks exist in the use of social media, these do not necessarily preclude the valid and valuable use of social media data. Rather, risks need to be enumerated, articulated and understood if we are to establish strategies to address these issues and to best meet the rights of the child.

SECTION 1: EVIDENCE GENERATION THROUGH SOCIAL MEDIA-BASED PROGRAMMES

This section reflects on the potential benefits and risks of programmes that use social media to engage children and their communities and to undertake evidence generation. It should be noted that the risks do not necessarily preclude the use of social media for evidence generation but rather highlight the need for reflection and development of mitigation strategies to address them. To this end, this section also enumerates the ethical considerations that need to be taken into account when using social media programmes for evidence generation.

1.1 Benefits of evidence generation using social media platforms

When considering the ethical implications of evidence generation involving social media, there are several potential benefits for both children and their communities.

Benefits that may accrue to children involved in social media programmes that collect data from children for evidence generation:

- **Providing a voice on matters that affect them.** Social media services have created new forms of 'safe' spaces for children and young people to initiate or become involved in civic engagement activities by allowing for information sharing and the bringing together of young people to plan and engage in various political and social actions (Montgomery 2007; Vromen 2007; 2008).
- **Possibility of two-way engagement and consequent access to support and advice.** Social media programmes can provide safe spaces for children to access services, information and advice that may not be available or socially acceptable to seek within the local, physical environment (Bender et al., 2011; Moorhead, 2013). Through engagement and interaction, young people can be made aware of resources, such as information, helplines and referral mechanisms. Social network services can drive demand side requests and in turn, generate evidence to support resourcing of these services. As we strive for greater cost efficiencies across all programmes, the benefit of free or low cost mechanisms that facilitate engagement and evidence generation involving children and young people is becoming more important as traditional, higher cost sources of information and communication become less affordable.

Case study: Ebola and WhatsApp

During the 2014 Ebola crisis in Sierra Leone, more than 12,000 people signed up for WhatsApp groups organized by BBC Media Action which allowed them to send comments, questions and programming requests. An evaluation of the project also found that people were keen to share their experiences publicly, suggesting that this activity may not only serve as a vehicle for dissemination of information but also meet refugees' psychosocial need to express themselves (BBC Media Action, 2015). According to the findings, this service also provided a vital lifeline to other people at a time when physical contact or gathering in groups was not advisable or in some cases not allowed.

Benefits in using social media for evidence generation in organizational programmes

Using social media services in organizational programmes to collect and exchange information has a number of benefits:

- **Advocacy and participation.** With respect to the organizational advantages for UNICEF, social media services provide an extraordinarily powerful platform for advocacy, enabling both passive and active engagement of large populations. Digital marketing and social media strategies not only allow for global dissemination of messages (on a scale that far exceeds historic communications mediums) but also provide a vehicle for the empowerment of children to voice their opinions and raise awareness of issues that affect them (Moestue and Muggah, 2014). It should be noted that the potential reach of social media has had significant impacts in relation to marginalized and traditionally hard-to-reach children and their communities.

- **Providing a voice for the voiceless.** Directly related to the point above, social media can and has been used to give a voice to those affected by violence. This is particularly important given that under-reporting of violence against children is common. Fear of an abuser is one of the primary determinants of under-reporting, which may be compounded by the fact that traditional reporting systems can be overly bureaucratic, slow and stigmatizing. The potential anonymity afforded by mobile or web-based reporting can provide a vehicle to allow people, including children, to report on and speak about sensitive subjects (including abuse) in locations where these issues remain taboo and/or informally sanctioned by social norms (Moestue and Muggah, 2014).

- **Engaging communities to understand and consequently address social norms and encourage positive/pro-social behavioural change.** Case studies show that the use of social media for evidence generation may, in turn, positively impact behavioural change through heightened awareness of peer and community attitudes. For example, awareness of peer participation in voting has been shown to have a strong relationship to peer voter registration (Bond et al., 2012).

- **Raising awareness of key messages and engagement on issues that support the rights of the child and UNICEF's programming.** The sheer reach of social media as previously noted, facilitates the possibility of communicating vital UNICEF messages to millions of people. Traditional media is a fragmented ecosystem which means reaching millions with a message critical to young people is not only costly, but also complicated and burdensome to plan and successfully execute. UNICEF Bangladesh recently showed that with relatively limited resources, a social media programme was able to access and engage millions of persons. In a similar vein, the following case study reflects on this type of work on a global scale.

Case study: Menstrual hygiene management live chat (Part 1)

As part of the 2017 Menstrual Hygiene Day programme, UNICEF WASH and the Global Innovation Centre launched a poll using U-Report that asked girls whether they attend school during their period. The polls differed slightly by country, mostly targeting girls and some including specific questions for boys. This successful programme elicited responses from over 45,000 U-Reporters across 19 countries via SMS, Facebook and Twitter.

Informed by the poll, a live chat on menstrual hygiene management was undertaken using U-Report Global via Facebook Messenger, Twitter Direct Message and Viber. The live chat was set up by the Global Innovation Centre and messages were to be answered by UNICEF programme specialists with assistance from the World Association of Girl Guides and Scouts (WAGGS). To prepare the team responding to messages for the live chat, WASH, Gender and Adolescent Development programme specialists prepared 65 frequently asked questions that addressed key topics with advice provided by the Office of Innovation on length and language. Over a period of three hours, 540 messages were received from U-Reporters and responses were provided to nearly 431 of these.

The learning from this project is now being applied in Nigeria, and consequently a doctor will be available to respond to any medical questions that may be posed.

- **Social media can provide a vehicle for greater transparency and accountability** of organizations working with and for children. In light of the open nature of networks, social media can provide greater accountability through the provision of forums and mechanisms for evidence generation, facilitating engagement with and input into decision-making processes.
- **Social media platforms can also be used to provide real-time information on events as well as environmental and social conditions (Phillips et al., 2017).** The advent of bot platforms has enabled the collection of data from an unlimited number of people in real time. Facebook, LINE and Viber have already developed bot platforms, primarily for monetization of their platforms to e-commerce companies. However, these platforms have an adaptable purpose in development contexts whereby automated bots containing potentially lifesaving information can receive queries from millions of people, collect their information, questions or messages for analysis in real time, and then offer a seamless, immediate response. The full potential may yet to be realized (and the sophistication of responses may not yet be equivalent to human interaction). However, the possibility to receive timely information and offer a timely response now exists.
- **Crowdsourcing to gather information and for real-time monitoring.** Crowdsourcing can facilitate the gathering of information including on rapidly changing events or unreported incidents. It can provide data in instances where accessibility was previously not possible or where volatility or lack of security and danger impede comprehensive data collection. In these contexts, crowdsourcing can also provide a sense of community and community engagement for those involved (Omoush al- and Yaseen, 2017).
- **The low costs of using social media or social media data**. Many social media platforms are free to access, or low cost/free access can be negotiated via agreement. In resource-constrained environments they present opportunities for engagement of child audiences at a scale that was previously prohibitive. Furthermore, social media companies have hitherto provided UNICEF and other UN organizations (e.g. Global Pulse) with free access to their APIs (application programming interface software), allowing for qualitative or quantitative analysis of data collected without access to the raw, personally identifiable data.

Case study: U-Report – chatbots and social media

In April 2016 at Facebook's annual developer conference, F8, UNICEF launched a chatbot that integrates with U-Report, a service running in 28 countries worldwide that allows young people to answer polls and report on a broad range of development issues in their communities. U-Report, which uses the open source software platform RapidPro, was built to receive information primarily through SMS. Although it will continue to do so, messaging apps have been added as further communication channels because it was recognized that as people have more access to the Internet, they will have a preference for using apps that they are already using. The introduction of messaging apps was also seen as a way to reduce messaging costs, as SMS costs were relatively more expensive in many countries. The bot is integrated with Facebook Messenger and Telegram, and UNICEF worked directly with a team from Messenger to implement the integration. It asks young people a weekly series of questions about issues that affect them, including education, sexual and reproductive health, access to health services and their legal rights. Messenger has enabled UNICEF and its partners who run the platform to connect a wide range of countries. Users' answers are recorded in a database, analysed in real time and shared in aggregated form on public websites, with UN agencies and programmes and with decision makers. When UNICEF and the U-Report partners receive unsolicited messages on a specific issue from members known as 'U-Reporters', UNICEF's partner organizations can log in and respond using a separate piece of software (CasePro – which uses anonymous ID numbers) that recognizes keywords relating to those partners' areas of expertise. For example, in Uganda, UNICEF's partner, the HIV/AIDS organization Mildmay, will respond to messages received that ask questions about HIV/AIDS (reported in ICRC et al., 2017).

1.2 Risks of evidence generation using social media platforms

This section outlines the potential risks of using social media for evidence generation. As noted previously, these risks do not necessarily preclude the use of social media for evidence generation, but rather should, at a minimum, inform clear risk mitigation strategies.

While some of the risks noted below pertain exclusively to children, many apply to both children and their communities and require considered reflection to ensure ethical evidence generation.

Age-based concerns

- **Lack of awareness of legal age requirements for children's participation.** The age below which children legally should not access social media or need informed consent to use social media services varies according to the terms and conditions of the social media service and any relevant local legislation. This has implications for the legal age range that can and should be targeted to for participation in evidence generation programmes involving social media.
- **Difficulties in verifying the age of users online** (UNICEF Innocenti, 2011). The difficulty of verifying children's ages calls for significant reflection when considering the sensitivity of the subject matter for evidence generation involving children.
- **Children may be legally entitled to have their data removed from social media servers and other databases containing this data**[3] even if they previously provided consent for the use of their data or if their parent provided consent. The risk here is the potential difficulty in identifying and removing

3 Under the EU General Data Protection Regulation (2016), this may also apply to adults. However, specific consideration is given to children notably in relation to consent and ethics.

the data from all databases. For countries of the European Union, this regulation is in force as of 25 May 2018. Under the European General Data Protection Regulation, if consent was provided during childhood, the right to have information removed will continue into adulthood. Further, if the personal data in question has been shared with third parties, they must be instructed to erase this personal data, unless it is impossible to do so. This legal requirement will need to be considered if UNICEF is to use data from children in Europe.

- **Difficulties authenticating parental consent.** In terms of ensuring parental consent, there is little if no guidance within pre-existing regulations as to how providers can and should authenticate parental consent when this is required by legislation or organizational terms and conditions for the sharing of data. Further, there are few if any effective mechanisms for oversight of this process. Hence, it is incredibly difficult to verify whether the parent has, in reality, provided informed consent.

Privacy, confidentiality and security

The following risks pertain to the potential for invasions of privacy, breaches of confidentiality and compromised security of persons providing data and information in evidence generation activities using social media platforms.

Privacy and confidentiality issues that pertain directly to children:

- **There are heightened risks associated with identification when the subject matter is sensitive** (e.g. discussions regarding sexuality or political positions) or the participants are vulnerable within the context (Elgesem, 2015). 'Harm is defined contextually and assessing how to conduct ethically sound research must be made according to the specific context' (Luders, 2015: 81). This is particularly relevant when working with children in light of the significance and impact of digital footprints on a child's digital identity and, in turn, their offline development and socialization (Berman and Albright, 2017).

  Related to the above is **the ease with which quotes can be traceable on the Internet** and the consequent difficulties in maintaining the anonymity of children and young people if the quote is attached to any identifying information. Even pseudonyms may be problematic if the individual uses the same pseudonyms in different settings (Elgesem, 2015).

- **Determination about what is considered private by participants in the programme and what is public cannot always be made and hence privacy/confidentiality conditions and arrangements need to be clearly, simply and explicitly defined and stated in agreements to participate and/or prominently displayed on the landing site of a platform**. As noted by Luders (2015) in her research, young people can perceive their presence within social media as private even though the technology is public and hence privacy conditions need to be communicated, to allow children to make an informed decision as to whether they wish to participate.

- **Risks exist as a result of the persistence/enduring nature of data on the Internet.** Data collected over the Internet is frequently automatically registered and stored and/or shared. The persistence of data collected for children is particularly problematic given the enduring nature of the data and its potential to impact them over their lifetime with significant implications for their public/digital identity, their capacity to shape this sphere, and longer term impacts and outcomes (Ess, 2015;

Berman and Albright, 2017). In light of this persistence, securing permanent and universal removal of data on request may not be possible.

Privacy, security and confidentiality issues relating to social media use for evidence generation for all participants:

- **Terms and conditions of social media services frequently do not allow participants to exempt their data from being shared with a host of organizations determined by the company.** These organizations can include: the family of companies owned by the social media company; vendors; service providers, including analysts and research institutions; and other partners. Consequently, participants must relinquish a degree of control over the sharing or their data as an agreement of use of service (Berman and Albright, 2017) or simply not use the service.
- **Privacy settings on social media services may change rapidly without consultation** or public disclosure (ICRC et al., 2017) with implications for the confidentiality of social media user data relating to the number and nature of third parties with whom they share this data.
- **There are different legal ramifications (including those related to privacy and security) when creating a new platform (or tailoring an open source platform) as opposed to using an existing social media platform**. If/when creating a new platform, terms and conditions need to be established at the outset to ensure appropriate protections for participants. Appropriate terms and conditions would need to be established to ensure that the platform's approach to data handling does not contravene existing local legislation and international regulations. In these instances, the organization's legal office should also be consulted.
- **Sharing of phones within families and communities may** pose the risk that activities and communications of participants are accessible beyond the targeted participant (Hosein and Nyst, 2013). It should however be noted that this may be perceived as a benefit in contexts of reaching or engaging children that may otherwise be unreachable. This may be particularly relevant for the most marginalized.[4]
- **Restrictions and blocking of social media use**. According to the publication *Silencing the Messenger: Communication Apps under Pressure: Freedom on the Net 2016*, governments in 24 out of 65 countries were assessed as impeding access to social media and communication tools between June 2015 and May 2016. This is up from 15 the previous year. WhatsApp faced the most restrictions, with 12 out of 65 countries blocking the entire service or disabling certain features (Kelly et al., 2016). These types of restrictions can limit the efficacy of social media programmes and impact the robustness of time-sensitive data from these countries.
- **False crowdsourcing platforms** may be used to track individuals espousing opposing political or social views and opinions (Al Omoush - and Yaseen, 2017). While this may not be a direct risk of an organizational platform, it does have implications regarding the need for clear branding of any social media based programme and its online presence.

4 South Africa, where only 34 per cent of 8–13 year-old children own a phone but 78 per cent have accessed one in the last four weeks, is a case in point (Hampshire et al., 2015). Accessing other people's phones may facilitate communication for marginalized communities. However, it may also present a risk in the context of communications on sensitive subjects.

Risk aversion leading to lost opportunities

- **Dismissing the value of using social media** (without being informed by an appropriate risk-benefit analysis) for evidence generation and missing significant opportunities to ensure results for children.

Risks relating to data quality and use of data

There are a number of potential risks that need to be considered relating to the data obtained via social media platforms. These risks pertain to various phases of evidence generation from collection, processing and sharing, to the analysis and finally the use of data for decision making and assessment. It should be noted that many of these risks are similarly applicable to existing traditional data collection practices.

Potential risks of data processing

- The time required to clean and validate data sets so that they are useable to those on the ground may make social media data use redundant, particularly in contexts where information is time sensitive. In the instance where a social media platform is used because of its perceived timeliness, this may present a more significant risk.

Potential risks of data sharing

- Lack of data stewardship by the social media service or by UNICEF programme management may result in a failure to ensure that access to personally identifiable information (PII) data is limited if this is not explicitly articulated in MOUs or contracts and/or noted within policies and procedures of participating parties.
- Even when data is de-identified, there is the always the potential for re-identification of the data when combined with other data sets.

Potential risks of data analysis

- Poor problem definition can lead to data being analysed in a way that does not add value and therefore diverts time and resources from other activities.
- Data analysis may result in data that does not personally identifying a specific individual but may still enable them to be tracked or classified according to ethnicity, class, gender, age, health, location, occupation or other demographic data (known as demographically identifiable data – DII). This in turn, could result in discrimination against the individual.

Potential risks of data use

- Using the data to generalize to the population when it is not representative. In this case, the generalizability of the findings is likely to be limited, requiring significant caveats and clear articulation of populations omitted when findings are presented.
- The usability of the data and analysis will also depend on the technology infrastructure. In contexts where Internet connectivity may be limited or subject to consistent disruptions, the system may be unreliable and its use for real-time monitoring may be questionable.
- The accuracy and reliability of crowdsourced data cannot be assumed and needs to be interrogated prior to acting on this information.

Potential risk of data storage

- Despite UNICEF adopting practices and partnering with organizations that adopt best practice as pertains to the security of data, personally identifiable data stored on cloud or physical servers could still be accessed or stolen by governments, militants or malicious parties. This could occur through hacking, access to backdoors, or as a result of legislative provisions.

Potential risk related to data disposal

- The primary risk relating to disposal of data is that the data is not appropriately or fully disposed of and that it remains on servers, both known and unknown.

Case study: Considerations when using WhatsApp and Facebook Messenger to collect data

Ahead of South Africa's municipal elections in August 2016, the non-profit organization 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 matter to them. 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.

Africa's Voices Foundation felt that their use of WhatsApp groups encouraged conversations that would yield particularly useful feedback. However, the foundation had concerns about privacy when using both Facebook Messenger and WhatsApp, noting that informed consent was sought and data was stored securely but that they could not control how the data would be used in the future (due to lack of ownership of the data). This was viewed as particularly problematic because personal information such as voting and demographics were requested of participants. "They decided not to undertake a similar project again if the privacy risks were not well understood in advance." (ICRC et al., 2017, p. 67).

Box 1: Technical considerations relating to privacy and security features when selecting a social media platform for evidence generation.

When considering using social media services for evidence generation and communication, **the legal, social, political and organizational contexts should be investigated or understood and taken into account.** This includes engaging in critical reflection on these issues when: deciding whether to use the social media platform; considering the choice about which social media service to use; or informing participants/social media users of potential privacy risks. When undertaking this assessment, the following should be considered:

- The terms and conditions of the social media company including any age requirements for use *(See Annex 3).*
- Any relevant local laws (see Data Protection Laws of the World to find the relevant law/s for your country: https://www.dlapiperdataprotection.com/).
- The subject matter if wanting to engage younger children – particularly given the difficulty of validating informed consent online.
- The local political context and historical and contemporary government access to and blocking of social media services and data.
- The privacy and security features of the social media platform or services considered. These features include:
  - **Whether data is secure in transit/use of end-to-end encryption.** Use platforms that have SSL certificates and are secured by https to ensure that names and contact details are encrypted as they transit online.
  - **Whether anonymity is permitted** i.e. no requirement for authenticated identity, or possibility for individuals to adopt pseudonyms (participants should generally be encouraged to adopt the latter).
  - **Whether there is retention of message content on servers**
  - **Whether, and to what extent, the social media user has control over their personal data and profile.** A socially responsible social media service should make efforts to provide social media users with some control over their personally identifiable data as well as the contents of their messages. The efficient removal of data and profiles and limited or no on-sale of data for commercial purposes are approaches through which an organization can contribute to greater control of data by social media users. The degree of control that social media users have over their personal data may be established and reflected in national laws in some countries and/or within the social media organization's terms-of-service agreements (ICRC et al., 2017).
  - **Whether the social media service company rigorously vets disclosure requests from law enforcement** agencies and openly publishes requests (including source) and information provided.
  - **Whether there is no or minimal retention of metadata**
  - **Whether the surveillance powers of governments are likely to limit or infringe on the privacy of individuals** using a social media service domiciled in that country.

1.3 Ethical considerations for evidence generation using social media

The following are approaches to be considered prior to using social media for evidence generation:

- Determining the value of the data and obligations to those providing the data
- Ensuring the confidentiality of data and protecting participants

Determining the value of the data and obligations to those providing it

- **Reflect on the value of the data.** This will require reflection on the resources and time required to ensure the data is useable. It will also depend on the nature of the data collection, the target community for evidence generation, its added value to current information sources and its potential as a vehicle for two-way communication and advocacy.
- **Reflect on the capacity to respond to requests for help.** Consideration will be required if data collection also allows for personal communications from participants (social media users) and the implications in terms of the capacity to respond if individual requests for assistance are received. In these circumstances, decisions will need to be made as to whether assistance can be provided (Carrion, 2015). The capacity to provide support and the nature of this support or help should be clearly articulated to participants at the outset.
- **Establish referral and/or support services and channels** for when advice or support is requested. Even in online contexts, support services and arrangements should be established prior to data collection or engagement. The use of technology to collect data and communicate with communities and individuals does not obfuscate the responsibility to ensure appropriate protection protocols for participants.

Case study: 2017 Menstrual Hygiene Day programme MHM live chat (Part 2)

The UNICEF and WAGGS teams were well prepared to respond to menstruation and sexual health queries received via the live chat on menstrual hygiene management. However, on later reflection, staff noted that if girls or women had potentially serious medical issues they would not have had any channels for referral in their country. In the future, it is recommended that if Country Offices hold a live chat on menstruation, they develop a clear protocol for responding to medical questions. This protocol would require that a health professional (either a qualified UNICEF colleague or an outside party) be available at the country level to advise or refer girls to services in their country, particularly in instances where serious medical issues were highlighted.

Ensuring the confidentiality of data

- **Wherever possible and appropriate, ensure data is anonymized** from start to finish. This would include making it clear to participants that they should not provide any PII data[5] unless absolutely necessary and, in the instance of children, unless vital to their health or well-being.[6] It is advisable to let participants know what location data is being collected and why and to ensure that publicly available data is aggregated to a level where the location or community is not negatively impacted by inadvertent identification. Further, companies that do not share PII should be given preference over organizations that do not maintain these standards.[7] It is always preferable to select a messaging app that does not share any data with third parties other than that which is strictly necessary for the technical operation of the service (ICRC et al., 2017).
- **Minimize the amount of information submitted by participants and be strategic about data collection**. Consideration should be given to minimizing the data collected to what is absolutely necessary while also ensuring that collection processes are systematic and not reactive (i.e. that all data needs in the short- and medium-term are met) to avoid unnecessary repetition of data collection processes. Data collection processes should, wherever appropriate, be considered within the context of broader planning in regional and field offices.
- **When using a social media platform from a company registered in a country with broad surveillance powers, limit the information collected** to that which you would comfortably share with the government.
- **Consider whether crowdsourcing data could put participants at risk** during the physical data collection process (i.e. when mapping) or consequent to the disclosure of this data and findings.
- **Ensure that non-disclosure agreements are in place** prior to any sharing of PII data.
- **Wherever possible, explain potential privacy and confidentiality risks of using these technologies** in simple terms in relevant languages, either directly as a message to potential participants or in a prominent position on the relevant webpage of the social media platform. As frequently noted in the literature, while technologies and relevant social network services are being embraced on a global scale, the presumption that the greater proportion of users have a wholesale and nuanced comprehension of issues such as persistence, third party sale of data, analytics and applications, let alone legal jargon related to data collection or the implications of advanced website/browser tracking programmes, is overly optimistic (Acar et al., 2014; Berman and Albright, 2017). Explanations should include the types of organizations with whom the social media service shares the data.[8] Providing this information should be a means of supporting more informed participation.
- **Provide cybersafety tips and advice about privacy and security settings to participants**. In the instance of primary data collection and communication programmes, providing participants with cybersafety tips and advice about privacy and security settings and measures ensures that you have sought to minimize potential harms to programme participants. Tips could be provided on the

5 This could include, but would not be limited to, names, addresses, photos, etc.

6 Wherever possible, children should be encouraged not to use their real names on their profiles and/or to create accounts that do not have identifying information like their real name and photo.

7 There are some instances where PII data, such as geolocated data, may be necessary (see brief on geospatial technologies for further information and limitations). In these instances, an understanding of the information that is absolutely necessary for the evidence generation is needed in order to determine the most appropriate social media platform/s to use.

8 As an example, see the explanation of Instagram's privacy policy for children available at https://qz.com/878790/a-lawyer-rewrote-instagrams-terms-of-service-for-kids-now-you-can-understand-all-of-the-private-data-you-and-your-teen-are-giving-up-to-social-media/).

specific page/s of the social media platform or via direct messaging *(See Annex 5: Example of Social Media Safety Tips)*.

- **Ensure appropriate terms and conditions** are established for both the use of the platform and for data collection, storage and sharing **when creating a new platform**. In these instances, consult with your legal office (for UNICEF staff also see UNICEF's Policy on Information Security and UNICEF Policy on Information Security: Information Systems Acquisition and Development).

- **Provide opt out options**. Opt out options should be made available to participants to allow their data to be removed from lists or forums and, more generally, from data collection on request. Further, consideration needs to be given to the 'possibility of removing data on request from participants' (Greenwood et al., 2017). There may be instances where removal of data from all databases is impossible; in these cases, participants should be aware of this but still retain the option of, at a minimum, removing their information or data from the site/page if not from all databases (which may be unknown).

- **Ensure requisite skills and infrastructure** are available to appropriately manage and implement each component of the evidence generation activity, including ensuring appropriate monitoring, assessment and feedback loops (not only to encourage lessons learnt but to ensure transparency) (Raymond et. al., 2017).

- **Adhere to relevant local, international and organizational legal and ethical standards** pertaining to data protection, storage, transfer, removal and security. Where these differ, adhere to the highest relevant standards possible (Raymond et. al., 2017). Where conflicts exist, particularly where legislative environments potentially conflict with organizational ethical standards, seriously consider the harms versus the benefits of the programme and/or limiting data collected to an absolute minimum and ensuring that any resulting non-sensitive data collected would still be of value.

- **Monitor (prior to and throughout programme implementation) legislation and policy pertaining to community and government access to and use of telecommunications** infrastructure and hardware, particularly in fragile, autocratic and conflict affected states. Reflect on whether to continue to use a social media service if the policy will potentially allow government access to PII into the future.

- **Be aware of any government restrictions on and blocking of messaging app usage**. As noted in the risks section above, content transmitted on messaging apps has increasingly becoming a focus of overt and covert government interventions including restricting their use. This phenomenon can limit the extent to which these applications can truly be platforms for ongoing, real-time communication and exchange of ideas, experiences and information (ICRC et al., 2017). The potential for governments to block or disable apps or their features needs to be considered in the selection of social media tools for communication and data collection, with clear arrangements made to mitigate against or change platforms used in countries listed as impeding social media services.

- **Ensure that the platform/site is clearly branded** to make the affiliation to your organization clear and to differentiate it from other crowdsourcing or social media platforms, particularly those that might be used to entrap those espousing particular political views.

- **Ensure that a platform accurately reflects any role a host government may have** in the evidence generation programme and, where the government is the owner of the project, ensure the project is branded accordingly.

- **Reflect on the impacts of using data that may not be verifiable and the potential for misinformation.** When using social media apps, verifying data may be difficult. The ICRC et al. (2017) noted that 'rumours and misinformation can spread rapidly on messaging apps, in part because information is usually shared in closed groups that are based on peer-to-peer trust' (Raymond et.al., 2017) also note that the lack of barriers to participation can result in significant noise in the data. Conversely, the use of social media to identify and debunk rumours or misinformation can be critical to child survival.

  To address this issue, wherever possible, crowdsourced data and particularly crowdsourced data pertaining to political and environmental conditions, should be triangulated and/or complemented by other data (Raymond et.al., 2017) to ensure that misinformation and false rumours do not lead to misallocation of resources or placing staff or other individuals in physical locations where they may be at risk.

SECTION 2: USING THIRD PARTY DATA COLLECTED AND ANALYSED BY SOCIAL MEDIA SERVICES

The following section reflects on the potential benefits and risks when using third party data collected and analysed by social media services. It should be noted that these risks do not necessarily preclude the use of social media data for evidence generation but rather highlight the need for reflection and development of mitigation strategies. To this end, this section enumerates the ethical considerations that need to be taken into account when working in partnership with social media services to obtain and analyse data.

2.1 The benefits of using third party data and/or analysis from social media services

There are various benefits of establishing partnerships with social media companies and their affiliates for the collection and analysis of social media data. The following explores these benefits in detail.

- **Situational awareness and real-time monitoring.** Data derived from social media services can provide an alternate source of information to enhance service provision and to monitor environmental and population based conditions in real time. For example, this data may facilitate monitoring of migration patterns and identify early warnings of conflict and natural hazards (Dredze et al., 2016; Bello, 2016; Kryvasheyeu, 2015). Moreover, it may be particularly useful in cases where visual imagery (such as satellite images) is insufficient (not visible or audible or not sufficiently fine grained) to appropriately map locations and situations. This could include particular geographical areas (e.g. forest areas), locations where dwellings are dense (e.g. shanty towns) or instances where there is value in knowing the frequency of specific interpersonal interactions (such as the perpetration of violence or abuse). In these instances, crowdsourcing using social media to populate mapping can replace or supplement visual imagery. Alternatively, it can be used to source feedback on service delivery or to provide real-time information regarding resource levels and service outcomes. Finally, it is worth noting that social media could potentially be used to inform Sustainable Development Goals (SDG) indicators. Examples of data collected through this process that may inform SDG indicators include youth unemployment and air quality (Llorente et al., 2015; Martín-Corral et al., 2016)

- **Facilitation of human mobilization/crowdsourcing.** Social media may be used to quickly mobilize people for evidence generation activities such as mapping of populations and hard to reach geographical locations (Cebrian, 2016) (See also Joint Research Brief on geospatial technologies and ethics, for further details).

- **Providing a relatively cheap, less resource intensive source of data.** Social media platforms and attendant messaging services provide a relatively cheap vehicle to engage with children and can be a similarly cheap source of data for an organization. Data from social media services is less costly and time consuming to collect (assuming collaboration with the social media service) than primary research (ICRC et al., 2017) and can mitigate against survey fatigue amongst over-researched populations. Further, through appropriate partnerships with social media providers, data and analytics may be secured via data collaboratives at a fraction of the cost and to mutual benefit.

- **Allows for trend analysis, modelling and predictive analysis.** Social media services provide a sufficiently large data source to enable trend analysis, modelling and predictive analysis. The

benefits of this modelling can accrue in areas as diverse as child survival and development, which includes: population health surveillance; social norms and trend analysis; improved service provision and information; the prevention of violence; and, as noted above, the early warning detection of natural disasters and other social and environmental hazards (UN Global Pulse, 2013; Berman and Albright, 2017; Bello, 2016) including epidemics (Wesolowski et al., 2015). These types of analysis can be undertaken by software programmes known as webscraping tools. These tools facilitate the extraction of relevant data from websites enabling qualitative or quantitative analysis. In social media contexts, webscraping may be undertaken via social media sites' application programming interface (API) (rather than directly), allowing companies to maintain control over access to individuals' information and activities and hence to provide a measure of privacy for them.

Case study: Zika, Facebook and C4D

In order to better appreciate understandings and awareness of Zika in Brazil, UNICEF worked with Facebook to gather data on discussions and posts related to the mosquito transmitted disease. According to Facebook, more than 90 per cent of the population that accesses the Internet in Brazil (110 mill users) use the platform every month. To protect the privacy of users, Facebook pulled together anonymized insights from posts about the Zika conversation in Brazil and shared only the aggregate findings with UNICEF. The data provided was primarily quantitative and did not identify geographic details beyond absolute numbers of Facebook users at state and city level.

Further, it should be noted that the quotes that were ultimately used for the final report only expressed support for increased awareness, were sufficiently generic as to maintain relative anonymity and were uncontroversial and benign, thereby limiting any negative repercussions for the author.

The results and consequent learnings from this analysis were then incorporated into a data-driven campaign. One aspect of the campaign was designed to engage men as allies in the fight against Zika. The UNICEF ad was based on an insight from Facebook that 58 per cent of posts about Zika in Brazil came from men. The ad campaign also went beyond Zika, with another post calling on people to protect themselves from other illnesses transmitted by the *Aedes aegypti* mosquito.

To assess the efficacy of the campaign, a survey was undertaken pre and post campaign regarding knowledge of Zika. Though inadvertently, the survey also provided a vehicle to inform participants of the work that UNICEF was undertaking in collaborating with Facebook to understand discourse on Zika in the public domain.

2.2 The risks of using third party data and/or analysis from social media services

The following section outlines the potential risks of using third party social media data. As noted previously, these risks do not necessarily preclude the use of social media data for evidence generation, but rather should, at a minimum, inform clear risk mitigation strategies. Various risks noted below were identified above as relevant for social media projects using social media platforms to engage children and their communities. They have also been included in the following section to allow practitioners and academics to focus and refer exclusively to their primary area of interest (i.e. ethics of generating/collecting data via participant engagement in social media vs. ethics of using social media data of third parties).

Silencing children's voices

The use of social media data from third parties for forecasting and to capture attitudes or priorities can be problematic if findings are increasingly used by decision makers instead of direct dialogue. The potential replacement of engagement with algorithms could have significant implications for children and may be counter to article 12 of the Convention on the Rights of the Child (1989), which states that children have a right to have a say on matters that affect them. Risks exist where webscraping is used to collect data generated for other purposes to predict behaviours, attitudes and preferences, and where this data exclusively informs programming, advocacy and policy responses. This is compounded where (a) the data is not representative and (b) the biases inherent in publicly-disclosed data are ignored. In these instances, the findings may not be robust or reflective of attitudes, priorities or even behaviours resulting in highly skewed or biased predictions. Without direct consultation of children, the best interest of the child may not be served. To mitigate this risk, use of this type of big data may best be used in combination with qualitative research as opposed to replacing it.

Privacy, confidentiality and security

The following are possible risks that may arise when using third party social media. These risks relate to: the potential for invasion of privacy, breaches of confidentiality, and risks to the security of the persons providing data. These issues should be reflected on when considering collection and analysis of this type of data and when deciding whether and/or which social media service to partner with.

- **Restrictions and blocking of social media use.** According to the publication *Silencing the Messenger: Communication Apps under Pressure: Freedom on the Net 2016*, in June 2015 to May 2016 governments in 24 out of 65 countries were assessed as impeding access to social media and communication tools. WhatsApp faced the most restrictions, with 12 out of 65 countries blocking the entire service or disabling certain features (Kelly et al., 2016). These types of restrictions can severely limit the representativeness of data sets.

Risk aversion leading to lost opportunities

- **Dismissing the value of using social media** (without being informed by an appropriate risk benefit analysis) for evidence generation and missing significant opportunities to ensure results for children.

Informed consent

- **Not securing informed consent for use of information.** Those participating in a social network may have a reasonable expectation that their information and postings will be limited to their network (Hoser and Nitschke, 2010; Elgesem, 2015) and hence reflection is required as to whether secondary use of this data for evidence generation processes can be justified taking into account privacy conditions and potential benefits. If obtaining consent is not possible, all efforts should be made to ensure that information regarding the evidence generation programme is available in relevant public domains.

Risks relating to data quality and applications

There are a number of significant risks that need to be considered relating to the data obtained via social media platforms. These risks pertain to each phase of the data cycle from collection, processing and sharing to the analysis and finally to the use of data for decision making and assessment.

These risks may not be exclusive to online data gathered from social media providers but may also pertain to existing traditional data collection practices.

The risks at each phase of the data cycle are:

Potential data collection risks

- Data collected may not be useful or may merely replicate data already available without clearly identifying any added value such as using the data for validation and triangulation.
- Data may be unrepresentative. Data collected on a particular platform will reflect the population of users of that platform. In cases where social networking sites are developed for smartphones, this excludes populations that do not have access to this relatively more expensive technology. The exclusion of particular cohorts (for instance, children under 13) means that the findings will not reflect their realities or opinions.
- Poor data quality. If the data is old or incomplete, the consistency and quality may be sufficiently poor to render its analysis inaccurate or redundant.

Potential data processing risks

- Use of third party data means that determining the validity of specific insights (such as trends and predictions) is likely to be less straight forward, often due to lack of direct access to and formulation of the data fields themselves. This implies that insights may need to be interrogated and possibly qualified, with explicit recognition of the strength or limitations of the explanatory power of the model.
- Potential re-identification of PII. Even if information is initially stripped of PII, identification of individuals may be possible in the future if this information is combined with another data set. It is extremely difficult (arguably impossible) to guarantee that a certain type of anonymization will hold over time since new data sources might be released by third parties that could, if combined, compromise the confidentiality of persons within the particular database created by the social media provider (Sweeney, 2002; De Montjoye et al., 2013; Sharad and Denezis, 2013).
- Lack of transparency. The processes used to 'clean data' can lack transparency leading to uncertainty in relation to omitted variables, representation and consistency in data sets.
- The time taken to clean data negating the timeliness of data. The time required to clean and validate data sets so that they are useable and in a format understandable to those on the ground may make third party data use redundant or counter-productive, particularly where information is time sensitive.
- Loss of contextual integrity of data. Secondary data provided by a third party may be analysed and

used for contexts which differ from the context, intent and audiences for which it was originally provided or shared. In certain instances, this discrepancy may result in lack of contextual integrity with true meaning and intent lost. Consequently, the findings may be questionable.

- Data from social media may not reveal actual preferences and behaviours but rather socially acceptable preferences and behaviours; hence, using this data for prediction may be questionable in certain contexts where socially acceptable responses and behaviours are likely.

Potential risk of data sharing

- Lack of data stewardship. Unless formalized in memoranda of understanding, contracts or institutional practice, PII may not be sufficiently protected without a clear agreement relating to its responsible use that seeks to protect and limit access to this type of data.

Potential data analysis risks

- Poor problem definition leading to data being analysed in a way that does not add value and therefore diverts time and resources.
- Inappropriate data modelling undertaken by persons who do not consider the limitations of the data and/or do not understand and take into account the social, political and environmental contexts in which the data was collected. This can lead to bias in the findings and inaccuracies in predictions and trends.
- Discrimination being built into algorithms. Discrimination can be consciously or unconsciously built into algorithms without the final user's knowledge. Correlations between location, poverty, gender and race may result in trends and predictive models that discriminate against certain persons or groups.

Potential risks in use of data

- Discriminatory policies and programmes resulting from decisions based on biased algorithms. As noted above, discrimination can be embedded in algorithms resulting in decision making, programming and advocacy that reflect the bias and limitations of the model, potentially resulting in reduced opportunities, inappropriate distribution of resources, poorly conceived programmes or policies or shaming of persons from particular locations and sub-populations.
- Limited generalizability of the findings in light of poor data quality or unrepresentative data.

Potential data storage risks

- Inaccessibility of the data generated due to a social media company's physical or cloud servers being hacked. In time-sensitive contexts this could have significant implications, particularly in cases where 'on the ground' decision making is strongly dependent on this data.

Potential data disposal risks

- Data may not be appropriately or fully disposed of and may remain on servers, both known and unknown.

2.3 Ethical considerations when using third party data collected and analysed by social media services

Before identifying steps to be taken to support ethical evidence generation activities undertaken in partnership with social media companies, it is worth highlighting a couple of points. A number of the issues and the mitigation strategies identified are just as relevant for data collection and analytics undertaken in offline contexts as in online contexts. Their inclusion in this brief is to ensure a more comprehensive overview of the issues to be considered.

The following should be considered and taken into account when embarking on a partnership with a social media provider:

- The nature and value of the data
- National and organizational privacy frameworks
- Consent and transparency
- Considerations relating to the data cycle
- Understanding the data and limitations
- Understanding the algorithms

The value and timeliness of the data

- **Reflect on the value of the data.** In instances where data from third parties is used or collected from social media services, reflection is required on how useful the data will be in answering relevant questions in a timely manner. This requires considering the availability of resources and the time required to ensure the data is useable (i.e. any time and resources that will be required to clean the data).
- **Understand the representativeness of the data.** When data provided by social media services is focussed on particular cohorts or particular populations, an understanding is required of the target populations' access to various technologies as well as their use of and representativeness within the social media platform (Raymond and Achkar, 2016).

National and organizational privacy frameworks
(See Attachment 4 for the United Nations Global Pulse Privacy and Data Protection Principles)

- **Adhere to relevant local, international and organizational legal and ethical standards** pertaining to data protection, storage, transfer, removal and security. Where these differ, adhere to the highest relevant standards possible (Raymond et. al., 2017).
- **Ensure that partners agree to the anonymization of data provided to the greatest extent possible.**[9] Ensure that non-disclosure agreements are in place prior to any sharing of PII. Consider giving preference to social media platforms that will only provide anonymous data to partners.

9 Unless PII is absolutely requisite as may be the case for some programmes. In these instances, additional security measures should be considered (e.g. multiple authentication systems, etc.)

Consent and transparency

- **Wherever possible, inform those whose data is likely to be collected** and used by UNICEF about the nature of the project, the privacy conditions agreed to within the partnership and the use of the findings. Where this is not directly possible, at a minimum, provide this information on the organization's/field office's website or their social media landing page.
- **When receiving secondary data, take into account data providers' expectations regarding the privacy of data.** In principle, the data someone has posted, e.g. on a social network site or newsgroup, should reasonably be used in contexts and by the audience he or she intended it for. The intended audience is the community he or she joined and it is unlikely that participants in a community have the expectation that a third party will use and analyse their data (Hoser and Nitschke, 2010). Care should therefore be taken in the use of this secondary data, reflecting on the context in which the data was collected, the nature of the population whose data is being analysed, the information used, the likelihood of identification of individuals and the potential for inadvertently or otherwise stigmatizing the cohort under analysis.
- **When determining which organizations to establish collaborative partnerships with for data provision** it is important to value, advocate and prefer companies with clear and fair terms of service, strong privacy settings, and provisions that give data ownership to their users.

Use of a risk assessment framework

- **Use a risk assessment framework.** A risk assessment framework should be used that reflects on the risks and mitigation strategies of using data and/or using third party analytics based on this data for decision making. (The checklist contained in this brief may provide a very basic framework for risk assessment. Risk mitigation strategies however, would still need to be clearly outlined in a separate document or in the comments section of the template).

  A risk assessment framework would include reflection on and elaboration of contingency plans in the event that: (a) access to social media services or infrastructure is blocked unexpectedly (and, for example, this data was to be used to monitor communities on the move in order to meet day to day needs); (b) data is wiped remotely; or (c) a privacy breach occurs. Other tools that may be useful include:

  – UN Data Privacy Policy Group has created a risk assessment tool that can be adopted and adapted. http://unglobalpulse.org/sites/default/files/Privacy%20Assessment%20Tool%20.pdf
  – The Information Accountability Foundation (2016) Big Data Assessment Framework and Worksheet http://informationaccountability.org/wp-content/uploads/IAF-Big-Data-Ethics-Initiative-Part-B.pdf).

- **Collaborate with all relevant stakeholders to populate the risk assessment framework.** To ensure that the technical, social and political implications are understood, the population of any assessment framework should be undertaken collaboratively with all relevant stakeholders. This could include data analysts, relevant local and international project management staff and communities and, wherever possible, social network services providers.

Aggregation of findings to avoid or limit identification of groups or individuals

- **Wherever possible, ensure aggregation of findings as early as possible in the data cycle.** The more aggregated the data findings are, the less likely they are to be traceable to individual communities and persons (UN Global Pulse and MIT, 2015). Aggregation should be undertaken to the maximum degree while maintaining the usefulness of the data and should take place as close as possible to the initial data collection (De Montjoye et al., 2016).

Understanding the data and limitations

- Limitations of the data could include: data gaps, who is included or excluded from the data (determined by the accessibility of technologies, the use of devices and the profiles and demographics of participants), merging of incompatible databases/datasets, inclusion of outdated data, etc. Any limitations of geospatial data (whether collected directly, or indirectly through a third party) should be understood. Discussions should be had with data providers and data experts on these limitations in order to:
  - Understand whether the data is fit for purpose
  - Ensure that any findings are appropriately qualified with clear consideration of the implications of the limitations
  - Ensure that recommendations based on findings are similarly qualified with clear consideration of the implications of the limitations

- **Understand the context of data creation and the implications for use.** The implications and limitations of applying data to a context different to the purposes for which it was originally provided should be explicitly accounted for and understood via conversations with data providers. In these contexts, issues that may exist include revealed versus actual preferences, public versus personal personas, purposive dissemination of misinformation and lack of applicability to your context.

- **Be clear about the potential lack of replicability and representativeness of data.** It may be difficult to determine if data is, in fact, representative (particularly with regard to child populations – as disaggregated data for children between the ages of 12 and 18 is not always publicly available). In these instances, determine if age disaggregated data is available and, if not, care should be taken when applying findings to national contexts, with clear caveats that the data is, at a minimum, limited to those with access to relevant technologies and may or may not be representative of children of particular ages. (This is particularly true for the many large social media services in places such as the United States and China where it is illegal for children under the age of 13 to subscribe). Further, wherever possible, findings should be triangulated with other sources.

- **Reflect on the value of quantitative metrics versus qualitative research – make sure children's voices are not silenced**. Consideration should be given to the value of quantitative versus qualitative data to ensure that children have voices, that findings are contextualized and that the complexity of the social phenomenon being explored is not oversimplified or unrepresentative, but rather reflective of their lived reality (Berman and Albright, 2017; Moestue and Muggah, 2014; Lupton and Williamson, 2017). Wherever possible, modelling should augment and not supplement children's, child protection specialists' and advocates' voices.

Understanding the implications of algorithmic based findings

- **Third party big data raises major questions about:**
  - **The loss of individual and community agency** when deterministic knowledge is applied to human behaviour (Schroeder, 2014, p.8). In other words, reflect on the potential for individuals or community to lose control over decisions that are made about them if these decisions are based on predictive models rather than as a result of consultation (Schroeder, 2014, p.8).
  - **The possibility of discrimination against disadvantaged groups**. Correlations and interactions between geography and poverty, gender and race may result in trends and predictive models that discriminate against certain persons.

- **Extreme care should therefore be taken when using findings based on social media data and clear explanations should be requested of analysts concerning** any potential limitations of this data and the model used. Further, clear disclosure of the limitations of the algorithms or the potential for bias in the data should be disseminated alongside any findings, with appropriate qualifications made to recommendations based on these findings. Care also needs to be taken in the dissemination of findings with reflection on the potential for stigma and discrimination. Where discrimination is a possibility, the use of social media data and its analysis should be reconsidered and/or findings carefully triangulated with other data sources and dissemination of these findings undertaken with utmost care.

CONCLUSION: REFLECTIONS ON THE LONGER TERM

This paper has attempted to identify existing limitations and potential risks of using social media platforms for data collection and analysis and to explore the numerous possibilities and opportunities presented by such data. It is important that the potential benefits of these technologies be acknowledged, particularly given their potential to shed light on social structures and dynamics and to provide a powerful tool for advocacy and engagement on critical social issues.

When using social media to directly engage children and their communities, or when establishing partnerships with these organizations for data collection and analysis, adoption of these technologies and their resultant data should not be exclusively driven by short-term necessity but also by the long-term needs of our younger partners. When engaging with social media and indeed most technology, thoughtfulness, reflection and ongoing interrogation is required. While certain risks can be anticipated and are already apparent, as technologies develop, so will the risks. This requires continued vigilance, awareness and ongoing research in this domain.

For those amongst us who are not social media experts or data analysts, we can still actively engage with, and take responsibility for, the programmes that we undertake and the partnerships we establish. We simply need to be equipped with the appropriate information/questions/tools that can help guide us to better interrogate and understand the potential benefits and implications of using these technologies. In the absence of technological expertise, we need to ensure that the experts we work with are able to explain both the value and the risks in relatively simple terms. In this way, we can ultimately ensure that the rights of children and their communities are safeguarded throughout the data cycle.

Further, we need to account for the growing importance of and need for 'experts' with these competencies and skills in child-based organizations – individuals with both data/digital communications expertise and a child rights lens.

At a minimum, we need to ensure the highest possible ethical standards in data collection involving social media. In many instances, this is not a matter of ensuring that everyone is technically proficient but rather ensuring that those who are not are able to ask the right questions, putting the well-being of children now and into the future at the heart of those questions.

BIBLIOGRAPHY

Al Omoush, K.S. and S. G. Yassen, 'Motivations and Risks of Social Media Crowdsourcing in War-torn Societies: Evidence from Syria', *CDS 2016 : The Tenth International Conference on Digital Society and eGovernments*, 2017, available at <www.researchgate.net/publication/314187507_Motivations_and_Risks_of_Social_Media_Crowd_sourcing_in_War-torn_Societies_Evidence_from_Syria>.

Bender, J., Jimenez-Marroquin, M.C. and Jaddad, A., 'Seeking Support on Facebook: A Content Analysis of Breast Cancer Groups', *Journal of Medical Internet Research*, vol. 13, no. 1, Jan – Mar 2011.

Berman, G. and Albright, K., 'Child Rights and Ethics in A Big Data World', UNICEF *Innocenti Working Paper* 2017-05, UNICEF Office of Research, Florence, 2017.

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

Bond R., et al., 'A 61-million-person experiment in social influence and political mobilization', *Nature*, vol. 489, 2012, pp. 295–298.

Boyd, D. and Ellison, N., 'Social Network Sites: Definition, History & Scholarship', *Journal of Computer-Mediated Communication*, vol. 13, 2008, pp. 210–230.

Cebrian, M., 'SEARCHING FOR SOMEONE, From the "Small World Experiment" to the "Red Balloon Challenge," and beyond', 18 February 2016, accessed at MIT Media Lab, available at <https://medium.com/mit-media-lab/searching-for-someone-688f6c12ff42>.

Colin, P., 'Building and Connecting to Online Communities for Action: young people, ICT and everyday politics', *International Journal of E-Politics: Special Edition on E-Democracy - Online Youth Participation and Engagement*, vol. 1, no. 3, 2010, pp. 1–18.

Colin, P., et al., *The Benefits of Social Networking Services, Cooperative Research Centre for Young People, Technology and Wellbeing*, 2011, available at <http://researchrepository.murdoch.edu.au/id/eprint/11804/1/FINAL_The_Benefits_of_Social_Networking_Services_Lit_Review.pdf>.

Currion, P., 'If all you have is a hammer…"—How useful is humanitarian crowdsourcing?', 9 November 2015, available at <https://medium.com/@paulcurrion/if-all-you-have-is-a-hammer-how-useful-is-humanitarian-crowdsourcing-fed4ef33f8c8>.

De Montjoye, Y., et al., 'Unique in the Crowd: the privacy bounds of human mobility', *Scientific Reports,* vol. 3, no. 1376, 2013.

De Montjoye, Y., et al., 'Privacy-conscientious use of mobile phone data', *Communications of the ACM*, 2016, available at <http://web.media.mit.edu/~yva/PrivacyConscientious_rUehNriY.pdf>.

Dredze, M., et al., 'Twitter as a source of global mobility patterns for social good', presented at 2016 ICML Workshop on #Data4Good: Machine Learning in Social Good Applications, New York, NY, arXiv:1606.06343 [cs.SI], 2016.

Elgesem, D., 'Consent and information – ethical considerations when conducting research on social media' in *Internet Research Ethics*, edited by in Fossheim, H. and H. Ingierd, Cappelen Damm Akademisk, 2015, available at <www.cappelendamm.no/_internet-research-ethics-hallvard-fossheim-9788202480356>.

Ess, C., *Ethical decision-making and Internet research*, Recommendations from the AoIR ethics working committee, Association of Internet Researchers, 2002.

Gibbs, S., 'Facebook Questions Use of 'Right to be Forgotten' Ruling', *The Guardian*, Tuesday 7 July 2015, available at <www.theguardian.com/technology/2015/jul/07/facebook-questions-use-of-right-to-be-forgotten-ruling>.

Greenberg, A., 'Hacker Lexicon: What Is End-to-End Encryption?', *Wired*, 25 November 2014, available at <www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption>.

Greenwood, F., et al., 'The Signal Code: A Human Rights Approach to Information During Crisis', *Standards and Ethics Series 02*, Harvard Humanitarian Initiative, Signal Human Security and Technology, Cambridge, 2017.

Hosein G. and Nyst, C., *Aiding Surveillance: An Exploration of how Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries,* Privacy International, London, October 2013, available at <www.privacyinternational.org/sites/default/files/Aiding%20Surveillance.pdf>.

Hoser, B. and Nitschje, T., 'Questions on ethics for research in the virtually connected world', *Social Networks,* vol. 32, 2010, pp. 180–186.

ICRC et al., The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps*, January 2017, available at <www.icrc.org/en/publication/humanitarian-futures-messaging-apps>.

Ito, M., Okabe, D. and Matsuda, M., *Personal, Portable, Pedestrian*, MIT Press, Massachusetts, 2006.

Jenkins, H., *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*, MacArther Foundation, Chicago, 2007.

Kelly, S., et al., *Silencing the Messenger: Communication Apps under Pressure: Freedom on the Net 2016*, Freedom House, 2016, available at <https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf>.

Kryvasheyeu, Y., et al., 'Performance of social network sensors during Hurricane Sandy', *PLoS one*, vol. 10, no. 2, 2015.

Leung, L., 'Phoning home', *Forced Migration Review*, vol. 38, October 2011, available at <www.fmreview.org/technology/leung.html>.

Livingstone S. and E. Locatelli, 'Ethical Dilemmas in Qualitative Research with Youth On/Offline', *International Journal of Learning and Media,* vol. 4, no. 2, Spring 2012, pp. 67–75.

Llorente, A.,et al., 'Social Media Fingerprints of Unemployment', *PLoS one*, vol. 10, no. 5, 2015.

Luders, M., 'Researching Social Media: Confidentiality, Anonymity and Reconstructing Online Practices' in *Internet Research Ethics*, edited by Fossheim, H. and H., Ingierd, Cappelen Damm Akademisk, 2015, available at <www.cappelendamm.no/_internet-research-ethics-hallvard-fossheim-9788202480356>.

Lupton, D. and Williamson, B., 'The Datafied Child: The Dataveillance of Children and the Implications for their Rights', *New Media and Society*, 23 January 2017, pp. 1–15.

Martín-Corral, D., et al., 'Study of the Effects of Air Quality and Climate upon Human Health using Social Digital Traces', *Digital Epidemiology and Surveillance*, presented at DELVE2016, Amsterdam, September 2016.

McKee, H.A. and Porter, J.E., *The Ethics of Internet Research*, Peter Lang, 2009.

Moe, H. and Larsson, A. O., 'Methodological and Ethical Challenges Associated with Large-scale Analyses of Online Political Communication', *Nordicom Review*, vol. 3, no. 1, 2012, pp. 117–124.

Moestue H. and Muggah, R., 'Digitally Enhanced Child Protection: How new technology can prevent violence against children in the Global South', Strategic Paper 10: 36, Igarapé Institute, Rio De Janeiro, November 2014.

Montgomery, K., Gottlieb-Robles, B. and Larson G.O., *Youth as E-Citizens: Engaging the Digital Generation*, Center for Social Media, American University, 2004.

Moorhead, A., et al., 'A New Dimension of Health Care: Systematic Review of the Uses, Benefits, and Limitations of Social Media for Health Communication', *Journal of Medical Internet Research*, vol. 15, no. 4, April 2013.

NESH (Norwegian National Committees for Research Ethics), *Forskningsetiske retningslinjer for forskning på Internett*, 2009, available at <www.etikkom.no/Forskningsetikk/Etiske-retningslinjer/Samfunnsvitenskap-jus-og-humaniora/Internett-forsking>, referenced in English in Elgesem, D., 'Consent and information – ethical considerations when conducting research on social media' in *Internet Research Ethics*, edited by Fossheim, H. and H. Ingierd, Cappelen Damm Akademisk, 2015, available at <www.cappelendamm.no/_internet-research-ethics-hallvard-fossheim-9788202480356>.

Phillips, L., et al., 'Using Social Media to Predict the Future: A Systematic Literature Review', *Computers and Society*, arXiv:1706.06134 [cs.CY], 2017, available at <https://arxiv.org/abs/1706.06134>.

Raymond, N. and Z. Al Achkar, *Data preparedness: connecting data, decision making and humanitarian response,* Harvard Humanitarian Initiative, Standards and Ethics Series 01, Signal Human Security and Technology, Cambridge, 2016.

Raymond, N., 'Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data', Springer*, Philosophical Studies Series (PSSP),* vol. 126, 2016, available at <https://link.springer.com/chapter/10.1007/978-3-319-46608-8_4>.

Raymond, N., et al., 'Building data responsibility into Humanitarian Action', *OCHA Policy and Study Series 018*, May 2017.

Schroeder, R., 'Big Data and the brave new world of social media research', *Big Data & Society*, July–December 2014, pp. 1–11.

Sharad, K. and Danezis G., 'De-anonymizing D4D Datasets', *Privacy Enhancing Technologies, 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013, Proceedings*, edited by De Cristofaro, E. and M. Wright, 2013.

Shaw A. and Sender, K., '*Queer technologies: Affordances, affect, ambivalence. Critical Studies in Media Communication'*, vol. 33, 2016, pp. 1–5.

Sweeney, L., 'K-anonymity: a model for protecting privacy', *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, 2002, pp. 557–570.

United Nations High Commissioner for Refugees, *Connecting Refugees: How Internet and Mobile Connectivity can Improve Refugee Wellbeing and Transform Humanitarian Action*, UNHCR, Geneva, September 2016, available at <www.unhcr.org/en-us/connectivity-for-refugees.html>.

UNICEF Innocenti, 'Child Safety Online: Global challenges and strategies', UNICEF *Innocenti Publications,* Florence, 2011, available at <www.unicef-irc.org/publications/650>.

United Nations Global Pulse, *Big Data for Development: A Primer*, UN Global Pulse, 2013, available at <www.unglobalpulse.org/sites/default/files/Primer%202013_FINAL%20FOR%20PRINT.pdf>.

UN Global Pulse and Massachusetts Institute of Technology, 'Mapping the risk-utility landscape of mobile data for sustainable development and humanitarian action', Global Pulse Project Series, No. 18, 2015, available at <www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Mobile_Data_Privacy_2015.pdf>.

Vromen, A., 'Australian young people's participatory practises and internet use', *Information, Communication and Society*, vol. 10, no.1, 2007, pp. 48–68.

Vromen, A., 'Inclusion through voice: Youth participation in government and community decision-making' in *Social Inclusion and Youth Workshop Proceedings*, Brotherhood of St Laurence, Melbourne, 2008.

Wesolowski, A., et al., 'Impact of human mobility on the emergence of dengue epidemics in Pakistan', *Proceedings of the National Academy of Sciences*, vol. 112, no. 38, 2015, pp. 11887–11892.

ANNEX 1: CHECKLIST OF ETHICAL ISSUES FOR CONSIDERATION WHEN USING SOCIAL MEDIA FOR EVIDENCE GENERATION

The following are questions that need to be considered and reflected on in consultation with relevant stakeholders and experts to ensure that UNICEF is able to reap the benefits of social media platforms while also protecting the children and communities that it serves.

Tick = Yes Cross = No	Questions	Comments
Ethical considerations when managing a webpage or using an app for communication and information/data collection		
	Have you secured consent to the greatest extent possible regarding:	
	1. The purpose of engagement?	
	2. Subsequent use of any data?	
	3. Who will have access to data and in what form?	
	4. Any potential risks or privacy issues?	
	5. On a landing page that participants must access in order to participate or register to sign up?	
	Will you be able to reach relevant populations including the most disadvantaged or marginalised groups/ individuals amongst them considering:	If not, what are the implications for findings and how will you ensure that findings clearly note this limitation? How will you address the lack of information from this/ these cohort/s?
	1. The Internet coverage in your country?	
	2. The level of access to particular social media channels?	
	3. The cost of technologies?	
	Have you ensured as much as possible that information provided by participants is not personally identifiable information (PII)?	
	If some form of PII is necessary, how will you safeguard this data and ensure its confidentiality?	
	How is this built into the platform?	
	Have you provided cyber-safety advice about privacy and security settings to participants?	
	Do you have a process and the personnel to carefully curate content in forums or on webpages and to vet any offensive or harmful content?	
	Have you created opt out provisions for participants to remove themselves and their information from your lists or forums to the greatest extent possible?	
	Have you made it clear that even if you remove individuals' content from social media platforms that you cannot guarantee that this data will be removed from all databases and sites due to any unknown channels where information/data may be shared?	

Tick = Yes Cross = No	Questions	Comments
Ethical considerations when managing a webpage or using an app for communication and information/data collection		
	If you are working in a context where the Government has had a history of imposing restrictions on and blocking messaging app usage, have you considered alternate arrangements/social media services or channels for information if the service used is regularly blocked, restricted or monitored?	
	Have you considered means to verify findings from data collected?	
	Have you established clear channels to respond to participants' possible requests for help, support or advice?	
	If you cannot verify data, is there still value in collecting the data for triangulation purposes or to inform understandings of perceptions?	

ANNEX 2: CHECKLIST FOR PARTNERSHIPS WITH SOCIAL MEDIA PROVIDERS

The following are questions that need to be considered and reflected on in consultation with relevant stakeholders and experts to ensure that UNICEF is able to reap the benefits of the data and/or analytics provided by social media providers.

Tick = Yes Cross = No	Questions	Comments
Ethical considerations when using data from social media providers		
Consent		
	Have you secured informed consent from persons whose data you will be using?	
	If not, is it reasonable to use this data?	
	Is it de-identified?	
	What are the justifications for data use in terms of the benefits?	
	If it will be impossible to secure informed consent, have other forms of communication about the evidence generation been considered pre or post data collection on the UNICEF webpage or on the social media platform? Including:	
	1. What data will be provided by the social media service?	
	2. How it will be protected and/or de-identified?	
	3. How data will be used, where the findings will be reported and/or what they will be used to inform?	
	If you cannot secure informed consent, have you made sure that:	
	1. The data you have received is not identifiable to the greatest extent possible – while still being useable,?	
	2. There are strict protocols to ensure the security of the data in transmission and storage?	
	3. The release of any findings will not put those involved at risk or potentially stigmatize them in either the short- or longer- term?	
Undertaking a risk assessment		
	Have you planned to undertake this or another risk assessment exercise in collaboration with key stakeholders? (e.g. the social media service, data analysts, programme managers, community representatives?)	Other examples of risk assessment templates: http://unglobalpulse.org/sites/default/files/Privacy%20Assessment%20Tool%20.pdf http://informationaccountability.org/wp-content/uploads/IAF-Big-Data-Ethics-Initiative-Part-B.pdf

Tick = Yes Cross = No	Questions	Comments
	In undertaking the analysis and disseminating the findings, have you ensured that data findings are aggregated as much as possible (while still ensuring the usefulness of the findings) and reviewed prior to dissemination to mitigate against:	
	1. Identification?	
	2. Stigmatization of particular communities or persons?	
	Do you have contingency plans in the event that:	
	1. Access to social media services or infrastructure is blocked unexpectedly (and, for example, this data was to be used to monitor communities on the move in order to meet day to day needs)?	
	2. Data is wiped out remotely?	
	3. A privacy breach occurs?	
Understanding the data and limitations		
	Have you had a conversation with the social media service and data analysts to understand any limitations of the data including:	
	1. Data gaps?	
	2. Included and excluded populations (determined by the accessibility of technologies, the use of devices and the profiles and demographics of participants). How representative is the data?	
	3. Merging of databases/data sets (are they actually compatible)?	
	4. Inclusion of old/outdated data?	
	Have you understood the context in which the data was provided?	
	Is it relevant in answering your question? (e.g. will it provide insights into the real preferences of the target population rather than just their stated preferences)?	
	Is this important?	
	Have you considered the implications of using social media data rather than qualitative primary data in terms of ensuring that the voices of the communities and individuals you are trying to understand are truly heard?	
	Can you use both?	

Tick = Yes Cross = No	Questions	Comments
Understanding the algorithms		
	If you are planning to use data to predict human behaviours or responses and outcomes have you considered the algorithm that is being used being used and the data it was based on?	
	Have you had it explained to you by the data analyst?	
	Have you considered whether the findings may stigmatize or unnecessarily limit the opportunities or access to services for groups or individuals?	
	Have you considered the impacts on individuals who will not fit the model?	

ANNEX 3: SOCIAL MEDIA PRIVACY SETTINGS

Facebook & Facebook Messenger:

https://www.facebook.com/privacy/explanation

Twitter:

https://twitter.com/en/privacy

Instagram: (A subsidiary of Facebook since 2012)

https://help.instagram.com/155833707900388

Whatsapp (A subsidiary of Facebook since 2014)

https://www.whatsapp.com/legal/#terms-of-service

YouTube

https://www.youtube.com/static?template=privacy_guidelines&gl=IT

WeChat

https://www.wechat.com/en/privacy_policy.html

VK

https://vk.com/privacy

Weibo

https://www.weibo.com/signup/v5/protocol

ANNEX 4: PRIVACY-FRIENDLY FEATURES OF MESSAGING APPS [10]

PRIVACY-FRIENDLY FEATURES OF MESSAGING APPS

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

⚠ **HEIGHTENED LEVEL OF RISK.**

* Shared message content is retained.

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

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

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

10 ICRC et al., 2017.

ANNEX 5: EXAMPLE OF SOCIAL MEDIA SAFETY TIPS

Social media safety tips:

1. **Got a nickname?**
   Think about using a nickname instead of your real name if you're signing up to a microblogging site like Twitter. Consider setting up a separate, personal email account to use with social media sites, rather than using your work, or even your main personal email. Remember: only connect to people you know.

2. **Check your privacy and security settings (tailor to relevant social media service)**
   Use the privacy and security settings on social media sites so that only friends and family can see your pages. Then speak to friends and family and encourage them to tighten their privacy settings too as they could affect you. Even if your account is locked as private, personal information you have shared with others could still be accessed through their pages.

3. **Guard personal information**
   Don't post any personal information – your address, email address or mobile number – publicly online. Just one piece of personal information could be used by a complete stranger to find out even more. If you want to include your birthday in your profile, it's safer not to actually display it publicly – providing your full date of birth makes you more vulnerable to identity fraud.

3. **Photos and videos**
   Be careful about which photos and videos you share on social media sites – avoid photos of your home, work, school or places you're associated with. Remember, once you've put a picture of yourself online, other people may be able to see it and download it – it may not just be yours anymore.

4. **Check what's needed**
   Don't give out information online simply because it's asked for – think whether whoever is asking for it really needs it. When you're filling in forms online, for example to register with a website or sign up for a newsletter, always provide the minimum information possible.

9. **Delete old accounts**
   If you've stopped using a social media site or forum, then close your account down. There's no point in leaving personal information out there unnecessarily.

10. **Be careful of over-friending**
    As a member of a social networking group, it can be exciting to gain new 'friends' or followers. Looking through the network it is easy to find members with high numbers of friends, which can inspire a competitive streak in some. A high number of friends, however, is not always positive. Some 'friends' can be problematic by introducing spam into one's timeline or some may even have criminal intentions. When accepting friends, choose people who are actual friends.

11. **Don't share your location unless necessary**
    Disable photo geo-tagging, and change privacy settings so that they don't allow photo tagging on social networks. If you have a smartphone and you're using it to go on to the social media site, turn off the geo-location service (usually GPS). Avoid the option to check in at registered locations. Generally, switch the geo-location service off when using social media unless you are keeping it on for safety reasons.

Sourced from: http://www.bbc.co.uk/webwise/0/21259413

ANNEX 6: DATA PRIVACY AND DATA PROTECTION PRINCIPLES (UNITED NATIONS GLOBAL PULSE (2016)*

Purpose of use: We access, analyse or otherwise use data for the purposes consistent with the United Nations mandate and in furtherance of the Sustainable Development Goals

Right to use: We access, analyse or otherwise use data that has been obtained by lawful and fair means, including, where appropriate, with the knowledge or consent of the individual whose data is used

Purpose compatibility: We ensure to the extent possible, that all of the data we use for project purposes is adequate, relevant, and not excessive in relation to the legitimate and fair purposes for which the data was obtained

Individual privacy: We do not access, analyse or otherwise use the content of private communications without the knowledge or proper consent of the individual. We do not knowingly or purposefully access, analyse, or otherwise use personal data, which was shared by an individual with a reasonable expectation of privacy without the knowledge or consent of the individual

We do not attempt to knowingly and purposefully re-identify de-identified data, and we make all reasonable efforts to prevent any unlawful and unjustified re-identification

Data security: We ensure reasonable and appropriate technical and organizational safeguards are in place to prevent unauthorised disclosure or breach of data

Risk and harm assessment and risk mitigation: We perform a risk assessment and implement appropriate mitigation processes before any new or substantially changed project is undertaken We take into consideration the impact that data use can have not only on individuals but also on groups of individuals. We ensure that the risks and harms are not excessive in relation to the positive impact of the project

Data sensitivity: We employ stricter standards of care while conducting research among vulnerable populations and persons at risk, children and young people, and any other sensitive data

Data minimisation: We ensure the data use is limited to the minimum necessary

Data retention: We ensure that the data used for a project is being stored only for the necessary duration and that any retention of it is justified

Data quality and accountability: We design, carry out, report and document our activities with adequate accuracy and openness

Our collaborators: We require that our collaborators are acting in compliance with relevant law, data privacy and data protection standards and the United Nations' global mandate.

* Available at: https://www.unglobalpulse.org/privacy-and-data-protection-principles


unicef
Office of Research-Innocenti